Cisco Secure Agile Exchange User Guide

First Published: 2021-04-27

CONTENTS

Get Started with SAE GUI

This chapter describes the Cisco Secure Agile Exchange (SAE) GUI and how you can use it to design your services, create sites, deploy your services and sites, and view and edit details related to your SAE sites. For information on the Cisco SAE solution, its components, and deployment workflow, see Cisco Secure Agile Exchange (SAE) Solution Guide.

About SAE UI

The UI makes it fast and easy for you to design your services, create service chains, and deploy your services and sites. When you have brought up your CSP devices and switching, you can use the UI to perform all other service chain workflows.

Deploy SAE Solution QCOW2 in CSP

Recommended Resources, Pre-requisites, and Packages

Recommended resources for the qcow2 service is as follows:

- **CPU:** 4 CPU's

- **RAM:** 32 gigabytes

- **Hard Disk:** 300 gigabytes or more

Prerequisites

- CSP version should be greater than 2.5.1

- Have the host information like hostname, IP address, netmask, gateway, DNS IP address handy.

- VLAN # and Management Network for VNF running in the CSP where this host is going to be deployed.

Packages

The sae-solution image and sae-sol-2-2-0-1.qcow2, is an image that packages the following OS/applications.

- **Harmon CentOS 7:** CentOS provided by Harmon with Linux kernel hardened up.

- **NSO Platform version:** 5.2.3.6

- **SAE Core Function Pack (CFP) version:** 2.2

- **Network Element Driver (NED):** Beside the NEDs that come with SAE CFP, additional NEDs are bundled in this qcow2.

  - **CSRv:** cisco-ios-cli-6.66 version 6.66.1

  - **ASAv:** cisco-asa-cli-6.11 version 6.11

  - **Palo Alto:** paloalto-panos_cli-cli-4.7 version 4.7.4

  - **Tailf-HCC:** tailf-hcc version 4.5.0

  - **Quagga:** quagga-bgp-cli-4.2 version 4.2.6

- **SAE GUI:** version 2.2.0-2020-Dec-21-15_09

Note For more information, on how to deploy the QCOW2 image on CSP, connect to our CISCO Support/Service team.

SAE Upgrade Procedure

Upgrade and Install SAE RPM package

Run the following command to check and remove previous version of RPM and Debian before installing new RPM.

For RPM

1. Verify if any previous RPM's are present on your VM by running the following command.

   ```
   rpm -qa saeui
   ```

2. Remove the previous RPM's by running the following command.

   ```
   sudo rpm -e <package name>
   ```

   Example is as follow:

   ```
   sudo rpm -e saeui-2-1.0.noarch
   ```

For Debian

1. Verify if any previous Debian's are present on your VM by running the following command.

   ```
   dpkg -l saeui
   ```

2. Remove previous Debian's by running the following command.

   ```
   sudo dpkg -r <package name>
   ```

   Example is as follow:

   ```
   sudo dpkg -r saeui
   ```

Log In

Access the SAE UI by entering the network IP address of SAE in the browser.

Use the UI continuously to remain logged in. You are logged out of your session automatically after 30 minutes of inactivity.

Step 1 Enter the URL in your browser.

Step 2 Enter the username and password that is assigned to you by the system administrator. The home page displays.

Step 3 To log out, expand the drop-down list next to your username at the top-right corner and click **Logout**.

Default Home Page

After you log in to SAE GUI, you see the home page and **Configuration** is selected by default. You will be on the **Site** area. If you have already configured sites using the GUI, a snapshot of all your sites is displayed. If you don't have any existing infrastructure and are starting from scratch, the site area will be blank.

The home page has the two main areas: **Configuration** and **Monitoring & Operations**

Configuration has the following areas: **Site**, **Service Design**, **Service Catalog**, and **Global**.

- **Site:** A Site is a collection of CSPs and physical network functions installed in one location. It allows you to onboard your installation into your SAE software. The Site area displays snapshots of your existing sites and tenants under each of your sites. For existing sites, you can perform the following actions: export infrastructure, add resource zone, add tenants to the site, discover site inventory, edit site, and delete site. Click **Add** to create a new site.

- **Service Design:** The Service Design area is the area where you create the templates i.e., Service templates as well as the Service Chain templates. The Service templates will define how the service will look like e.g. number of CPUs, type of VNFs, etc. The Service Chain templates will define the structure of the service chain. However, Service template is VNFD and Service Design template is NSD. The Service Design area has three subareas: **Virtual Services, Physical Services,** and **Service Chains**. If you have existing virtual services, the Virtual Services area displays them by default in card view. Click **Add** to add virtual services.

  The **Virtual Services** subarea displays your existing virtual service if any in card view by default.

  The **Physical Services** subarea displays your existing physical service if any in card view by default.

  The **Service Chains** subarea displays your existing service chains if any in card view by default. The card view displays the service chains according to the NSD Group name. If the NSD Group name is not defined the service chains created will be displayed in the **Default** group. Click **Add** to create a new service chain.

- **Service Catalog:** The Service Catalog area has the following subareas: **Catalog**, **Virtual Service Instance**, **Physical Service Instance**, **Service Chain Instance**, **Organization**, and **Server Profile**. The Catalog area displays your existing catalogs, if any, by default in card view.

• **Global:** The Global area has the following subareas: **IP Address Pool**, **ID Pool**, **Authentication**, **Settings**, **Devices** and **Config Parameters**. You can complete basic configuration tasks like creating authentication groups for NSO to access your devices and services and creating resource pools.

Monitoring & Operations has the following sections: **Device Notifications** and **Service State Changes**. The monitoring operation section display the notifications extracted from NSO.

Service Deployment Stages

Service deployment stages in SAE are broadly categorized into Infrastructure, Service Design, and Service Deployment. Each of these stages has a set of tasks that are associated with them. The tasks are like building blocks for deploying services. Unless stated otherwise, you can perform the tasks in any order.

Infrastructure

Setup: The infrastructure setup stage includes modeling and wiring the hardware devices and configuring them. These tasks are outside the scope of SAE GUI.

Infrastructure Discovery: When the infrastructure is set up, use the SAE GUI to discover it.

Authentication: Use the SAE GUI to complete some basic global configuration such as adding authentication groups. Authentication groups contain the credentials for NSO to access your devices.

Resource Pools: Resource pools include VLAN ID Pool, BGP autonomous system Pool, Management IP pool, Data IP Pool, and VNID Pool. You need resource pools at the time of creating a site. Resource pools are assigned to SAE sites and the tenants under the sites.

Catalog: Think of a catalog as a container that holds together information server profiles and service chain instances that SAE sites and tenants can use. You need a catalog at the time of adding your organization and tenant and creating service instances and service chain instances. When you associate a catalog with to your organization, the organization can use all the services and service chains associated with the catalog.

Organization: Adding organizations and tenants allow you to associate catalogs with them.

Site: Create an SAE site for your organization or tenants and allocate resource pools to them for use during service deployment.

Service Design

Services: In the service design phase, you add services like routers, firewall, and load balancers. At the time of adding services, you can also add specifications for each of the services: disk space, memory, the location where the software image of the service can be downloaded from, interfaces to be used, CPU, and so on.

Service Chains: Similar to how hardware appliances are connected to each other, service chains are formed by connecting services. All end-to-end service chains have a consumer endpoint and a provider endpoint. Half chains have either a consumer or a provider endpoint on one end and a chain endpoint on the other. Use the chain endpoints to connect two half chains.

Service Instances: Services are generic, whereas service instances are specific sets of configurations that can be applied to your services. You can define multiple service instances for a single service by changing some parameters like service flavor, and other variables. At the time of deploying a service chain, you choose a service instance to apply to the service you choose.

Service Chain Instances: Similar to service instances, you can create service chain instances for each of the services in a service chain. At the time of creating a service chain instance, you choose a catalog that the

service chain instance should be a part of. You also choose the service chain for which you are creating the instance. After this, you can specify service instances for each of the services in the service chains.

Service Deployment

Service Chains: In the Site area of the GUI, you can add consumer half chains, provider half chains, stitching chains, end-to-end chains, and gateways. The service chain models that you created during the Design phase will be available for you to add to your sites.

Endpoints: Create endpoints to connect service chains to the external network. Endpoints can be created at an organization (provider) level and at the tenant level. Both provider level and tenant level endpoints can be created from the Site area. When you click any tenants from the Site area, you can view and edit their details and also see all the provider level and tenant level endpoints.

About Global Configuration

You can use the SAE UI to configure some part of the infrastructure such as authentication groups and resource pools.

View Authentication Groups and Resource Pools

Step 1   Click **Configuration** at the top-right corner of the homepage.

Step 2   Click the **Global** tab.

Step 3   Depending on your requirement, click one of the following tabs: **IP Address Pool**, **ID Pool**, or **Authentication**, **Settings**, **Devices**, **Config Parameters**.

Your resource pools or authentication groups are displayed in card format by default, where each card represents a resource pool or an authentication group.

Note   For **Settings**, **Devices** and **Config Parameters**, there is no option to toggle between card view and list view. If you click either Settings or Devices or Config Parameters, the default view is displayed.

Step 4   Click **List View** to view your resource pools or authentication groups in a list format.

Create IP Address Pools

IP Address Pool: SAE core function pack assigns IP addresses to virtual links between services from this pool.

Create the following distinct resource pools.

• **Data IP Pool:** SAE core function pack assigns IP addresses to virtual links in service chain.

• **Management IP Pool:** SAE core function pack assigns IP addresses to management interface of the service from this pool.

Step 1   Click **Configuration** at the top-right corner of the homepage.

Step 2   Choose **Global** > **IP Address Pool**.

Step 3   Click **Add**.

Alternatively, on the card view click ☐ to copy an existing IP address pool and edit and save it with a new name.

Step 4   Provide the requested information.

a)   **Name:** Enter a name for your IP pool.

b)   **Alarm:** Choose **Enabled** or **Disabled** from the drop-down list.

When you select Enabled, NSO triggers an alarm when the IP address pool falls below the capacity threshold you set.

c)   **Low Capacity Threshold (%):** Enter a value for the low capacity threshold. Low Threshold percentage is the capacity threshold you set for IP address pools.

d)   **Tag:** Choose the resource pool tag ASN, VLAN, VNID, MGMT or DATA from the dropdown.

The created pool will get associated with the selected tag value and this tag value is helpful in deploying endpoint-gateway-vnf, service-chain and stitching services.

e)   **Subnet: Click** + next to **Subnet** and enter an IP address and Mask. Note: Subnet allows you to choose the pool of available IPs but it is not used for networking as a subnet mask.

f)   **Exclude: Click** + next to **Exclude** and enter an IP address and Mask to exclude.

g)   **Range: Click** + next to **Range** and enter a number From and To for the range.

Step 5   (Optional) Click **Validate** to verify your inputs.

Step 6   Click **Save** to save the IP address pool.

To edit an existing IP address pool, select the pool in the card view and update the information. Note: The name of the IP address pool cannot be edited however, you can edit the IP address pool if no service is deployed.

Click   to delete an existing IP address pool.

What to do next

Repeat this procedure to create all the IP address pools that you need for your SAE deployment.

Click **Back** to go back to the previous page.

Create ID Pools

ID pools are used to define pools of VLANs, BGP AS numbers, and VNIDs for spine-leaf topologies.

Step 1   Click **Configuration** at the top-right corner of the homepage.

Step 2   Choose **Global** > **ID Pool**.

Step 3   Click **Add**.

Alternatively, click   to copy an existing ID pool in card view and edit and save it with a new name.

Step 4   Provide the requested information.

    a) **Name:** Enter a name for your ID pool.

    b) **Start Range: Enter** a number for the start of your ID pool range.

    c) **End Range:** Enter a number for the end of your ID pool range.

    d) **Alarm:** Choose **Enabled** or **Disabled** from the drop-down list.

        When you select Enabled, NSO triggers an alarm when the ID pool fall below the low threshold capacity you set.

    e) **Low Capacity Threshold:** Enter a low threshold capacity percentage. If you select Enabled in the previous step, NSO triggers and alarm when the ID pool falls below the threshold you set here. By default, it is set to 10 for 10%.

    f) **Tag:** Choose the resource pool tag ASN, VLAN, VNID, MGMT or DATA from the dropdown list.

        The created pool will get associated with the selected tag value and this tag value is helpful in deploying endpoint-gateway-vnf, service-chain and stitching services.

    g) **Excludes:** Click + next to **Exclude**. The **Exclude details** window opens. Enter start and end numbers for the range to be excluded for the ID pool.

Step 5 (Optional) Click **Validate** to verify your inputs without pushing configuration into NSO database.

Step 6 Click **Save** to save the ID pool.

To edit an existing ID pool, select the pool in the card view and update the information. Note: The name of the ID pool cannot be edited however, you can edit the ID pool if no service is deployed.

Click [trash icon] to delete an existing ID pool.

Click **Back** to go back to the previous page.

Add Authentication Information

The authentication information that you add enables NSO to access your devices and services. Add authentication for every device and service that is managed by NSO: CSP devices, Nexus 9000 switches, VNFs, and ESC. Define access authentication parameters such as: username, password (used by NSO to SSH), and secondary password (used by NSO to access configuration mode).

Step 1 Click **Configuration** at the top-right corner of the homepage.

Step 2 Choose **Global** > **Authentication**.
All your existing authentication groups display. To edit any of the existing authentication information, click the authentication group in the card view and update your username, password, or secondary password. Note that the name of the authentication group cannot be edited.

Step 3 Click **Add**.

Step 4 Provide the requested information.

a) **Name:** Enter a name for the auth group.
b) **Tag:** Choose the type of authgroup tag from the dropdown.
c) **Username:** Enter a username for the auth group.
d) **Password:** Enter a password for the auth group.
e) **Confirm Password:** Enter the same password to confirm password the auth group.
f) **Secondary Password:** Enter a secondary password for executing privilege command as some device may require it to execute. Note: It is called as CISCO parlance <enable password>.

g) **Secondary Confirm Password:** Enter a secondary password to confirm the execution of the privilege command.

Step 5 (Optional) Click **Validate** to verify your inputs.

Step 6 Click **Save** to save the authentication details.

Click 🗑 to delete an existing set of authentication details.

What to do next

Repeat this procedure to add authentication details for all the devices and services that you plan to use for your SAE deployment.

Click **Back** to go back to the previous page.

Add SAE Settings

This section allows you to add settings like timeout, network capability and ACI interface type.

Step 1 Click **Configuration** at the top-right corner of the homepage.

Step 2 Choose **Global** > **Settings** > **SAE Settings**.

Step 3 Provide the requested information.

a) **Time Out:** Enter a timeout value. The permitted range is 1320 to 65535.

b) **Network Capability:** Enter the network capability in the following format:

- **NIC _TYPE: Click** + next to **Network Capability** and enter NIC physical hardware component for the network connection.

- **NW_Type: Click** + next to **Network Capability** and enter the network type for the SAE.

c) **ACI Interface Types:** Click the + sign next to ACI Interface Type and enter the ACI Interface Type.

458083

Step 4 (Optional) Click **Validate** to verify your inputs.

Step 5 Click **Save**.

What to do next

Repeat this procedure to create all the SAE Settings that you need for your SAE deployment.

Add Devices Global Settings

This section allows you to add device global settings for read, write, and connect for new connections.

Step 1 Click **Configuration** at the top-right corner of the homepage.

Step 2 Choose **Global** > **Settings** > **Devices Global Settings**.

Step 3 Provide the requested information.

    a) **Read Time Out:** Enter a read timeout value for reading the data. The permitted range is 1320 to 65535.

    b) **Write Time Out:** Enter a write timeout value for writing the data. The permitted range is 1320 to 65535.

    c) **Connect Time Out:** Enter a connect timeout value for a new connection. The permitted range is 1320 to 65535.

458084

Step 4 (Optional) Click **Validate** to verify your inputs.

Step 5 Click **Save**.

Add a Device

The devices screen shows you your device inventory. You can add new devices from this area.

Follow these steps to directly add devices using the GUI.

Step 1 Click **Configuration** at the top-right corner of the homepage.

Step 2 Choose **Global** > **Devices**.

Step 3 Click **Add**.

Step 4 Provide the requested information.

a) **Skip SSH:** Select this check-box if you want the device to skip the step to fetch SSH keys.

b) **Name:** Enter a name for your device.

c) **Address:** Enter the IP address of your device.

d) **Port:** Enter the port number to be used to connect to the device.

e) **AuthGroup:** Choose the appropriate auth group from the drop-down list.

f) **Type:** Select netconf, generic, or CLI from the drop-down list.

g) **Trace:** By default *cisco-apicdc-gen-3-9* trace is selected.

All the interactions between the device and NSO are logged in the trace log. Choose the following options from the dropdown.

 • **Pretty:** The trace log will print in Pretty-print data structure.

 • **Raw:** The trace log will print in unformatted structure.

 • **False:** The trace log will not be generated.

Note you can edit the existing trace log after the device is created in the table list view.

Step 5 Click **Save** to add the device.

A pop-up screen shows the progress of the new device you added in terms of device creation and connection.

Click the **Select Columns** dropdown list and select the checkbox to add the columns in the device table list view.

Select the **Filter Row** checkbox and enter the value in the respective column to filter the device table.

Enter the device name in **Search Device** to search the device.

Click the **Export** button to export all the devices in bulk.

You can edit an existing IP Address and Authgroup in table list view column to update the information.

Click ⬚ in **Delete** column to delete an existing device.

By default, the device table displays 10 rows per page. Click on the **Rows per page** dropdown to change the pagination. You can add maximum 40 rows per page.

Add APIC Device

The devices screen shows you your device inventory. You can add new APIC devices from this area.

Follow these steps to directly add APIC devices using the GUI.

Step 1	Click **Configuration** at the top-right corner of the homepage.
Step 2	Choose **Global** > **Devices**.
Step 3	Click **Add**.
Step 4	Provide the requested information.

 a) **APIC Device:** Select this checkbox if you want the add APIC device

 b) **Skip SSH:** Select this check-box if you want the device to skip the step to fetch SSH keys.

 c) **Name:** Enter a name for your device.

 d) **Address:** Enter the IP address of your device.

 e) **Port:** Enter the port number to be used to connect to the device.

 f) **AuthGroup:** Choose the appropriate auth group from the drop-down list.

 g) **Type:** By default, *generic* type is selected.

 h) **Trace:** By default, *cisco-apicdc-gen-3-9* trace is selected.

  All the interactions between the device and NSO are logged in the trace log. Choose the following options from the dropdown.

   • **Pretty:** The trace log will print in Pretty-print data structure.

   • **Raw:** The trace log will print in unformatted structure.

   • **False:** The trace log will not be generated.

  Note you can edit the trace log after the device is created in the table.

 i) **Connect TimeOut:** Enter a connect timeout number in seconds for a new connection. The permitted range is 1320 to 65535.

 j) **Read TimeOut:** Enter a read timeout number in seconds for reading the data.

 k) **Write TimeOut:** Enter a write timeout number in seconds for writing the data.

 l) **Out Of Sync Commit Behaviour:** Choose *Reject* or *Accept* option from the drop-down list.

Step 5 Provide the requested information for **NED Settings**.

 a) **Log Verbose:** Choose true or false from the drop-down list.

b) **Config Path:** Enter the configuration path to save the APIC configuration files.

c) **Local Host:** Choose true or false from the drop-down list.

d) **Host:** Enter the host number.

e) **User Name:** Enter the user name for the NED Settings.

f) **User Password:** Enter the user name for the NED Settings.

g) **Disable Check Sync:** Choose true or false from the drop-down list.

h) **Ignore Passwords:** Choose true or false from the drop-down list.

i) **Enable-L3ExtOut-CFG-Split:** Choose true or false from the drop-down list.

j) **Alternative Hosts:** Click + next to **Alternative Hosts** and enter the IP Address.

You can add maximum 10 IP addresses.

Step 6   Click **Save** to add the APIC device.

Click the **Select Columns** dropdown list and select the checkbox to add the columns in the device table list view.

Select the **Filter Row** checkbox and enter the value in the respective column to filter the device table.

Enter the device name in **Search Device** to search the device.

Click the **Export** button to export all the devices in bulk.

You can edit an existing IP Address and Authgroup in table list view column to update the information.

To edit an existing APIC device, in **Edit** column, click the pencil icon and update the information. Note that the APIC device name cannot be edited.

Click [icon] in **Delete** column to delete an existing APIC device.

By default, the device table displays 10 rows per page. Click on the **Rows per page** dropdown to change the pagination. You can add maximum 40 rows per page.

Add Config Parameters

This section allows you to add SAE Config Parameters for global settings.

Step 1   Click **Configuration** at the top-right corner of the homepage.

Step 2   Choose **Global** > **Config Parameters**.

Step 3   Click **Add**.

Step 4   Provide the requested information.

a) **Name:** Click + next to **SAE Config Parameters** and enter the name for the global configuration parameter.

b) **Value:** Enter the global parameter value for SAE Configuration.

Step 5   (Optional) Click **Validate** to verify your inputs.

Step 6   Click **Save** to save the Configuration Parameter.

Import and Export Global Configuration

This topic describes the following:

- How to import IP address pools, ID pools and Authentication individually or in bulk.

- How to export devices in bulk.

To be able to import files, the file should be in XML or JSON format. Similarly, the files are also exported in XML or JSON format.

Step 1   Click **Configuration** at the top-right corner of the homepage.

Step 2   Click the **Global** tab.

Step 3   Depending on your requirement, click one of the tabs: **IP Address Pool**, **ID Pool**, **Devices** or **Config Parameters**.

Action	Result
Click **IP Address Pool**	Your IP address pools are displayed in card view. **Import IP Address Pools in Bulk** • Click the **Import** button to import XML or JSON files containing configuration for single or multiple IP address pools. **Export IP Address Pools in Bulk** • Click the **Export** button to export your existing IP address pools in bulk in XML or JSON format. **Export Individual IP Address Pools** • Click the ⬇ on the card of the IP address pool to export in JSON and XML format.
Click **ID Pool**	Your ID Pools are displayed in card view. **Import ID Pools in Bulk** • Click the **Import** button to import XML or JSON files containing configuration for single or multiple ID pools. **Export ID Pools in Bulk** • Click the ⬇ on the card of the IP address pool to export in JSON and XML format. **Export Individual ID Pools** • Click the Download Icon on the card of the ID pools you want to export in JSON format.
Click **Devices**	Your existing authentication groups are displayed in card view. **Export Devices in Bulk** • Click the **Export** button to export all your existing devices in XML or JSON format. **Export Individual Devices** • Click the ⬇ on the card of the IP address pool to export in JSON and XML format.

Action	Result
Click **Config Parameters**	Your existing config parameters groups are displayed. **Import Config Parameter in Bulk** • Click the **Import** button to import XML or JSON files containing configuration for single or multiple Config Parameter. **Export Devices in Bulk** • Click the **Export** button to export all your existing config parameters. in XML or JSON format.

Design Your Service

In the design phase of SAE, you create service definitions for virtual and physical services that you have identified to be part of your service design. Next, you create service chains by connecting the services. Consumers connect with providers through service chains.

The **Service Design** area is where you create services and service chains.

List View for Services and Service Chains

Step 1 Click **Configuration** at the top-right corner of the homepage.

Step 2 Click **Service Design**.

Step 3 Depending on your requirement, click one of the following tabs: **Virtual Services**, **Physical Services**, or **Service Chains**.

Your services or service chains are displayed in card format by default, where each card represents a service or a service chain.

Step 4 Click the **List View** to view your services or service chains in a list format.

Add a Virtual Service

Service definitions include the following information about the virtual service: type of service, vendor, compute information, deployment flavors, storage profiles, and so on.

Step 1 Click **Configuration** at the top-right corner of the homepage.

Step 2 Choose **Service Design** > **Virtual Service**.

Your existing virtual services are displayed in card view by default. Click **List View** to view your existing virtual services as a list.

Step 3   Click **Add**.

Alternatively, click   to copy an existing service and edit and save it with a new name.

Step 4   Provide the requested information.
   a)   **Name:** Enter the name of your service.
   b)   **Service Type:** Specify the service type, such as, router, firewall, and so on. Based on the service type you select, the destination file may be auto-populated for some of the type.
   c)   **Vendor:** Enter the name of the service provider. Example: Cisco, AVI, Fortinet and so on.
   d)   **Version:** Enter the product version.
   e)   **Software Version:** Version of the software used for the product.
   f)   **Product Name:** Enter the product name of the service. Example: Cisco ASAv, CSR and so on.
   g)   **Product Information:** Provide a description for the service.
   h)   **VIM Type:** The server type where this service will be hosted.

Step 5   Click + next to **Flavor(s)**. In the section that expands, enter the required information.

Alternatively, click   to copy an existing flavor and edit and save it with a new name.

Click   to delete an existing flavour.

Table 1: Properties

Field	Description
Name	Enter a name for the flavor.
Description	Enter a description.
Virtual Memory	Enter the virtual memory in GB.
Virtual CPU	Enter the number of CPUs to be allocated to the service.

Storage: Click + to expand the field and enter the storage in GB to be allocated for this service.

Table 2: Image

Field	Description
Name	Enter the name of the software image.
URL	Provide the url to the software image.
Version	Enter the version number of the software image.
Disk Format	Choose one of the disk formats: qcow2, raw, vmdk.
Disk Type	Choose the disk type to be used while deploying the service. The options are ide or Virtio. However, we recommend you to use Virtio.

Field	Description
Serial Console	Choose True or False to enable or disable serial console connectivity to the service.

Day 0 Configuration Files

According to the **Service Type** selected the day0 file (bootstrap file) name will be auto populated.

- If applicable, click + to expand the field.

- Filename: Enter the name of the day-0 file as used in the service.

Table 3: Device Management Protocol

Field	Description
Device Type	From the drop-down list, choose one of the following: generic, netconf, CLI or none. NSO uses your selected protocol to communicate with the service and depending on the options chosed the **Protocol** and **Port** fields are displayed.
NED ID	From the drop-down, choose the NED ID that NSO should use to communicate with the service. The drop-down list only shows the NED IDs that have already been loaded on NSO.
Protocol	The protocol is used by NSO to communicate with this service. **Note** For **CLI** device type, choose from the drop-down list any one of the following protocol: Telnet or SSH.
Port	The port number is auto-populated according to you selction.

Table 4: VNIC

Field	Description
Name	Enter a name for the VNIC.
Interface-ID	Enter interface ID. This is the interface ID that is used within the service.
Management	Select the Management checkbox if this interface will be used for managing the service.
Logical Interface	Select this checkbox if the interface you are adding is a logical interface. This interface is used to create interfaces, which are not directly associated with a physical interface.

Field	Description
BIT Rate Requirement	Enter the bit rate that the interface requires. This information is used for computing used bandwidth of this VNIC when this interface is mapped to a physical link. **Note** If you don't specify the bit rate at the time of creating a service chain, the service chain bandwidth is used as the interface bandwidth.
Internal Virtual Link Descriptor	From the drop-down, choose any one of the following: inside, outside, out-inside or out-outside.
NW Type	From the drop-down, choose SRIOV or VIRTIO interface for the service.
NIC Type	Select a NIC type from the drop-down list. This is the physical NIC for this interface while mapping it to a physical port. You can select multiple NIC types using the multi select option. In such a case either of the NIC types may be used. If you don't select a NIC type, any of the available NICs is used. Note: It is recommended that you choose a single NIC type.

Table 5: Network Capabilities

Field	Description
Name	The GUI generates a random name for each new requirement.
Network Capabilities	You can configure one or more key-value pairs for each requirement.

Click **Add More VNICs** link at the right bottom corner to add additional VNICs.

Step 6   (Optional) Click **Validate** to verify that you have entered all the information on the page correctly. If not, an error report displays. Correct the errors, if any.

Step 7   Click **Save**.

Click ⬇ to export an existing virtual service.

Click ◆ to go to the existing service instance card view page.

Click ▢ an existing service to view and edit its details.

Click 🗑 to delete an existing virtual service.

Click **Back** to go back to the previous page.

What to do next

Repeat this procedure to add or seach any other services that you plan to include in your service chain.

On **Search Service**, enter the name of the service you want to search in the card view.

Click **Import** next to **Add** to import all the virtual service instances.

Click **Export** to export all the physical service instances in JSON or XML format.

Add a Physical Service

Service definitions include the following information about the service: name of service, vendor, geographical location information, funcion description, and so on.

Table 6: Feature History

Feature Name	Release Information	Description
Physical Service	Cisco SAE GUI Release 2.2.0	This feature enables you to add, export, import,and delete a physical service.

Step 1 Click **Configuration** at the top-right corner of the homepage.

Step 2 Choose **Service Design** > **Physical Service**.

Step 3 Your existing physical services are displayed in card view by default. Click **List View**to view your existing physical services as list.

Step 4 Click **Add**.

Alternatively, click to copy an existing service and edit and save it with a new name.

Step 5 Provide the requested information.
   a) **Name:** Enter the name of your service.
   b) **Vendor:** Enter the name of the service provider. Example: Cisco, AVI, Fortinet and so on
   c) **Version:** Enter the product version.
   d) **Geographical Location Info:** Enter the geographical location of the physical network function.
   e) **Function Description:** Provide a description for the service.

Step 6 Click + next to **External Connection Point Descriptor**. In the section that expands, enter the required information.

Table 7: Properties

Field	Description
Name	Enter a name for the External Connection Point Descriptor
Interface ID	Enter the value of the interface ID

459277

Step 7   (Optional) Click **Validate** to verify that you have entered all the information on the page correctly. If not, an error report displays. Correct the errors, if any.

Step 8   Click **Save** to save the service.

Click ⬇ to export an existing physical service.

Click ◆ to go to the existing service instance card view page.

Click ⬜ an existing service to view and edit its details.

Click 🗑 to delete an existing physical service.

Click **Back** to go back to the previous page.

What to do next

Repeat this procedure to add or search any other services that you plan to include in your service chain.

On **Search Service**, enter the name of the service you want to search in the card view.

Click **Import** next to **Add** to import all the physical service instances.

Click **Export** to export in bulk all the physical service instances in JSON or XML format.

Create Service Chains

Consumers and providers connect through end-to-end, full service chains, or through two half chains that are connected. Typically, half service chains separate consumers and providers on the basis of trust and network speed.

Service chain creation can be broken down into the following steps.

1. Add services that you to include in your service chain.

2. Add external connections for your service chain. For end-to-end service chains, you should create one consumer endpoint, and one provider endpoint.

3. Connect the services to each other. Services are connected to each other through internal connections. When you draw a connection between services, the pop-up menu to add information about internal connections displays.

4. Connect the external connections to the services.

Limitations for Creating Service Chains Through the GUI

- Service chain flavors cannot be created using the SAE GUI. Although you can create service chain flavors using CLI, it is not recommended because such service chains will not be supported in the GUI.

- If you have created service chains using CLI, the UI supports them only if they have the configuration that is supported by the UI. For example, service chain flavors that are created using the CLI are not supported on the UI.

- Any service chains created using CLI must be edited in the Service Design area. You may have to reorder some of the services and draw connections between endpoints and services, if they are missing. Unless this step is completed for service chains created using CLI, you will not be able to deploy these chains using the GUI.

Step 1   Click **Configuration** at the top-right corner of the homepage.

Step 2   Choose **Service Design** > **Service Chain**.

Step 3   Click **Add**.

Alternatively, click [icon] to copy an existing service chain and edit and save it with a new name.

Step 4   Provide the requested information.

a) **Name:** Enter a name for your service chain.

b) **NSD Group Name:** From the drop-down list, choose any one of the NSD group name or you can enter your own group name for the service.

c) **NSD Version:** Enter the NSD Version for your service chain.

Step 5   Click + next to **Affinity** to expand the section and provide the requested information.

The following table shows the different combinations of affinity type and affinity scope and the resulting affinity behavior.

Affinity Type	Affinity Scope	Result
Affinity	server	The services are placed on the same CSP server
Affinity	zone	The services are placed on CSP servers within the same zone
Anti-affinity	server	The services will not be placed on the same CSP server
Anti-affinity	zone	The services will not be placed on servers in the same zone.

Step 6   **Note**   You can choose to add virtual service and the add physical service or vice-versa depending on your requirement.

Follow te below steps to add virtual service:

Click **Add Virtual Service**. Select a virtual service from the list of services.

Step 7   Choose the service flavor, Management VNIC, and Affinity from the drop-down lists.

Step 8   Click **OK**.

Repeat steps 6-7 as many times as needed until you have added all the virtual services that will be part of your service chain.

Step 9   **Note**   The next step is to add physical service.

Click **Add Physical Service** and choose the pysical service from the drop-down list.

Step 10   Click **OK**.

Repeat steps 9 as many times as needed until you have added all the physical services that will be part of your service chain.

Step 11   **Note**   The next step is to add external connections. You need to add two external connections, one for each end of the service chain.

Click **Add External Connection** and provide the required information.

a) **Name:** Enter a name for your external connection.
b) **SAPD:** Choose a Service Access Point Descriptor (SAPD) from the drop-down list. For end-to-end service chains, choose consumer from the drop-down list. For half chains, choose chain from the drop-down list.

Repeat step 11 to add the second external connection. For end-to-end service chains, choose provider from the SAPD drop-down list. For half chains, choose chain again.

At this point, you should see all the services you want included in the service chain on the screen. You should also have two external connections.

Step 12   Ensure that the external endpoints and the services are arranged in a sequence from left to right, starting from the consumer-endpoint and ending with the provider-endpoint, with services in the middle.
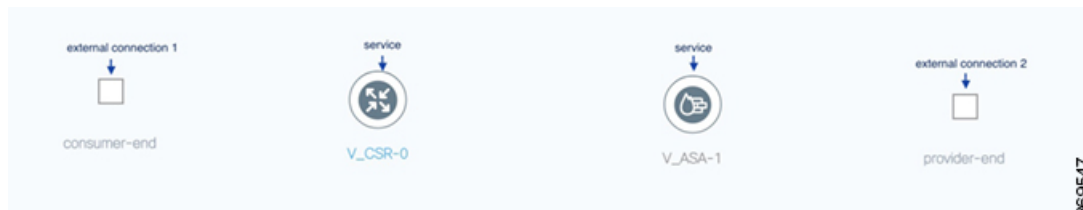

Step 13   In this step, you will connect the endpoints and services to form a service chain. There are two ways of connecting the components.

• Connect the services to each other first and then connect the endpoints to the services.

• Start from the left and connect the first endpoint to the first service. Next, connect the service to the other services in the sequence, and then connect the last service in the sequence to the other endpoint.

You can choose any way of connecting the endpoints and services. This topic shows the first option.

Step 14   To connect the services to each other, click the first service in the sequence. The connectors display around the service. Drag one of the connectors towards the other. The internal connection pop-up menu displays. Provide the requested
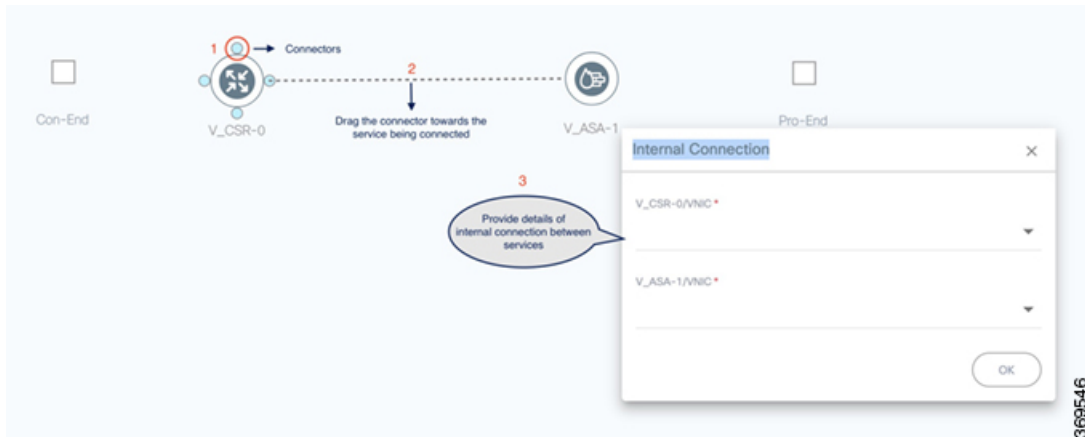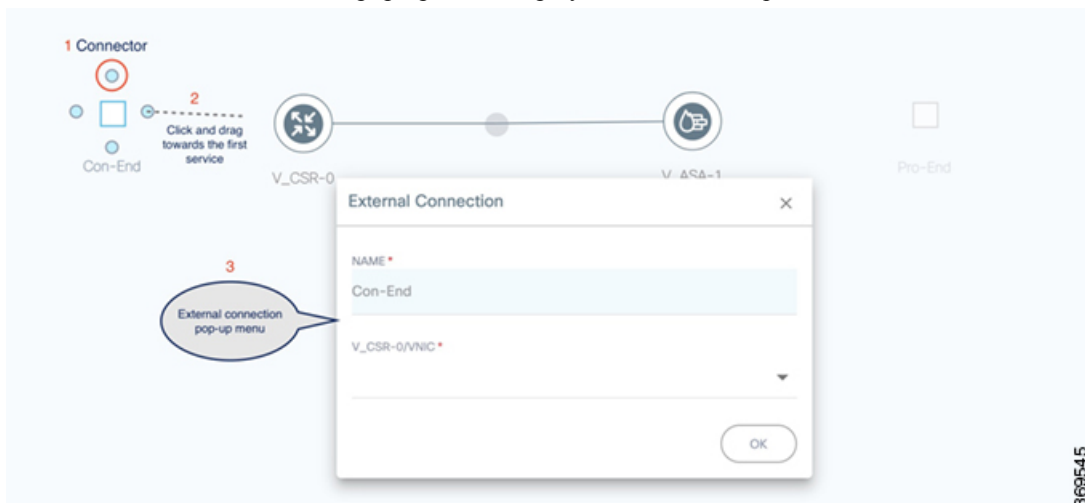

information.

Repeat step 14 to connect any other services to each other.

Note   • When you are creating a service chain diagram by connecting all the components together, ensure that the diagram is placed at the center of the page. This placement is crucial because how the service chain displays at the time of deployment depends on this placement.

• Place the consumer endpoint to the left of the services you are connecting, and the provider endpoint to the right.

Step 15   Click the endpoint on the left to view its connectors. Click and drag any of the four connectors toward the first service in the service chain. The external connection pop-up menu displays. Provide the requested

information.

Step 16   Click the endpoint on the right to view its connectors. Click and drag any of the four connectors towards the last service in the service chain. The external connection pop-up menu displays. Provide the requested information.
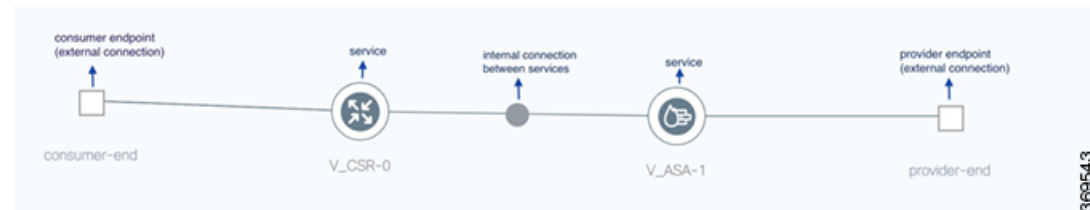
Step 17   (Optional) Click **Validate** to verify your inputs.

Step 18   Click **Save** to save the service chain.

Step 19   **Note**   Click the eye icon on the top right corner to view the SAPDs.

When all your services and endpoints are connected, the service chain should look as follows.

What to do next

Repeat this procedure to create any other service chains.

Click **Back** to go back to the previous page.

Note On the existing service chain, you can do the following tasks:

Click an existing service to view and edit its details. You cannot edit the service chain name however, you can redraw the service chain.

Click the download icon to export an existing service.

Click [trash icon] on a service chain to delete it.

On **Search Service**, enter the name of the service you want to search in the card view.

Click **Import** next to **Add** to import the backup file.

Click **Export** next to **Import** to export in bulk all the physical service instances in JSON or XML format.

Note When you delete a service chain, it goes to the list of deleted chains, from where you must delete it again to remove it permanently.

Import and Export Services and Service Chains

This topic describes the following:

- How to import services and service chains individually or in bulk.

- How to export individual services and service chains.

To be able to import files, they should be in XML format. Similarly, the files are also exported in XML format.

Step 1 Click **Configuration** at the top-right corner of the homepage

Step 2 Click the **Service Design** > tab.

Step 3 Depending on your requirement, click one of the tabs: **Virtual Service**, **Physical Service**, or **Service Chains**

Action	Result
Click **Virtual Service**	Your virtual services are displayed in card view. **Import Virtual Services in Bulk** • Click the **Import** button to import XML files containing configuration for single or multiple virtual services. **Export Virtual Services in Bulk** • Click the **Export** button to export your existing virtual services in bulk in JSON and XML. **Export Individual Virtual Services** • Click the ⬇ icon on the card of the virtual service to export in JSON and XML.
Click **Physical Service**	Your physical services are displayed in card view. **Import Physical Services in Bulk** • Click the **Import** button to import XML files containing configuration for single or multiple physical services. **Export Physical Services in Bulk** • Click the **Export** button to export your existing physical services in bulk in JSON and XML. **Export Individual Physical Services** • Click the ⬇ icon on the card of the virtual service to export in JSON and XML.
Click **Service Chains**	Your existing service chains are displayed in card view. **Import Service Chains in Bulk** • Click the **Import** button to import XML files containing configuration for single or multiple service chains. **Export Service Chain in Bulk** • Click the **Export** button to export your existing service chain in bulk in JSON and XML. **Export Individual Service Chains** • Click the ⬇ icon on the card of the virtual service to export in JSON and XML.

About the Service Catalog

An SAE service catalog has three main elements.

- **List of Server Profiles:** A server profile captures network details such as number of interfaces like Virtio, SR_IOV, and management network names for port channels on the CSP devices or the physical PFTD devices used in the SAE site.

- **List of Catalogs:** A service instance defines a service in terms of how it would be deployed.

- **List of Service Instances:** A service chain refers to a common model for connecting services together.

A catalog in the catalog list can be an organization (provider) catalog or a tenant catalog. If the catalog is for organization (provider) level, it will be associated with all server profiles used for the SAE clusters and will store all the Service Chain Instances which are shared by all tenants under the organization. The catalog for individual tenant cannot be associated with any server profile and will stores only the Service Chain Instances used within the tenant. These Service Chain Instances cannot be shared by other tenants.

View Service Catalog Components

To view the service catalog components follow the below steps:

Step 1 Click **Configuration** at the top-right corner of the homepage.

Step 2 Click **Service Catalog**.

Step 3 Depending on your requirement, click one of the following tabs: **Catalog**, **Virtual Service Instance**, **Physical Service Instance**, **Service Chain Instance**, **Organization**, or **Server Profile**.

The component you choose is displayed in card format by default.

Step 4 Click **List View** to view your catalogs, virtual service instances, physical service instances, service chain instances, organization/providers, or server profiles in form of a list.

What to do next

Repeat this procedure to create any other catalog.

Click **Back** to go back to the previous page.

Note To edit an existing catalog, select the instance and update the information.

Click ▽ to delete an existing catalog.

Create SAE Catalog

The SAE catalog is created and assigned to an organization or tenant. It consists of sever profiles and service chain instance that a provider or tenant can use.

Step 1 Click **Configuration** at the top-right corner of the homepage.

Step 2 Choose **Service Catalog** > **Catalog**.

Step 3 Click **Card view** or **List View** to toggle between the card form and list form views.

Step 4 Click **Add**.

Alternatively, click ⬚ to copy an existing catalogand edit and save it with a new name.

Step 5 **Name:** Enter the name of the catalog. The created catalog are assigned to the organization or tenant.

Step 6 **Server Profiles:** Click + next to **Server Profiles** to add the server profile and service chain instance that provider or tenant will use.

Note First you have to create the Server Profile. The created server profile is reflected in this dropdown and you can choose it. *To create it, refer to the section* ***Add a Server Profile***.

Second, all the Service Profiles should be added only to the Provider Catalog and should **NEVER** be added to the Tenant Catalog.

Step 7 (Optional) Click **Validate** to verify your inputs.

Step 8 Click **Save** to save the catalog.

What to do next

Repeat this procedure to create any other catalog.

Click **Back** to go back to the previous page.

Note To edit an existing catalog, select the instance and update the information.

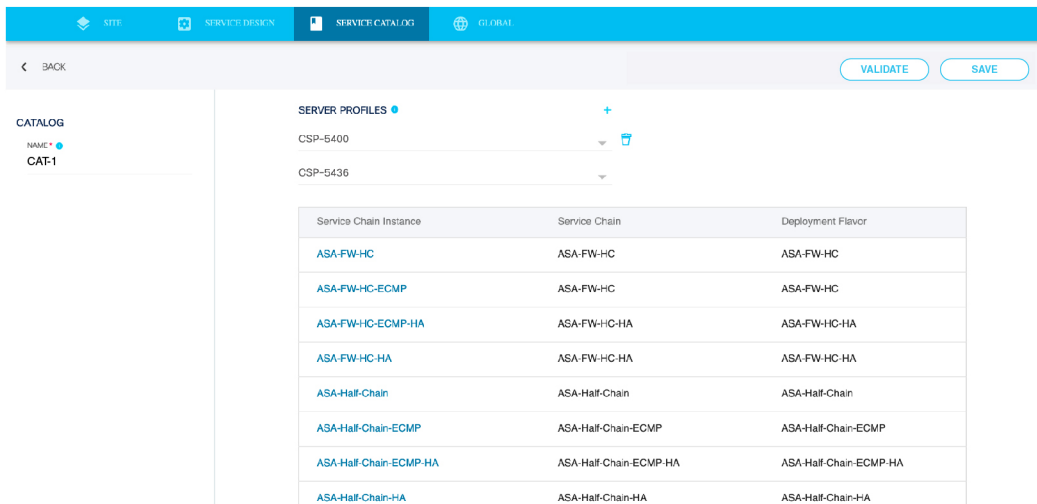Click ⬛ to delete an existing catalog.

Create Virtual Service Instance

A service instance defines a service in terms of how it is to be deployed. It specifies the following for a service: type, HA settings, role (active or standby) and so on.

Step 1 Click **Configuration** at the top-right corner of the homepage.

Step 2 Choose **Service Catalog** > **Service Instance**.

Step 3 Click **Add**.

Alternatively, click ⬜ to copy an existing service instance and edit and save it with a new name.

Step 4   Enter the requested information.

| Field	Description
Name	Enter a name for the service instance.
Service	From the drop-down list, choose the service that you are creating the service instance for.
Flavor	If the service that you selected has a single flavor, the Flavor field populates automatically. However, if the service has multiple flavors, you can choose the desired one from the drop-down list.
Service Configuration Parameters	**Note** The fields in the right panel of the screen populate only after you have selected a service and a flavor. • **Name:** Enter a name for your service configuration.
	Extensions: The Routed check-box is selected by default. • **VNIC Password:** When the service instance is deployed on a CSP device, you can access the services through a VNC. The password that you enter here helps protect against unauthorized access to this service from the console. • **Service Type:** From the drop-down list, select the type of the service. Example types: generic, asav, fdtv. Depending upon the service you select, additional settings may have to be entered.
	Monitoring: When Monitoring checkbox is selected user has to provide values for all the parameters. • **Bootup-Time:** Max time for ESC to wait for the VNF comes up fully. • **Recovery-Wait-Time:** ESC to wait before starting recovery of the VNFPolling • **Frequency:** Wait time for ESC to check the VNF up or down. • **Metric Occurrences Success:** Number of times for ESC to check the VNF success continuiously. Note: If the checks fails within the number of time. You have to restart the check again. • **Metri Occurrences Failure:** Number of times ESC checks the VNF failure. After reaching this number, ESC will give up the VNF with failure sent to NSO

Field	Description
	• **Recovery Max Retries:** ESC waits for recovery max time and during this period, if VM does not come up due to any reason, ESC sends recovery completed with error notification to NSO. Note: Default value is 3.
	Day0 Configuration Files: Provide the destination filename, URL path to day0 file, and configuration parameters.
	• Managed by NSO: Select the check-box if you want the service to be managed by NSO • Management AuthGroup: From the drop-down list, choose the appropriate authentication to enable NSO to access the service instance. • **Day 1:** Click + next to the Day1 option to add the day1 configuration file.
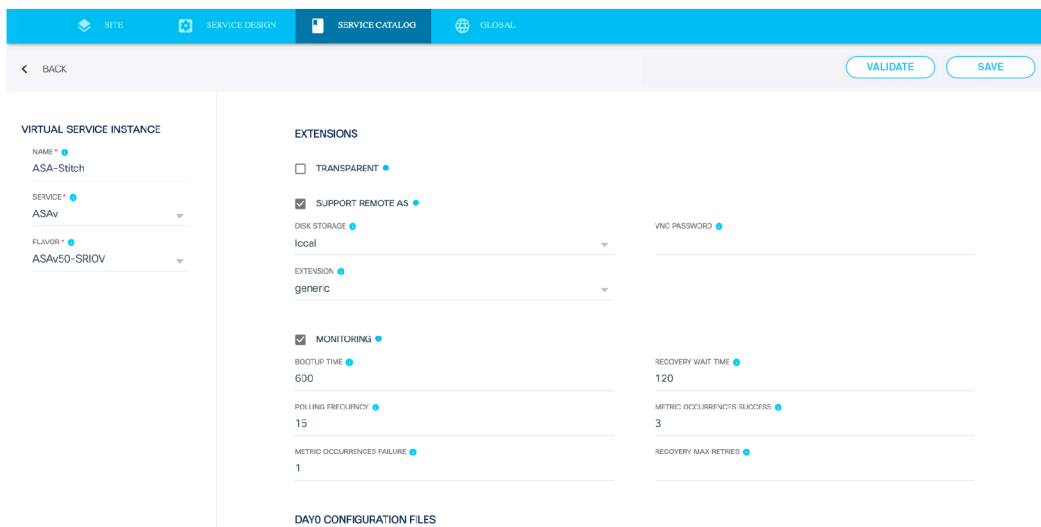
Step 5   (Optional) Click **Validate** to verify your inputs.

Step 6   Click **Save** to save the service instance.

What to do next

Repeat this procedure to create any other service instances.

Note	To edit an existing service instance, select the instance and update the information.
	Click ⬚ to delete an existing service instance.

Create Physical Service Instance

A service instance defines a service in terms of how it is to be deployed. It specifies the following for a service: type, HA settings, role (active or standby) and so on.

Step 1   Click **Configuration** at the top-right corner of the homepage.

Step 2   Choose **Service Catalog** > **Physical Service Instance**.

Step 3   Click **Add**.

Alternatively, click ⬚ to copy an existing service instance and edit and save it with a new name.

Step 4   Enter the requested information.

Field	Description
Name	Enter a name for the service instance.
Service	From the drop-down list, choose the service that you are creating the service instance for.
Physical Service Config	Enter the name of a physical service configuration to be used for this physical service instance.
	The Routed check-box is selected by default.
	Configuration Parameters: Click + next to the configuration parameters to enter the configuration parameters
	Name: Enter the name of the configuration parameter.
	Value: Enter the value for the configuraiton parameter.
	Day 1: Click + next to the Day1 option to add the day1 configuration file.

Step 5   (Optional) Click **Validate** to verify your inputs.

Step 6   Click **Save** to save the service instance.

What to do next

Repeat this procedure to create any other physical service instances.

Click **Back** to go back to the previous page.

Note   Click download icon to export the physical service instance and physical service config.

To edit an existing physical service instance, select the instance and update the information.

Click to delete an existing service instance.

Create Service Chain Instance

A service chain instance defines a service chain in terms of its service profiles and how they are deployed.

Step 1   Click **Configuration** at the top-right corner of the homepage.

Step 2   Choose **Service Catalog** > **Service Chain Instance**.

Step 3   Click **Add**.

Step 4   **Name:** Enter the name for the service chain instance.

Step 5   **Service Chain Name:** Select a service chain from the **Service Chain Name** drop-down list.

When you choose the service chain from the drop-down list, the services that are associated with it populate automatically. You can then choose a service instance for each of the services.

Step 6   **Catalog:** From the **Catalog** drop-down list, choose the catalog to associate with the service chain instance.

Step 7 (Optional) Click **Validate** to verify your inputs.

Step 8 Click **Save** to save the service chain instance.

What to do next

Repeat this procedure to create any other service chain instances.

Click **Back** to go back to the previous page.

Note Click download icon to export the service chain instance.

To edit an existing service chain instance, select the instance and update the information.

Click ⬚ to delete an existing service chain instance.

Add Your Organization

When you add an organization, you are required to specify a catalog. This ensures that all the service chain instances and server profiles that are contained in the catalog are available for your organization to use. On the Add Organization screen, you can also add tenants. Tenants are various departments within an organization, such as, HR, Finance, Workplace Resources, and so on. You can even associate different catalogs to different tenants within your organization. Organizations and tenants represent a downward hierarchy for your site.

Step 1 Click **Configuration** at the top-right corner of the homepage.

Step 2 Choose **Service Catalog** > **Organization**.

Step 3 Click **Add**.

Alternatively, click ⧉ to copy an existing organization, and edit and save it with a new name

Step 4 Provide the requested information.

a) **Name:** Enter a name for your organization.

b) **Catalog:** Choose a catalog from the drop-down list. NOTE: If there is no catalog in the drop-down list, you have crreate it. Refer the section *Create SAE Catalog* to create the catalog. The selected Catalog must be associated with all Server Profiles for all CSPs and PNFs in the setup.

Step 5   Provide the requested Tenant information. You must add at least one tenant to complete this procedure.

a) **Name:** Enter a name for the tenant.

b) **Catalog:** Choose a catalog from the drop-down list. NOTE: The selected catalog will be the catalog for the tenant you are creating now. A tenant can have its own tenant catalog which is selecting here. It also shares all service chain instances in its organization catalog with other tenants under the organization.

a) **Configuration Parameters:** Add additional configuration parameters.

(Optional) Click + to add more tenants.

Step 6   (Optional) Click **Validate** to verify your inputs.

Step 7   Click **Save** to save the organization and tenant information.

What to do next

Repeat this procedure to add more organizations or tenants, as required.

Click **Back** to go back to the previous page.

Note   Click an existing organization to view or edit its details.

Click the 🗑 on the organization to delete it.

Add Server Profile

You can create two types server profiles: CSP and Physical FTD (FTD) devices. Server profiles define a server in terms of its type (CSP of physical FTD) and the server's physical interfaces. Server profiles serve as a server definition templates that can be references at the time of creating your site infrastructure.

Step 1   Click **Configuration** at the top-right corner of the homepage. Choose **Service Catalog** > **Server Profile**.

Step 2   Click **Add**.

Alternatively, click on an existing server profile to copy and edit it, and save it with a new name.

Step 3   **Name:** Enter a name for the server profile.

Step 4   **VIM Type:** From the **Type** drop-down list, choose either CSP or PFTD. The options to be entered in the right panel of the screen differ based on your selection.

If you select CSP as the type, enter the following requested information.

- **Management Network:** Name of the management network interface
- **SRIOV Networks:** Name of the SRIOV network interface. Click + to add multiple SRIOV network interfaces.
- **VIRTIO Networks:** Name of the VIRTIO network interface. Click + to add multiple VIRTIO network interfaces.

If you select PFTD as the type, enter the following requested information.

- **Management Network:** Name of the management network interface
- **Data Networks:** Name of the data network interface. Click + to add multiple data network interfaces.

Step 5   (Optional) Click **Validate** to verify your inputs.

Step 6   Click **Save** to save the server profile.

What to do next

Repeat this procedure to create any other server profiles.

Click **Back** to go back to the previous page.

Note   Click an existing server profile to view or edit its details.
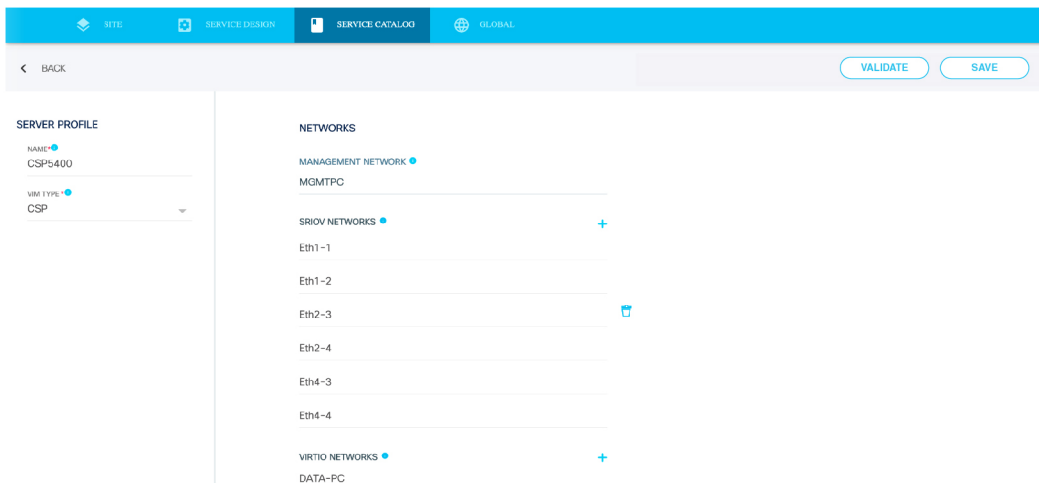
Click download icon to export the service chain instance.

Click ⬜ on a server profile to delete it.

Import and Export Service Catalog Components

This topic describes the following:

- How to export catalogs, virtual service instances, physical service instances, service chain instances, organization information and server profiles individually.

- How to import catalogs, virtual service instances, physical service instances, service chain instances, organization information and server profiles in bulk.

To be able to import files, the file should be in XML format. Similarly, the files are also exported in XML or JSON format.

Step 1   Click **Configuration** at the top-right corner of the homepage.

Step 2   Click the **Service Catalog** > **tab** .

Step 3   Depending on your requirement, click one of the tabs: **Catalog**, **Virtual Service Instance**, **Physical Service Instance**, **Service Chain Instance**, **Organization** or **Server Profile**.

Table 8:

Action	Result
Click **Catalog**	Your catalogs are displayed in card view. **Import Catalogs in Bulk** - Click the **Import** button to import XML files containing configuration for single or multiple catalogs. **Export Individual Catalogs** - Click the ⬇ icon on the card of the catalog you want to export.

Action	Result
Click **Virtual Service Instance**	Your virtual service instances are displayed in card view. **Import Virtual Service Instances in Bulk** • Click the **Import** button to import XML files containing configuration for single or multiple virtual service instances. **Export Individual Virtual Service Instances** • Click the ⬇ icon on the card of the virtual service instance you want to export.
Click **Physical Service Instance**	Your physical service instance are displayed in card view. **Import Physical Service Instances in Bulk** • Click the **Import** button to import XML files containing configurations for single or multiple physical service instances. **Export Individual Physical Service Instances** • Click the ⬇ icon on the card of the physical service instance you want to export.
Click **Service Chain Instance**	Your existing service chain instances are displayed in card view. **Import Service Chain Instances in Bulk** • Click the **Import** button to import XML files containing configuration for single or multiple service chain instances. **Export Individual Service Chain Instances** • Click the ⬇ icon on the card of the service chain instance you want to export.
Click **Organization**	Your existing organizations are displayed in card view. **Import Organization Information in Bulk** • Click the **Import** button to import XML files containing configuration for single or multiple organization information. **Export Information about Individual Organizations** • Click the ⬇ icon on the card of the organization information you want to export.

Action	Result
Click **Server Profile**	Your existing server profiles are displayed in card view. **Import Server Profiles in Bulk** • Click the **Import** button to import XML files containing configuration for single or multiple server profiles. **Export Individual Server Profiles** • Click the ⬇ icon on the card of the server profile you want to export.

Create SAE Site and Deploy Services

An SAE site allows you to define your infrastructure and instantiate services on the infrastructure. Infrastructure definition allows you to group Nexus 9000 devices (that are in vpc pairs) and associated CSPs together as a cluster. An SAE site provides the most flexible way of defining and instantiating services on the infrastructure.

The Site area of the GUI displays the existing sites. Use this area to create new sites, add endpoints to a site, and deploy services on a site.

View Site Details

The Site area of the GUI displays a snapshot of each of your existing sites and the tenants associated with the sites. The site snapshot displays the name of the site and icons for Exporting Infrastructure, Site Inventory, Inventory Discovery, Edit, Delete and so on as shown below.

Figure 1: Site Details

1	Exporting Infrastructure Only	5	Delete Site
2	Edit/Add Provider Endpoints Site Inventory	6	Resource Zone
3	Site Inventory	7	Add Tenant
4	Discovery		

Step 1 Choose the site that you want to view the details for, click the ⬜ icon.

The devices, physical network functions and topology associated with the site display.

Step 2 Click **Inventory** to view the device inventory and status for the selected site.

The switches, servers and physical network functions that are associated with the site are displayed.

Click on the cluster or servers to minnimize the display.
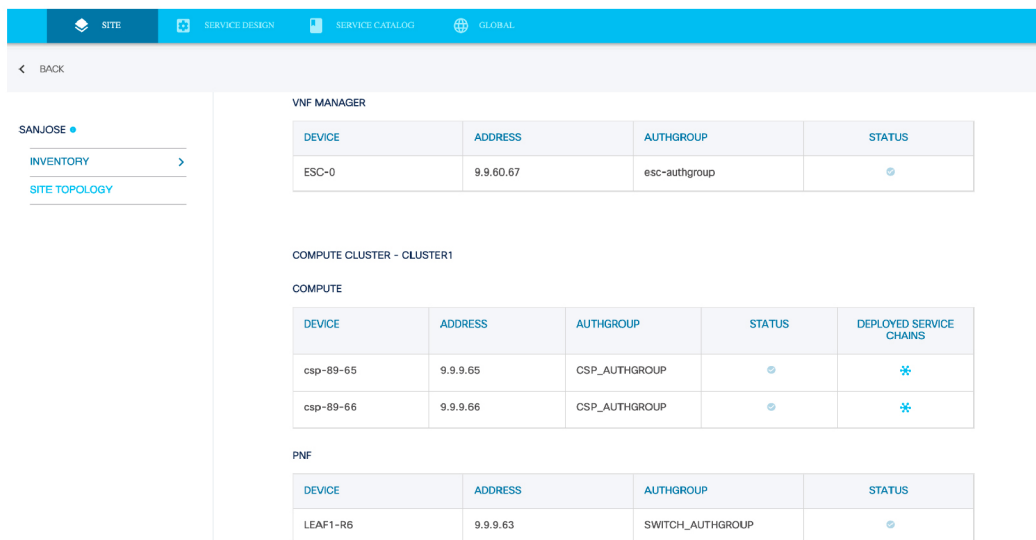
Step 3 Click **Site Topology** to view the site hierarchy and various physical network functions, devices and interfaces in the site along with the legends icons to differentiate between servers, switches and PNFs.

By default, expanded topology of site is displayed.

You can also minimize the clusters and components. To view the clusters within a site, click the representative site. To view the components of the cluster, click the clusters to expand them. Continue to click the various components that appear to view more details.
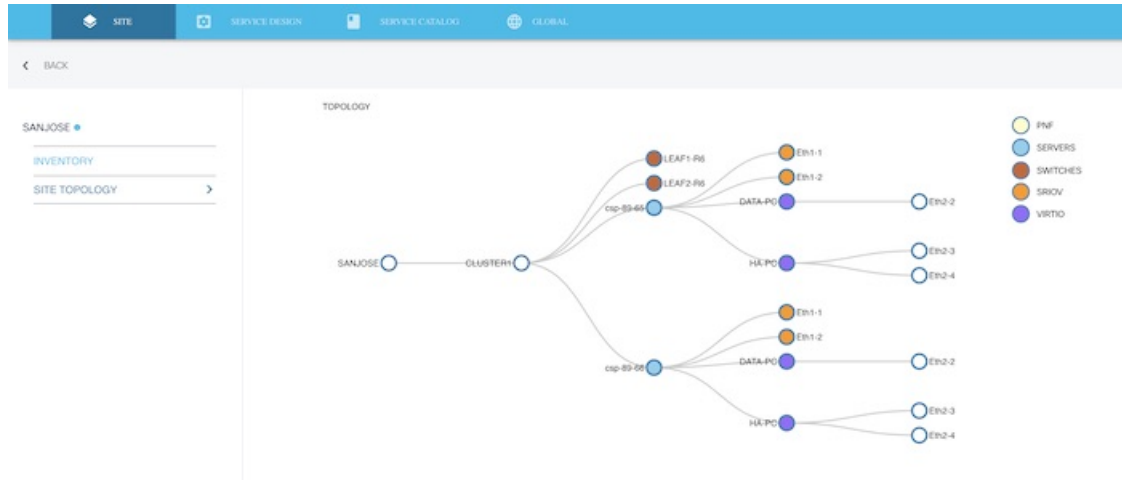
Create Site

Step 1   Click **Configuration** at the top right corner of the homepage.

Step 2   In the Site area, click **Add**.

Step 3   Provide the requested information.

Field	Description
Name	Enter a name for the site.
Organization	From the drop-down list, choose your organization.
AS pool	Select an AS pool from the drop-down menu for chosing BGPs AS numbers for creating chains on this site.
BGP ASN	Enter the BGP ASN.
ACI Controller (Optional Field)	If you select the ACI Fabric checkbox, the ACI Controller drop-down list displays. Choose the appropriate ACI Controller pool. **Note** The ACI Controller dropdown list will display the active and connected APIC devices in NSO.
Router ID Pool (Optional Field)	If you select the ACI Fabric checkbox, the Router ID Pool drop-down list displays which is tagged to ip pools. Choose the appropriate Router ID Pool pool.

Field	Description
Compute Clusters (Optional Field)	**Compute Clusters:** Click + next to the Compute Clusters field. Enter the name of the compute cluster and choose a pool from VLAN-Pool drop-down list.
	Leaf Switches: Choose the switches from the **Switch1** and **Switch2** drop-down menus. Click + next to Custom Template and select a custom template from the **Name** drop-down menu. The custom template pushes the day1 config to the service.
	Servers: Click + next to the Servers option. Select a server from the Name drop-down menu. Select a profile from the Server Profile drop-down menu.
	PNF Devices: Click + next to the PNF Devices option. Select physical device name from the Name drop-down menu. Note: The physical device name is populated according to the cluster.Enter the BGP AS number for this device.
Configuration Parameters (Optional Field)	Add the variables and values to set any additional configuration parameters.Enter the name and value for day0 configuration parameters. These values will be used as variables in day0 file before deploying the service.

Step 4 (Optional) Click **Validate** to verify your inputs.

Step 5 Click **Save** to save the site.

What to do next

Click **Back** to go back to the previous page.

Expand the **Select Site** dropdown and choose the site.

Enter name of the tenant in **Search Tenant** to search the tenant in the site.

Note   Click 🗑 on top right corner to delete an existing site.

Discover Site Inventory

When you have created an SAE site, you can use the Discovery option to discover the infrastructure for the site instead of adding it manually. To learn how to create a site, visit the Create Site section.

When you have configured your CSP devices and switches, the discovery option in the UI uses LLDP to discover all other devices.

Limitations

- The inventory discovery option does not support discovery of physical FTD devices.

Step 1   Click the **Discovery** icon next to the name of a site to discover inventory for the site.

1	Exporting Infrastructure Only	5	Delete Site
2	Edit/Add Provider Endpoints Site Inventory	6	Resource Zone
3	Site Inventory	7	Add Tenant
4	Discovery		

Step 2   Provide the requested information.

- **Start Device IP:** Enter the IP address of Nexus 9000 switch.

- **Switch Authgroup:** From the drop-down, choose the authgroup that contains the username and password for accessing the Nexus 9000 switches.

- **CSP Authgroup:** From the drop-down, choose the authgroup that contains the username and password for accessing the CSP devices.

- **ASR Authgroup:** From the drop-down, choose the authgroup that contains the username and password for the accessing the Cisco ASR devices.

- **VLAN Pool:** Select a VLAN pool from the drop-down list.

- **Server Type:** Select the server profile from the drop-down list. The server profile you choose in this drop-down here should be present in the catalog that is associated with the site.

- **Cluster Name:** Choose the resource cluster from the drop-down list. The list shows all the clusters configured under the Compute Cluster for this site.

Step 3   Click **OK**.

Your site inventory appears in the **Site Inventory** > **Inventory** page and in the following format.

Add Resource Zones to a Site

You can add, view, and delete resource zones for a particular site in the Site Area of the UI. Resource zones are always attached to sites.

CSP Resource Zones: CSP resource zones are used for CSP devices.

- When there are CSP devices attached to a site, a CSP zone is created by default. Such a default CSP zone includes all the CSP devices within a site.

  Note If you don't have any CSP devices associated with your site, the CSP resource zone will not be created by default.

- You can create additional resource zones and add one or more CSP devices from your site to the resource zones. However, to be able to create a resource zone, you must have at least one CSP device within your site.

Step 1 In the Site area, click **Resource Zone** next to the site for which you want to create resource zones.

Step 2 The Site field is populated automatically.

Step 3 To create a CSP Resource Zone, click + next to CSP Resource Zones option.

Note The + sign to add a resource zone is visible only if you have CSP devices or physical FTD devices within your site.

Step 4 Provide the requested information.

a) **Name:** Enter a name for the resource zone

b) **VCompute:** Select a device to be added to the resource zone from the drop-down menu.

Step 5 (Optional) Click **Validate** to verify your inputs.

Step 6 Click **Save** to save the resource zone.

What to do next

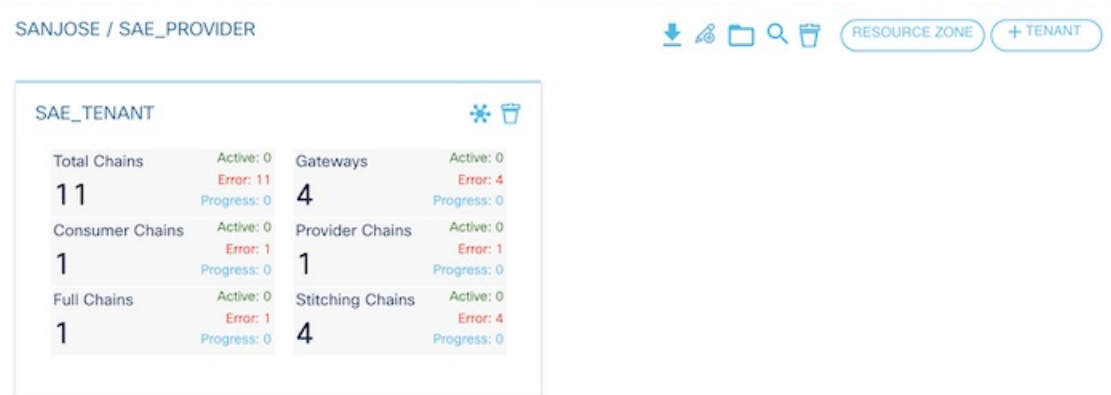Click **Back** to go back to the previous page.

Note Click ⬚ within the resource zone window to delete an existing resource zone.

Click ⬚ next to a device to remove the device from the resource zone.

Add Tenants to a Site

You can add, view, and delete tenants for a particular site in the Site Area of the UI. Any tenants under a site, they are displayed below the Site tile.

Step 1   In the Site area, click the + **Tenant** button next to the site to which you want to add a tenant.

Step 2   From the **Name** drop-down list, choose the tenant.

Step 3   From the **Data IP Pool** drop-down list, choose an IP pool to pick IP addresses for all data traffic from.

Step 4   Provide the requested information in the right panel of the screen .

Option	Description
Management	• **Management IP Pool:** From the drop-down list, choose an IP address pool to pick IP addresses for management connections. . • **VLAN:** Enter the VLAN ID for management network within the tenant. • **Netmask:** Enter a management network netmask. • **Gateway:** Enter a gateway IP address for network management.
Resource Zone	Click + next to the Resource zone option to add a resource zone. Select a resource zone from the drop-down list. Click the + sign again to add more resource zones.
Configuration Parameters	Add the variables and values to set any additional configuration parameters.

Step 5   (Optional) Click **Validate** to verify your inputs.

Step 6   Click **Save** to save the tenant.

What to do next

Click **Back** to go back to the previous page.

Note   Click on the tenant snapshot to delete the tenant. Click to edit an existing tenant.

About the Service Deployment Screen

The Site area displays all your existing sites and the tenants associated with them. Click the icon on the tenant for which you want to view or deploy services.

The page displays the site properties, the gateways, and service chains deployed for the site, and a graphical representation of the service chains deployed.
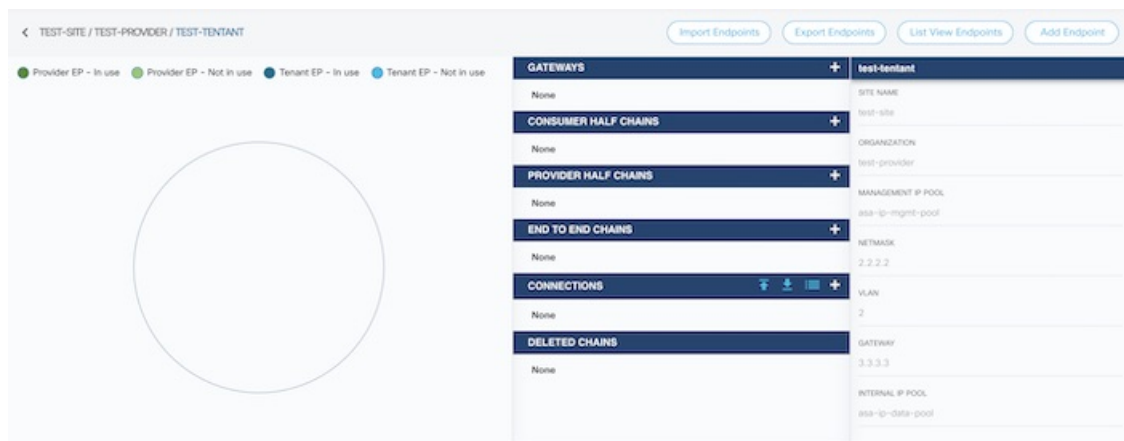
- The circular image on the left side of the screen represents the site. The endpoints that you add to the site appear along the circumference of the circle.

- The section in the middle shows the gateways, service chains and deleted chains that are deployed or removed on the site. If there is no data in this section, it means that there haven't been any deployments. You can add gateways and service chains by clicking the + icon in this section.

- The panel on the far right of the screen shows site properties.

Gateways

Gateway services are shared endpoint gateways that are connected to one or more external endpoints. Such gateways are attached to service chains, thus allowing multiple service chains to share an endpoint gateway.

Service Chains

The page includes separate headings for consumer half chains, provider half chains, connections, end-to-end chains and deleted chains.

Each of these sections lists the service chains deployed for the site. Each chain has setting icons for add/delete endpoints, sub-interface and tunnel, delete and download icon to delete and export the chain. Also it has either a checkmark or a warning sign next to it. The checkmark indicates that the service chain was successfully deployed. The warning sign indicates that the chain was not deployed due to errors.

Service Chain Status

The status of a service chain is displayed next to the name of the chain. A checkmark next to the chain, indicates that the chain was successfully deployed. Click any service chain to know about its components and their status. An image of the service chain is displayed at the bottom of the page. Any component marked in red indicates issues with the component.

Click individual components for more details about their status. A VNF profile pop-up screen displays the status of the component. The component is shown in red if there are issues to be addressed. Click on the **Service Chain Instance** or **Service Chain** link to redirect to those screen respectively.

Hover over the VNF component to view a snapshot of the error. Click the VNF component to view all the details of the PNF profile of the component.

PNF Profile

Click on the VNF component, a pop-up screen displays the details of the components.

Click on the **Virtual Chain Instance** or **Virtual Chain** link to redirect to those screen respectively.

Enable Monitor on ESC: On the header, click to Enable/Disable Monitor on ESC.

Recovery on Same or Different CSP: On the header, click setting icon, two options **Recover on Same CSP** and **Recover on Different CSP**are displayed. Click on the approproiate option.

A pop-up screen displays, enter the VNF undeploy wait time in seconds. The wait time should be in between 600 and 65535.

Note: When you choose to **Recovery on Same CSP** the CSP option in payload is changed from *realloc-on-same* to *recover-on-same*.

Site Properties

The section on the far right of the page displays site properties such as the organization associated with the site, management IP poolassociate with the site, and the netmask, VLAN, and gateway for VNF management and innnternal IP pool.

Add and Edit End Points

Add Provider-Level or Tenant-Level Endpoint

Endpoints connect your service chain to the external network.

Step 1   On the **Site** screen, click the **Add/Edit Provider Endpoint**.

Step 2   Click the ✳ icon on the Site page to add an endpoint to an existing site provider.

Step 3   Click **List View Endpoints** to view the list of existing endpoints.

Step 4   On the Provider screen, click **Add Endpoint**.

Step 5   Provide the requested information:

Field	Description
Name	Enter a name for the endpoint

Field	Description
Traffic Handoff Method	Indicate how traffic is delivered to SAE.
VLAN Number	Enter a VLAN number if you choose VLAN or VLAN over Port Channel in the previous field.
Endpoint ASN	Enter the BGP AS number of the endpoint.
Endpoint Remote ASN	Enter a BGP AS number of the servicechain end.
Endpoint IP Address	IP address of the endpoint
Endpoint Netmask	Netmark of the external end-point IP address
Subinterface ID	Subinterface ID
Subinterface Group	Check the checkbox to enter sub-interface group name and sub-interface ID. Note: The group name can be any string.
Name (Optional)	Enter the sub-interface group name. You can add more than one endpoints to the sub-interface group.
ID (Optional)	Enter the sub-interface ID.
Switch	The Nexus 9K switch through which the endpoint is connected to the SAE complex
Interface	The Nexus 9K interface through which the endpoint is connected to SAE complex

Step 6 (Optional) Click the + sign next to Additional Peers to add peers and enter the requested information:

Step 7 (Optional) Click **Validate** to verify your inputs.

Step 8 Click **Save** to deploy the endpoint on the site.

Step 9 Click **Cancel** to cancel the created provider endpoint on the site.

Step 10 When deployed, you can see the endpoint on the circumference of the circle on the left of the screen. The circle represents the site.
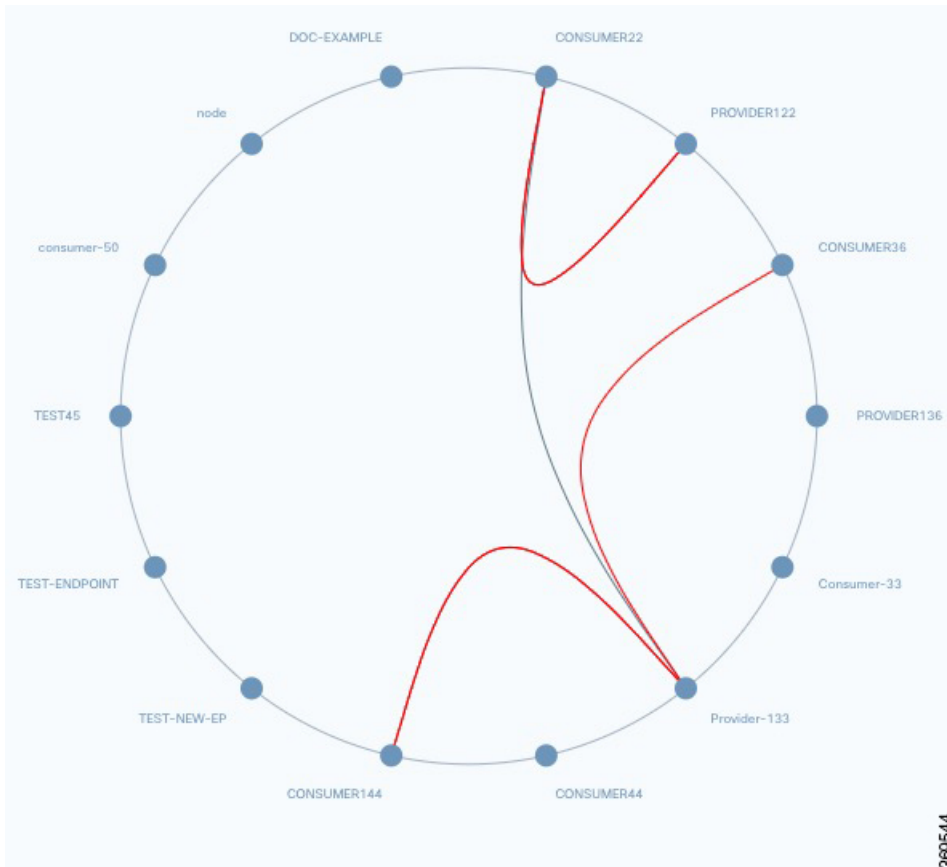
Note	• If two or more service chains share the same endpoints, the service chains are not represented by separate lines between the endpoints.
	• You cannot connect an endpoint to itself. In other words, the two ends of a service chain (consumer end and provider end) must have separate endpoints.

Add a Tenant Endpoint

Endpoints connect your service chain to the external network.

Note	When you click a site for which you want to add an endpoint, you enter the provider-level. From here, you can only add or edit provider-level endpoints. To add or edit tenant level endpoints, you must click a tenant and enter the tenant-level.

Step 1 On the **Site** screen, click on the service deployment icon on your desired site.

Step 2 Click **Import Endpoints** to import the existing endpoints in bulk.

Step 3   Click **Export Endpoints** to export the existing endpoints in bulk in JSON and XML format.

Step 4   Click **List View Endpoints** to view the list of existing endpoints.

Step 5   Click **Add Endpoint**.

**Step 6**   Provide the requested information:

Field	Description
Name	Enter a name for the endpoint
Traffic Handoff Method	Indicate hoe traffic is delivered to SAE. In the drop-down menu, you can choose from VLAN, VLAN over Port Channel, or VPN tunnel.
VLAN Number	Enter a VLAN number if you choose VLAN or VLAN over Port Channel in the previous field.
Endpoint ASN	Enter a local BGP AS number
Endpoint Remote ASN	Enter a remote BGP AS number
Endpoint IP Address	IP address of the endpoint
Endpoint Netmask	Netmark of the external end-point IP address
Subinterface ID	Subinterface ID
Subinterface Group	The group that the subinterface ID belongs to
Name (Optional)	Enter the sub-interface group name. You can add more than one endpoints to the sub-interface group.
ID (Optional)	Enter the sub-interface ID.
Switch	The Nexus 9K switch through which the endpoint is connected to the SAE complex
Interface	The Nexus 9K interface through which the endpoint is connected to SAE complex
Additional Peers	Click +next to Additional Peers and enter the endpoinnt IP address, endpoint ASN and endpoint remote ASN.

Step 7   (Optional) Click the + sign next to Additional Peers to add peers and enter the requested information:

Step 8   (Optional) Click **Validate** to verify your inputs.

Step 9   Click **Save**.

When deployed, you can see the endpoint on the circumference of the circle on the left of the screen. The circle represents the site.
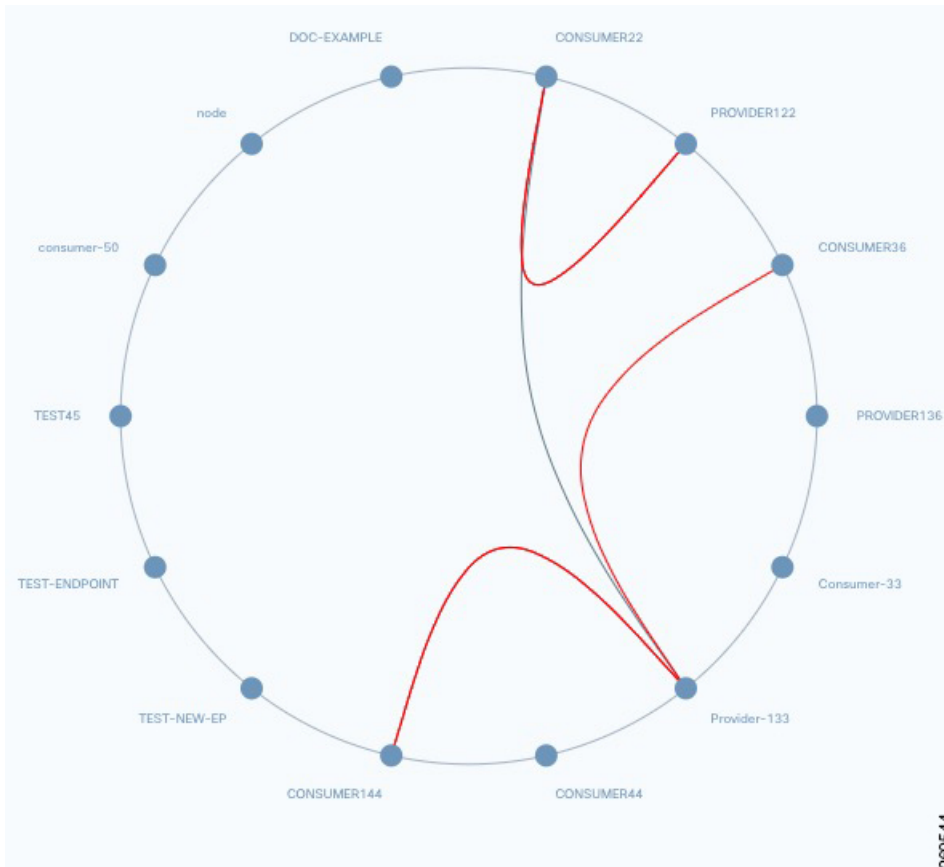
Note	• If two or more service chains share the same endpoints, the service chains are not represented by separate lines between the endpoints.
	• You cannot connect an endpoint to itself. In other words, the two ends of a service chain (consumer end and provider end) must have separate endpoints.

Delete an Endpoint

Step 1	Click ✳ on the site snapshot to open the Service Deployment view.
	A circular image representing a site and its endpoints in displayed on the left side of the screen.
Step 2	On the circle, double-click the endpoint that you want to delete.
Step 3	Next, press the **delete** button on your keyboard or click icon present next to **Edit Endpoint**.
	A pop-up is displayed to confirm whether you want to permanently delete the endpoint.
Step 4	Click **OK**.

Add, Edit, Delete Gateways and Chains

Add Gateway

Gateway services are shared endpoint gateways that are connected to one or more external endpoints.

Step 1   On the **Site** screen, click ✳ on the site snapshot to open the Service Deployment view.

Step 2   On the middle pane, click the + sign next to **Gateways** to add the gateway to a tenant.

Step 3   On the far right pane, **Add Gateway** opens.

Step 4   Click **Import** to import the existing gateways.

Step 5   Provide the requested information:

Field	Description
Site Name	Enter a name for the gateway.
Endpoint	Choose one or more endpoints from the drop-down list.
Service Chain Instance Name	Choose the service chain instannce name from the drop-down list.
MD5 Naming (Optional)	Check the MD5 naming checkbox, for the sevice. A unique md5 hash will be generated with the service path and vnf-profile and the length of the character will be 32.

Step 6   Click the **Next** button, Create Gateway pop-up opens.

Step 7   To connect the gateway to the components, drag one of the connector to the other component.

Step 8   Provide the requested information on the right panel for Connectivity.

Field	Description
IP	Enter the IP address for the connectivity.
Virtual IP	Choose the Virtual IP from the dropdown and enter the IP address for the it.
Next HOP Access Point	Enter the name and Subnet size for the next hop gateway to which packet will be forwarded.

Step 9   Click **Save** button to save the connectivity and move to the next screen.

Step 10   On the Configuration Parameter screen.

Step 11   Click + sign enter the **Name** and **Value** for the configuration parameter.

Step 12   Click **Next** button.

Step 13   On the **Additional Properties** screen.

Step 14   (Optional) Provide the requested information:

Field	Description
Bandwidth Requirement (Mbps)	Enter number in Mbps.
Resource Zone	Choose the resorce zone from the drop-down list.
Virtual Service Profile	By default the virtual service profile name is displayed.
Custom Name	Enter the custom name for the virtual service profile.

Step 15   Click **Next** button.

Step 16   On the **Template** screen.

Step 17   For the VNF profile, choose either **Custom Template** or **Switch Template**.

Step 18   (Optional) Click the + sign next to Cutom Template to add the custom template from the drop-down list.

Step 19   (Optional) Click **Validate** to verify your inputs.

Step 20   Click **Deploy** to deploy the endpoint on the site.

What to do next

Click ✳ setting icon, next to the existing gateway to **Add Endpoints** , **Delete Endpoints**, **Add sub-interface**, **Delete sub-interface** or **Add tunnel**.

Click 🗑 to delete an existing gateway.

Click ⬇ to export the individual gateway.

Add Consumer Half Chain

You can add, export and delete consumer half chain, add endpoints, delete endpoints, add sub-interface, delete sub-interface and add tunnel.

Step 1   On the **Site** screen, click ✳ on the site snapshot to open the Service Deployment view.

Step 2   On the middle pane, click the + sign next to **Consumer Half Chains** to add the consumer half chain.

Step 3   On the right panel, **Add Consumer Half Chains** screen opens

Step 4   Alternatively, click **Import** to import the existing consumer half chain.

Step 5   Provide the requested information:

Field	Description
Name	Enter a name for the chain.
(Optional) MD5 Naming	Check the MD5 naming checkbox, for the service. A unique md5 hash will be generated with the service path and vnf-profile and the length of the character will be 32.

Field	Description
(Optional) Endpoint	Choose one or more chain endpoints from the drop-down list.
(Optional) Gateway	Choose the chain gateway from the drop-down list.
Service Chain Instance Name	Choose the chain service chain instance name from the drop-down list.

Step 6 Click **Next** button, Create Half Chain pop-up screen opens.

Step 7 The graphical representation of the chain is visible on the middle panel, and on the far right panel, **PNF Profile Details** screen opens.

Step 8 Choose **PNF Device** from the dropdown list.

Step 9 Click **Next** button.

Step 10 (Optional) Click + sign next to the name-value pair and enter the **Name** and **Value** for the configuration parameter.

Step 11 Click **Next** button.

Step 12 On the **Additional Properties** screen.

Step 13 (Optional) Provide the requested information:

Field	Description
Bandwidth Requirement (Mbps)	Enter number in Mbps.
Resource Zone	Choose the resource zone from the drop-down list.

Step 14 Click **Next** button.

Step 15 On the **Templates** screen.

Step 16 For the PNF profile, choose either **Custom Template** or **Switch Template**. By default, **Custom Template** is selected.

Step 17 (Optional) Click the + sign next to Custom Template/Switch Template and choose the name value from the drop-down list.

Step 18 (Optional) Click **Validate** to verify your inputs.

Step 19 Click **Deploy** to deploy the consumer half chain on the site.

What to do next

Click ✳ next to the existing consumer half chain to **Add Endpoints**, **Delete Endpoints**, **Add sub-interface**, **Delete sub-interface** or **Add tunnels**.

Click 🗑 to delete an existing consumer half chain.

Click ⬇ to export the individual consumer half chain.

Click tenant link on top left corner to go back to the previous page.

Add Provider Half Chains

You can add, export and delete provider half chain, add endpoints, delete endpoints, add sub-interface, delete sub-interface and add tunnel.

Step 1   On the **Site** screen, click ✳ on the site snapshot to open the Service Deployment view.

Step 2   On the middle pane, click the + sign next to **Provider Half Chains** to add the provider half chain.

Step 3   On the right panel, **Add Provider Half Chains** screen opens.

Step 4   Alternatively, click **Import** to import the existing provider half chain.

Step 5   Provide the requested information:

Field	Description
Name	Enter a name for the chain.
(Optional) MD5 Naming	Check the MD5 naming checkbox, for the sevice. A unique md5 hash will be generated with the service path and vnf-profile and the length of the character will be 32.
Service Chain Instance Name	Choose service chain instance name for the chain from the drop-down list.
(Optional) Gateway	Choose the chain gateway from the drop-down list.
(Optional) Endpoint	Choose one or more chain endpoints from the drop-down list.

Step 6   Click **Next** button, Create Half Chain pop-up screen opens.

Step 7   The graphical representation of the chain is visible on the middle panel, and on the far right panel, **PNF Profile Details** screen opens.

Step 8   Choose **PNF Device** from the dropdown list.

Step 9   Click **Next** button.

Step 10   (Optional) Click + sign next to the name-value pair and enter the **Name** and **Value** for the configuration parameter.

Step 11   Click **Next** button.

Step 12   On the **Additional Properties** screen.

Step 13   (Optional) Provide the requested information:

Field	Description
Bandwidth Requirement (Mbps)	Enter number in Mbps.
Resource Zone	Choose the resource zone from the drop-down list.

Step 14   Click **Next** button.

Step 15   On the **Templates** screen.

Step 16   For the PNF profile, choose either **Custom Template** or **Switch Template**. By default **Custom Template** is selected.

Step 17   (Optional) Click the + sign next to Custom Template/Switch Template and choose the name value from the drop-down list.

Step 18   (Optional) Click **Validate** to verify your inputs.

Step 19   Click **Deploy** to deploy the consumer half chain on the site.

What to do next

Click ✱ next to the existing provider half chain to **Add Endpoints** ,**Delete Endpoints**, **Add sub-interface**, **Delete subb-interface** or **Add tunnels**.

Click 🗑 to delete an existing provider half chain.

Click ⬇ to export the individual provider half chain.

Click tenant link on top left corner to go back to the previous page.

Add End to End Chains

Gateway services are shared endpoint gateways that are connected to one or more external endpoints.

Step 1   On the **Site** screen, click ✱ on the site snapshot to open the Service Deployment view.

Step 2   On the middle pane, click the + sign next to **Gateways** to add the gateway to a tenant.

Step 3   On the far right pane, **Add Gateway** opens.

Step 4   Click **Import** to import the existing gateways.

Step 5   Provide the requested information:

Field	Description
Name	Enter a name for the chain.
(Optional) MD5 Naming	Check the MD5 naming checkbox, for the sevice. A unique md5 hash will be generated with the service path and vnf-profile and the length of the character will be 32.
(Optional) Endpoint	Choose one or more chain endpoints from the drop-down list.
(Optional) Gateway	Choose the chain gateway from the drop-down list.
Service Chain Instance Name	Choose the chain service chain instance name from the drop-down list.
(Optional) Gateway	Choose the chain gateway from the drop-down list.
(Optional) Endpoint	Choose one or more chain endpoints from the drop-down list.

Step 6   Click the **Next** button, Create Full Chain pop-up opens.

Step 7   The graphical representation of the chain is visible on the middle panel, and on the far right panel, **Configuration Parameter** screen opens.

Step 8   (Optional) Click + sign next to the name-value pair and enter the **Name** and **Value**for the configuration parameter.

Step 9   Click **Next** button.

Step 10   On the **Additional Properties** screen.

Step 11   (Optional) Provide the requested information:

Field	Description
Bandwidth Requirement (Mbps)	Enter number in Mbps.
Resource Zone	Choose the resource zone from the drop-down list.

Step 12   Click **Next** button.

Step 13   On the **Templates** screen.

Step 14   For the VNF profile, choose either **Custom Template** or **Switch Template**. By default **Custom Template** is selected.

Step 15   (Optional) Click the + sign next to Custom Template/Switch Template and choose the name value from the drop-down list.

Step 16   (Optional) Click **Validate** to verify your inputs.

Step 17   Click **Deploy** to deploy the consumer half chain on the site.

What to do next

Click ✳ next to the existing consumer half chain to **Add Endpoints** ,**Delete Endpoints**, **Add sub-interface**, **Delete subb-interface** or **Add tunnels**.

Click 🗑 to delete an existing consumer half chain.

Click ⬇ to export the individual consumer half chain.

Click tenant link on top left corner to go back to the previous page.

Add Connections

Gateway services are shared endpoint gateways that are connected to one or more external endpoints.

Step 1   On the **Site** screen, click ✳ on the site snapshot to open the Service Deployment view.

Step 2   On the middle pane, click the + sign next to **Gateways** to add the gateway to a tenant.

Step 3   On the far right pane, **Add Gateway** opens.

Step 4   Click **Import** to import the existing gateways.

Step 5   Provide the requested information:

Field	Description
Site Name	Enter a name for the gateway.
Endpoint	Choose one or more endpoints from the drop-down list.
Service Chain Instance Name	Choose the service chain instance name from the drop-down list.
MD5 Naming (Optional)	Check the MD5 naming checkbox, for the service. A unique md5 hash will be generated with the service path and vnf-profile and the length of the character will be 32.

Step 6   Click the **Next** button, Create Gateway pop-up opens.

Step 7   To connect the gateway to the components, drag one of the connector to the other component.

Step 8   Provide the requested information on the right panel for Connectivity:

Field	Description
IP	Enter the IP address for the connectivity.
Virtual IP	Choose the Virtual IP from the dropdown and enter the IP address for it.
Next HOP Access Point	Enter the name and subnet size for the next hop gateway to which packet will be forwarded.

Step 9   Click **Save** button to save the connectivity and move to the next screen.

Step 10   On the Configuration Parameter screen.

Step 11   Click + sign, enter the **Name** and **Value**for the configuration parameter.

Step 12   Click **Next** button.

Step 13   On the **Additional Properties** screen.

Step 14   (Optional) Provide the requested information:

Field	Description
Bandwidth Requirement (Mbps)	Enter number in Mbps.
Resource Zone	Choose the resource zone from the dropdown list.
Virtual Service Profile	By default the virtual service profile name is displayed.
Custom Name	Enter the custom name for the virtual service profile.

Step 15   Click **Next** button.

Step 16   On the **Template** screen.

Step 17   For the VNF profile, choose either **Custom Template** or **Switch Template**.

Step 18   (Optional) Click the + sign next to Cutom Template to add the custom template from the dropdown list.

Step 19   (Optional) Click **Validate** to verify your inputs.

Step 20   Click **Deploy** to deploy the endpoint on the site.

Deploy Services

The Site area displays all the sites on which you can deploy services. If no sites are displayed, see the Create Site topic to learn how to create a new site.

Step 1   To deploy a service for a tenant displayed on the Site area, click the Service Deployment icon on the tenant.

A list of all the gateways and service chains that are already deployed for the tenant are displayed along with their statuses.

Step 2   Depending on the type of service chain (consumer half chain, provider half chain, end-to-end chains, gateway and so on) you want to deploy, click + next to respective section and provide the requested information in the menu that appears on the right of the screen.

a)   **Name:** Enter a name for the service chain.

b)   **Service Chain Instance Name:** Choose a service chain instance from the drop-down list.

c)   **Gateway:** This step is optional and only required if you are deploying two half chains by stitching them together into a single one. From the drop-down list, choose a gateway to connect the consumer side of the service chain to the provider side. The drop-down list shows all the gateways that are created for a particular site.

d)   **Endpoint:** From the drop-down list, choose an endpoint. For end-to-end chains, you need to provide both consumer-side and a provider-side endpoints.

Alternatively, click **Import** at the top of the menu on the right and import consumer half chains, provider half chains, end-to-end chains, or gateways as applicable.

Step 3   Click **Next**.

Based on the endpoint services and service chain configuration you select, a graphical representation of the service chain is displayed.

Step 4   Provide the requested information under the Connectivity menu on the right and click **Next**.

Step 5   Add Configuration Parameters as applicable and click **Next**.

Step 6   In the Additional Properties menu, enter the requested details.

a)   **Bandwidth Requirements:** Specify bandwidth requirements in Mbps.

b)   **Resource Zone:** Select a resource zone from the drop-down list.

c)   **Virtual Service Profile / Physical Service Profile:** This is autopopulated based on your previous selections.

d)   **Custom Template:** From the drop-down list, select a custom template to apply. The drop-down list shows templates that you upload to NSO.

Step 7   Next, click **Next** at the bottom of the Connectivity menu to advance to the next menu and click < to go back to the previous menu. You can add variables and additional properties for the services and the service chain on these menus.

Step 8   (Optional) Click **Validate** to verify your inputs.

Step 9   Click **Deploy** to deploy the service chain.

If the service chain is deployed successfully, a checkmark displays next to the chain. If the deployment fails, a warning sign displays next to the chain.

CHAPTER 6

Monitoring and Operations

This chapter includes information about monitoring and operations devices that are part of the Cisco SAE solution.

View NSO Device Notifications

The notification screen displays the NSO notifications for devices and Service State Changes.

Table 9: Feature Hstory

Feature Name	Release Information	Description
View NSO Notifications	Cisco SAE GUI Release 2.2.0	This feature enables you to view notifications about devices and service state changes. The notifications you see are extracted from NSO.

Step 1 Click **Monitoring & Operations** at the top-right corner of the homepage. The page displays a list of device notifications by default for a preselected period.

Click **Notifications** > **Device Notifications** to view a list of notification for the devices.

Step 2 (Optional) To filter the notifications for a specific date range, click the calendar next to the Start Date and End Date to modify dates and click **Filter**.

Click the **Export** button to export in bulk either in JSON or XML format.

Step 3 (Optional) To select the columns, click the **Select Columns** dropdown list and select the appropriate checkbox.

(Optional) To filter a specific row, click the checkbox next to **Filter Rows** and in the table list view enter the value in the appropriate column to filter the rows.

View Service State Changes Notifications

The Service State Changes notifiation screen displays the information about the Provider and Tenant level services for component, state, operation and status.

Table 10: Feature History

Feature Name	Release Information	Description
View Service State Change notifications	Cisco SAE GUI Release 2.2.0	This feature enables you to view notifications about a service state change. The notifications you see are extracted from NSO.

Step 1 Click **Monitoring & Operations** at the top-right corner and click **Notificatios**>**Service State Changes**. The page displays a list of service state changes notifications by default for a preselected period.

Step 2 (Optional) To filter the notifications for a specific date range, click the calendar next to the Start Date and End Date to modify dates and click **Filter**.

Click the **Export** button to export in bulk either in JSON or XML format.

Step 3 (Optional) To select the columns, click the **Select Columns** drop-down list and select the appropriate checkbox.

(Optional) To filter a specific row, click the checkbox next to **Filter Rows** and in the table list view enter the value in the appropriate column to filter the rows.

View NSO Information

The NSO Info screen displays the HA info, NSO version, license summary and various packages with their versions and status. The informations displayed on the screen is static.

Step 1   Click your **Username** at the top-right corner of the homepage.

Step 2   Choose **NSO Info**. A pop-up screen for NSO information opens with HA info, license summary and packages tab.

Step 3   **HA Info:** By default the **HA Info** tab opens. It contains informations about the **NSO IP**, **NSO Version** and **HA Info**.

Step 4   **License Summary:** This tab consists of the license summary of the NSO.

Step 5   **Packages:** This tab contains the information about the various packages used **Name**, their version **Package Version** and status **UP** (UP or Down). The green checkmark indicates the UP status.

(Optional) To select the columns, click the **Select Columns** drop-down list and select the appropriate checkbox.

(Optional) To filter a specific row, click the checkbox next to **Filter Rows** and in the table list view enter the value in the appropriate column to filter the rows.