

Day One+

Contrail Service Orchestration (On-Premises Version)

IN THIS GUIDE

- [Step 1: Begin | 1](#)
- [Step 2: Up and Running | 7](#)
- [Step 3: Keep Going | 30](#)

Step 1: Begin

IN THIS SECTION

- [Meet Contrail Service Orchestration | 1](#)
- [Role-Based Access Control | 2](#)
- [SD-WAN Service | 3](#)
- [NGFW Service \(Security Services\) | 4](#)
- [Before You Begin | 5](#)
- [Log In to CSO | 5](#)
- [CSO Home Page | 5](#)

Meet Contrail Service Orchestration

Contrail Service Orchestration (CSO) is a comprehensive software platform that simplifies the deployment of software-defined WAN (SD-WAN) and next-generation firewall (NGFW) services, also called Security Services. You access CSO

through a graphical user interface (GUI). Its built-in automation capabilities make it easy to provision, manage, and monitor your WAN, campus, and branch networks.

You can subscribe to our cloud-delivered CSO software-as-a-service (SaaS) or deploy CSO as an on-premises software on your own hardware infrastructure.

This Day One+ guide walks you through the essential steps for deploying the SD-WAN services and NGFW (Security Services) with CSO On-Premises version. The on-premises version of CSO enables you (the customer) to install CSO on your own hardware infrastructure. Therefore, you are responsible for the maintenance and administration of CSO and the underlying hardware infrastructure. Based on your role (Service Provider (SP) Administrator, Operating Company (OpCo) Administrator or Tenant Administrator), we'll show you how to use CSO's intuitive GUI to add tenants and assign CSO licenses, and deploy the SD-WAN and NGFW services.

To understand the terminology used in CSO, see [CSO Terminology](#).

Role-Based Access Control

CSO supports role-based access control (RBAC), which lets users have access rights only to the information they need to do their jobs and prevents them from accessing information that doesn't pertain to them.

CSO has the following types of role scopes:

- **Service Provider**—Applicable to CSO on-premises deployments, in which you (or your company) function as the Service Provider administrator. In CSO SaaS deployments, Juniper Networks acts as the service provider.
- **OpCo**—Short for "Operating Company", an OpCo is a service provider who has multiple large tenants. A single instance of CSO can have multiple OpCos, each with multiple tenants. Tenants managed by one OpCo are isolated from tenants of another OpCo.
- **Tenant**—A tenant is an enterprise customer with many branches (sites) who subscribes to the service provider's (Juniper Networks) or OpCo's offerings. Sites are provisioned within a tenant. One tenant cannot see the sites or assets of another.

Here's an overview of the predefined roles in CSO:

Role	Role Scope	Access Privilege
SP Admin	Service Provider	<p>Users with the SP Admin role have full access to the Administration Portal UI and API capabilities.</p> <p>They can add one or more users with SP Admin, SP Operator, and custom roles. They can onboard tenants, and invite the tenant administrators during the tenant onboarding process. They can also add tenant administrators or operators by switching the scope to a specific tenant.</p>

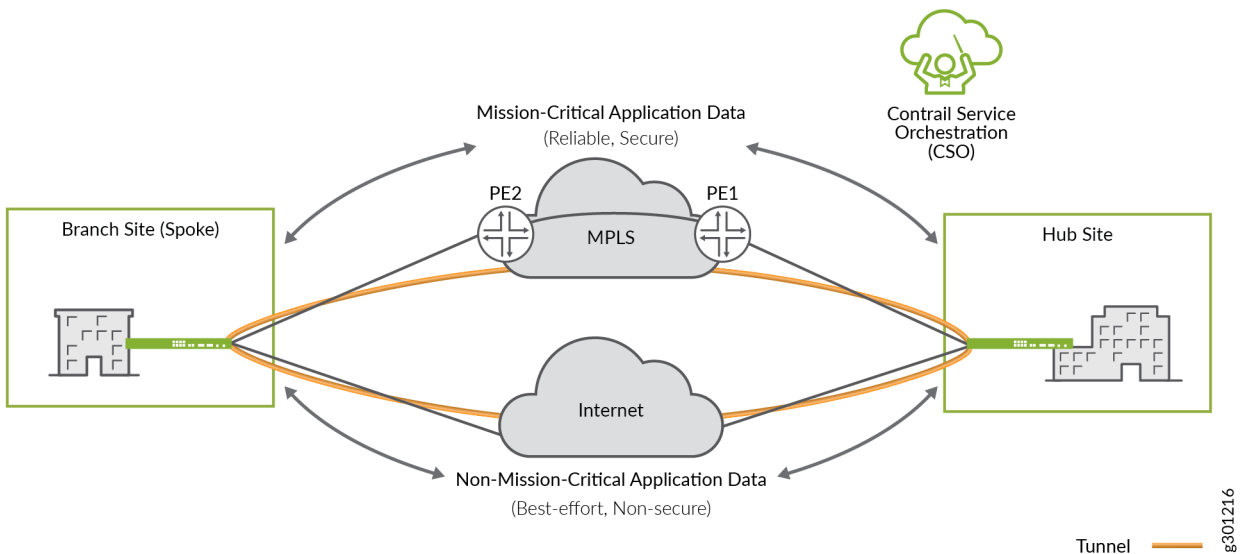
(Continued)

Role	Role Scope	Access Privilege
SP Operator	Service Provider	Users with the SP Operator role have read-only access to the Administration Portal and APIs.
OpCo Admin	Operating Company	Users with the OpCo Admin role have full access to the OpCo's Administration Portal. OpCo Admins can add users, onboard tenants, and much more. An OpCo Admin is the highest level of administrator available for CSO SaaS.
OpCo Operator	Operating Company	Users with the OpCo Operator role have read-only access to the OpCo's Administration Portal.
Tenant Admin	Tenant	Users with the Tenant Admin role have full access to the Customer Portal. They can add one or more users with the Tenant Administrator or Tenant Operator roles.
Tenant Operator	Tenant	Users with the Tenant Operator role have read-only access to the Customer Portal.

SD-WAN Service

If you deploy the SD-WAN service, CSO intelligently routes traffic through the optimal path based on the criteria you specify in CSO. For example, you can ensure that mission-critical application data is sent over the MPLS link (reliable and secure path) and the non-mission-critical application data is sent over the Internet link (best-effort, non-secure path). CSO also performs load balancing automatically and manages network congestion to route traffic efficiently.

Here's an illustration of a simple SD-WAN deployment:



This example shows how SD-WAN is applied using CSO in a topology that has one branch site and one hub site. CSO builds one tunnel for the WAN links going over the MPLS network and a second tunnel for the WAN links going over the Internet.

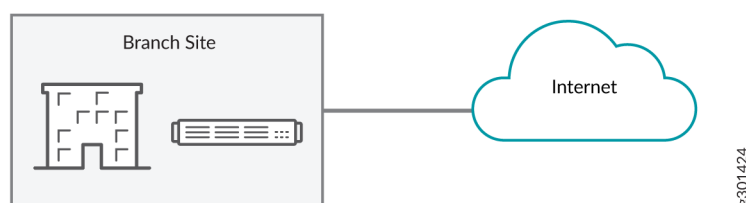
CSO supports the following SD-WAN services for a site:

- **Secure SD-WAN Essentials**—This service is ideal for small enterprises looking to manage simple WAN connectivity with comprehensive NGFW security services at the branch sites, using link-based application steering. The SD-WAN Essentials service allows Internet traffic to break out locally, thus avoiding the need to backhaul web traffic over VPN or MPLS links. You can create site-to-site VPN between branch sites (with or without hubs).
- **Secure SD-WAN Advanced**—Provides the complete SD-WAN service. This service is ideal for enterprises with one or more data centers, requiring flexible topologies and dynamic application steering. Site-to-site connectivity can be established by using a hub in a hub-and-spoke topology or through static or dynamic mesh VPN tunnels.

NGFW Service (Security Services)

If you deploy the NGFW service (Security Services) at a branch site, you can implement network security at this site using an SRX Series NGFW device as the CPE. You don't need to modify your existing network infrastructure to use the NGFW service. You only need to connect the SRX Series NGFW device to an OAM hub for monitoring and management.

Here's an illustration of a simple NGFW deployment:



Before You Begin

Before you begin, ensure that you've:

- Received the account activation e-mail (Subject line: CSO Account Created) that contains the CSO URL and login credentials.
- Activated your account by following the instructions specified in the account activation e-mail.
- Installed Google Chrome (version 60 or later) or Mozilla Firefox (version 78 or later) to access the CSO GUIs.

NOTE: If you're deploying CSO as an on-premises solution, you need to first install CSO. See the [Installation and Upgrade Guide](#) for the installation procedure.

Log In to CSO

1. Click the URL in the account activation e-mail to access CSO.

The CSO login page opens.

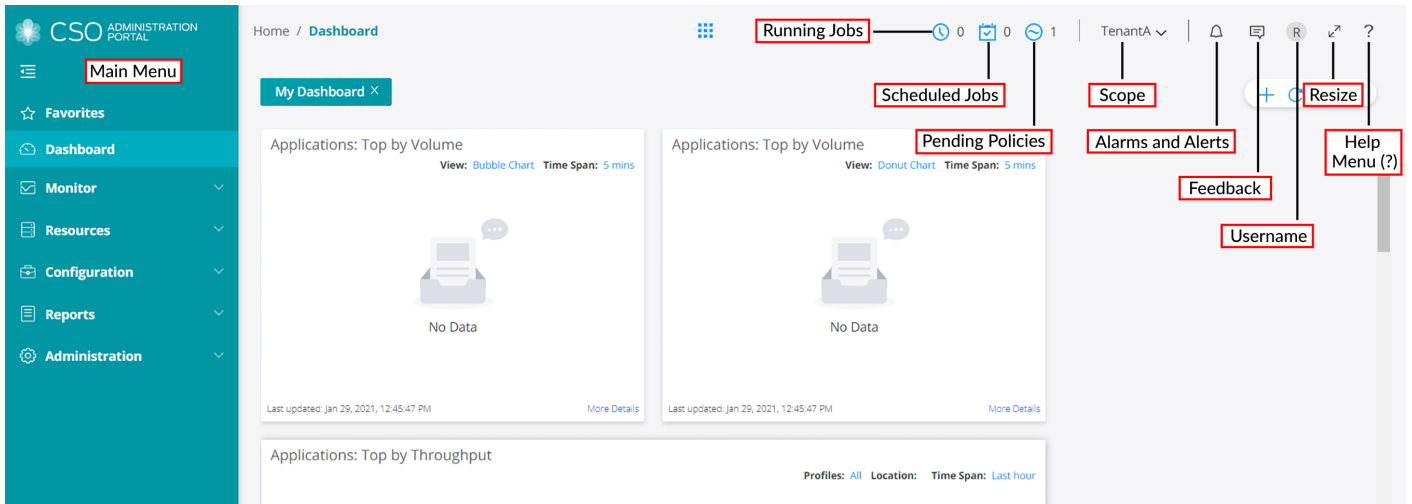
2. Log in with the username (the e-mail address to which the activation e-mail was sent) and the password that you set up. If two-factor authentication is enabled, you are prompted for a verification code.

If you're an SP or OpCo user, you're taken to the Administration Portal. If you're a tenant user, you're taken to the Customer Portal.

Once you're redirected to the portal, you'll see the Welcome screen. Click **Go to Dashboard** to view the CSO home page.

CSO Home Page

Here's an illustration that shows the GUI elements on the CSO home page:



Let's explore the GUI elements on the CSO home page.

GUI Element	Description
-------------	-------------

Left-nav Bar

Main Menu	Shows the main menu options available in the portals NOTE: There are different options for OpCo Administrators and Tenant Administrators.
-----------	---

Banner

Running Jobs	Shows the list of jobs that are currently in progress
Scheduled Jobs	Shows the list of jobs that are scheduled
Pending Policies	Shows the list of policies that are due for deployment on the devices managed by CSO NOTE: This icon is available only in the Customer Portal.
Scope	Displays the name of the OpCo or tenant. Click the down arrow to view the scope (OpCo scope or tenant scope) that you're currently in.

(Continued)

GUI Element	Description
Alarms and Alerts	Shows the following two tabs: <ul style="list-style-type: none"> Alarms—Shows the list of alarms that are generated by the device along with the timestamp and the severity of the alarms Alerts—Shows the list of alerts that are generated by the device along with the timestamp and the severity of the alerts
Feedback	Click this icon to provide feedback (through e-mail) about the product or report any issues that you're facing
Username	Hover over the icon to see the username of the user currently logged in to CSO
Resize	Click this icon to resize the page to full screen
Help Menu (?)	Click this icon to access the various embedded help panels and online help

Step 2: Up and Running

IN THIS SECTION

- [Prepare to Deploy SD-WAN or NGFW Services \(Service Provider Administrators\) | 8](#)
- [Deploy the SD-WAN Service \(Tenant Administrator\) | 14](#)
- [Deploy the NGFW or Security Services \(Tenant Administrator\) | 27](#)

Now that you've successfully logged in to CSO, let's use CSO's intuitive GUI to do the initial configuration.

TIP: When in doubt, hover over the ? (Help) icon displayed next to the page title or fields on the CSO GUI to know more about a page or a field on the page.

Prepare to Deploy SD-WAN or NGFW Services (Service Provider Administrators)

IN THIS SECTION

- [Configure SMTP Settings | 8](#)
- [Download the Signature Database | 8](#)
- [Upload a Device Image | 9](#)
- [Add a Point of Presence | 10](#)
- [Add an OAM Provider Hub Device | 10](#)
- [Add Tenants | 12](#)
- [Add CSO Licenses | 13](#)

Before a tenant administrator can deploy SD-WAN or NGFW (security services), a Service Provider (SP) administrator must configure SMTP settings; download the signature database; upload the device image; add points of presence, OAM provider hub devices, tenants, and CSO licenses.

Configure SMTP Settings

1. In the CSO Administration portal, click **Administration > SMTP**.

The SMTP page opens.

2. Configure the SMTP settings. Hover over the ? (Help) icon displayed next to the fields on the GUI to know more about a field.

NOTE: Fields marked with an asterisk (*) are mandatory.

3. Click **Save**.

The SMTP settings are saved and a confirmation message appears at the top of the page.

Download the Signature Database

1. Select **Administration > Signature Database**.

The Signature Database page opens.

2. Click **Signature Download Settings**.

The Signature Download Settings page opens.

3. Enter the download settings. Hover over the ? (Help) icon displayed next to the fields on the GUI to know more about a field.

4. Click **OK** to save the changes:

- If you specified that the signature database should be downloaded immediately, a Job Tasks page opens displaying information about the signature download job. Click **OK** to close this page and return to the Signature Database page.
- If you scheduled the signature download for later, a job is triggered and you are returned to the Signature Database page. A confirmation message (with the job ID) is displayed at the top of the page.

After the signature download operation is complete, predefined signatures (application and IPS) and IPS profiles are available in CSO. You cannot modify predefined signatures or IPS profiles. Users can create custom application signatures and IPS profiles as well.

Upload a Device Image

To upload a device image for the device:

1. Click **Resources > Images**.

The Images page opens.

2. Click the add icon (+).

The Upload Image page opens.

3. Complete the configuration settings according to these guidelines:

Field	Description
Name	<p>Enter the filename for the device image that you are uploading.</p> <p>Example: junos-srxsme-20.2R2-S3.5.tgz</p> <p>You must use the following filename format for device images of VNFs as listed below:</p> <ul style="list-style-type: none"> • vSRX—vsrx-vmdisk-15.1.qcow2 • NFX—juniper_nfx_1.5_img.tgz
Image Type	<p>Choose the type of device image.</p> <ul style="list-style-type: none"> • Device Image—Software image for the physical device (CPE). • VNF Image—Software image for the virtual device (VNF).
Vendor	<p>Choose the name of the device vendor.</p> <p>Example: Juniper Networks.</p>
Family	<p>Choose the device family.</p> <p>Example: NFX</p>

(Continued)

Field	Description
Supported Platform	Type the name of the platform supported by the device image. Example: NFX250
Build Number	Enter the build number of the device image. Example: X53-D102.2

4. Click **Upload**. If you want to discard the upload device image process, click **Abort** instead.

The Upload Image page displays the progress of the image upload.

5. Click **OK** to save the changes.

The Images page opens.

Add a Point of Presence

NOTE: Applies only to SD-WAN services.

In CSO, a POP refers to a location where one or more provider hub devices are located. Therefore, you must add at least one POP that you can assign provider hub devices to.

1. In the CSO Administration portal, select **Resources > POPs**.

The POPs page opens, displaying a list of existing POPs.

2. Click the Add (+) icon.

The Add POP page opens.

3. Complete the configuration settings.

4. Click **OK**.

CSO triggers a job to add the site, and displays confirmation messages when the job is triggered and when the job is completed. You are then returned to the POPs page.

TIP: Refresh the page and verify that the POP is added.

Add an OAM Provider Hub Device

NOTE: Applies only to SD-WAN services.

Create an OAM provider hub and include the point of presence (POP), which you created in the previous step, in it.

NOTE:

- For SD-WAN Advanced, we recommend that you configure a minimum of two OAM-capable provider hubs to provide redundancy in the OAM network.
- Before you add the provider hub, check the cable connections, review the NAT and firewall ports and protocols, and check the Junos OS version of the enterprise hub device, as explained in [Supported Devices for SD-WAN](#), and [Ports and Protocols to Open](#).

To add a provider hub device:

1. Select **Resources > Provider Hub Devices**.

The Provider Hub Devices page opens.

2. Click the add (+) icon.

The Add Provider Hub page opens, displaying the General settings to be configured.

3. Configure the General and WAN settings according to these guidelines:

Field	Guideline
Site Capability	<p>Select one of the following capabilities for the provider hub device:</p> <ul style="list-style-type: none"> • OAM_ONLY—Transmits only OAM traffic. <p>NOTE: This option is available only for SP Administrators in the on-premises version of CSO.</p> <ul style="list-style-type: none"> • OAM_AND_DATA—Transmits both data traffic and OAM traffic.
POP	Select the POP which you created in the previous step.
[Device Template]	<p>Ensure that you select the correct device template for the provider hub device from the carousel. For example, for an SRX1500 device, you can select SRX as SD-WAN Hub (or a modified version of that template) as the device template.</p> <p>NOTE: Check that the interface names in the device template match the ones on the device that you're using.</p>
OAM Interface	<p>For provider hubs with OAM or OAM and data capabilities, select the interface on the provider hub device that you want to use to connect the provider hub device to CSO. This interface is used only for OAM connectivity.</p> <p>The interface names are the names configured in the device template.</p>

(Continued)

Field	Guideline
OAM VLAN	For provider hubs with OAM or OAM and data capabilities, enter an OAM VLAN ID for in-band management of the hub device. If you specify an OAM VLAN ID, then in-band OAM traffic reaches the device through the selected OAM interface.
OAM IP Prefix	For provider hubs with OAM or OAM and data capabilities, enter an IPv4 address prefix for the OAM interface in the provider hub device. The prefix must be unique across the entire management network.
OAM Gateway	For provider hubs with OAM or OAM and data capabilities, enter the IP address of the next-hop through which the connectivity from the provider hub device to CSO is established.
EBGP Peer-AS	For provider hubs with OAM or OAM and data capabilities, enter the autonomous system (AS) number of the external BGP (EBGP) peer. The AS number is unique to the service provider and is needed to establish the EBGP peering session.

- Review the configuration in the Summary tab, and modify the settings, if required.

NOTE: (Optional) If you want to download the configured settings as a JavaScript Object Notation (JSON) file, click the **Download as JSON** link at the bottom of the page.

- Click **OK**.

Add Tenants

- From the main menu, go to the Tenants page (**Tenants > Tenants View**) and click **+**.
The Add Tenant page opens.
- Complete the configuration settings according to the following guidelines. After you complete the configuration in each of the tabs, click **Next**.

Tab	Field	Action
General	Name	Enter a unique name for the tenant. You can use alphanumeric characters and underscore; the maximum length allowed is 32 characters.
General	First Name	Enter the first name of the tenant.
General	Last Name	Enter the last name of the tenant.

(Continued)

Tab	Field	Action
General	Username (E-mail)	Enter the e-mail address, which will be used as the tenant's username.
General	Roles	Select one or more of the available roles to assign to the tenant.
Deployment Info	Services for Tenant	Based on your tenant's requirements, select either or both of the following services for the tenant: <ul style="list-style-type: none"> • SD-WAN—To enable Tenant Administrators to deploy and manage sites that have up to four WAN links with intelligent, SLA-based traffic routing among the WAN links • Next Gen Firewall (Security Services)—To enable Tenant Administrators to deploy and manage NGFW (Security Services) sites
Deployment Info	Service Level	<p>NOTE: This field appears only if you selected SD-WAN in the Services for Tenant field.</p> <p>Choose an SD-WAN service type for the tenant.</p> <ul style="list-style-type: none"> • Essentials—Provides the basic SD-WAN service (called Secure SD-WAN Essentials). • Advanced—Provides the complete SD-WAN service (called Secure SD-WAN Advanced).

3. Click **Finish** to add the tenant.

An Add Tenant job is created. When the job completes, the tenant is listed on the Tenants page.

Your tenant will receive an account activation e-mail.

Add CSO Licenses

To maintain a record of CSO licenses purchased by tenants or operating companies (OpCos), users with the SP Administrator role (or users with the necessary access privileges) can add the CSO license for a tenant or an OpCo from the CSO Licenses page.

To add a CSO license:

1. In the Administration Portal, select **Administration > Licenses > CSO Licenses**.

The CSO Licenses page opens.

2. Click the add (+) icon.

The Add CSO License page opens.

3. Complete the configuration. Hover over the ? (Help) icon displayed next to the fields on the GUI to know more about a field.

Setting	Guideline
License SKUs	<p>Add one or more license SKUs:</p> <ol style="list-style-type: none"> Click the add (+) icon. A row appears inline in the License SKU List grid. In the License SKU field, enter the SKU name. The SKU format is as follows: <i>S-CSO-Release-Type-License-Type-Device-Class-License-Period</i>. In the Device Quantity field, enter the maximum number of on-premise spoke sites that a tenant is authorized to add. You must enter a non-zero number to proceed. Click ✓ (check mark) to save your changes. The license SKU is saved and displayed in the grid. <p>You can modify a license SKU by selecting the corresponding row and clicking the edit (pencil) icon.</p>

4. Click **OK**.

The CSO Licenses page opens. A job is triggered to add the license. After the job completes successfully, a confirmation message appears and the page refreshes to display the newly added license SKUs.

Deploy the SD-WAN Service (Tenant Administrator)

IN THIS SECTION

- [Add Provider Hub Sites | 16](#)
- [Add an Enterprise Hub Site | 17](#)
- [Add an SD-WAN Branch Site | 21](#)
- [Upload and Push the Device License | 25](#)
- [Install the Signature Database | 25](#)
- [Add and Deploy a Firewall Policy | 26](#)
- [Deploy SD-WAN Policy Intents | 27](#)

To deploy the SD-WAN Advanced service, you'll need to add an enterprise hub site or a provider hub site, and a branch site. These tasks are optional for the SD-WAN Essentials service.

NOTE: Starting in Release 6.0.0, CSO supports IPv6 in the underlay.

Before you begin:

- Ensure that the Encapsulating Security Payload (ESP) protocol traffic is allowed on the network.
- Ensure that Network Address Translation (NAT) and firewall ports are open on the network. Here are the ports that must be open for your CPE device:

Device Model	NAT/Firewall Ports	CPE WAN Link Ports (minimum one port; maximum four ports)
SRX4100 and SRX4200	50, 51, 53, 123, 443, 500 or 4500, 514 or 3514, 7804	xe-0/0/0 through xe-0/0/7
SRX4600	50, 51, 53, 123, 443, 500 or 4500, 514 or 3514, 7804	xe-1/1/0 through xe-1/1/7 et-1/0/0 through et-1/0/3
SRX300, SRX320, and vSRX	50, 51, 53, 123, 443, 500 or 4500, 514 or 3514, 7804	ge-0/0/0 through ge-0/0/7
SRX340 and SRX345	50, 51, 53, 123, 443, 500 or 4500, 514 or 3514, 7804	ge-0/0/0 through ge-0/0/15
SRX380	50, 51, 53, 123, 443, 500 or 4500, 514 or 3514, 7804	ge-0/0/0 ge-0/0/2 through ge-0/0/15 xe-0/0/16 through xe-0/0/19
SRX550M	50, 51, 53, 123, 443, 500 or 4500, 514 or 3514, 7804	ge-0/0/0 through ge-0/0/9
NFX250	50, 51, 443, 500 or 4500, 514 or 3514, 2216, 7804	ge-0/0/10, ge-0/0/11, xe-0/0/12, and xe-0/0/13
NFX150	50, 51, 443, 500 or 4500, 514 or 3514, 7804	heth0 through heth5

- For provider hubs, ensure that the following ports and protocols are open on the network:

Device Model	Ports and Protocols	Hardware Documentation Links
SRX1500	IP Protocol 50 IP Protocol 51 TCP and UDP Ports 53 (for DNS) UDP Port 123 (for NTP) TCP Port 443 UDP Port 500 UDP Port 4500	SRX1500 Chassis
SRX4100	IP Protocol 50	SRX4100 Chassis
SRX4200	IP Protocol 51	SRX4200 Chassis
SRX4600	TCP and UDP Ports 53 (for DNS) UDP Port 123 (for NTP) TCP Port 443 UDP Port 500 UDP Port 4500	SRX4600 Chassis
vSRX	IP Protocol 50 IP Protocol 51 TCP and UDP Ports 53 (for DNS) UDP Port 123 (for NTP) TCP Port 443 UDP Port 500 UDP Port 4500	vSRX Deployment Guides

Add Provider Hub Sites

To add one or more provider hub sites:

1. Select **Resources > Site Management**.
The Site Management page appears.
2. Click **Add** and select **Add Provider Hub**.

The Add Provider Hub for *Tenant-Name* page appears.

3. Complete the configuration settings according to these guidelines:

Field	Description
<i>Configuration</i>	
Service POP	Select the POP from which you want to specify the provider hub device.
Hub Device Name	<p>Select one or more provider hub devices from the list. (Provider hub devices with DATA_ONLY and OAM_AND_DATA capabilities are listed.)</p> <p>If you select two or more provider hubs, the CSO provisions the provider hub sites in the order in which you selected the provider hub devices.</p>

NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **OK**.

CSO triggers a job and displays a job link. The Site Management page opens. When the job is finished, the Site Status of the provider hub sites changes to Provisioned.

Add an Enterprise Hub Site

NOTE: If you intend to use an existing Juniper Networks provider hub site, adding an enterprise hub site is optional.

1. From the main menu, go to the Site Management page (**Resources > Site Management**), click **Add**, and select **Enterprise Hub**.

The Add Enterprise Hub page opens.

2. Complete the configuration settings according to these guidelines:

Tab	Field	Action
General	Site Name	<p>Give the enterprise hub site a unique name. You can use alphanumeric characters and hyphen (-); the maximum length allowed is 32 characters.</p> <p>Example: E-hub1</p>

(Continued)

Tab	Field	Action
General	Device Host Name	The device host name is auto-generated and uses the format <i>tenant-name.host-name</i> . You cannot change the tenant-name part in the device host name. Use alphanumeric characters and hyphen(-); the maximum length allowed is 32 characters.
General	Site Capabilities	<p>NOTE: Device Management, enabled by default, allows you to create a site with only device management capability (without any services) and add services later.</p> <p>To add an SD-WAN capability for this site, choose one of the following SD-WAN service types:</p> <ul style="list-style-type: none"> Secure SD-WAN Essentials—(Available for tenants with SD-WAN Essentials service level) Provides basic SD-WAN services. You can upgrade an SD-WAN Essentials site to an SD-WAN Advanced site by editing the site information. Secure SD-WAN Advanced—(Available for tenants with SD-WAN Advanced service level) Provides the complete SD-WAN services. You cannot downgrade an SD-WAN Advanced site to an SD-WAN Essentials site.
Device	Device Series	Select SRX .
Device	Device Template	<p>Select a device template for the SRX Series device.</p> <p>The SRX Series device template contains information for configuring the SRX Series device.</p> <p>For example, for an SRX4100 device, select SRX4x00 as SD-WAN CPE (or a modified version of that template) as the device template.</p>

(Continued)

Tab	Field	Action
Device	Use for Fullmesh	<p>Click the toggle button to enable the WAN link to be part of a full-mesh topology.</p> <p>You typically implement a full-mesh topology to connect remote offices within an organization. A full-mesh topology is not commonly used to connect separate organizations because it allows each site to communicate directly with other sites.</p> <p>Configure the two additional fields that appear:</p> <ul style="list-style-type: none"> • Mesh Overlay Link Type: Keep the default selection (GRE over IPsec) as the type of encapsulation to be used for the overlay tunnels in the full-mesh topology. • Mesh Tags: Select one or more mesh tags for the WAN link. <p>The tunnels between the enterprise hub site and the branch site are added based on matching mesh tags. So, if you want meshing to take place between a WAN link on the enterprise hub and a WAN link on the branch site, the mesh tags must be the same for both sites.</p>
Device	Enable Local Breakout	<p>Click the toggle button to enable local breakout on the WAN link. By default, local breakout is disabled.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • If you enable this option, the WAN link can be used for local breakout. • If you do not enable local breakout on at least one WAN link for a single CPE connection plan and at least two WAN links for a dual CPE connection plan, the local breakout is disabled for the site.
Device	Preferred Breakout Link	<p>Click the toggle button to enable the WAN link as the most preferred breakout link.</p> <p>If you disable this option, the breakout link is chosen using ECMP from the available breakout links.</p>

(Continued)

Tab	Field	Action
Device	Connects to Provider Hubs	<p>NOTE: The Connects to Provider Hubs field is available only if you have selected a provider hub.</p> <p>Click the toggle button to specify that the WAN link of the site connects to a provider hub.</p> <p>NOTE:</p> <ul style="list-style-type: none"> For sites with a single CPE, you must enable at least one WAN link to connect to the hub so that OAM traffic can be transmitted. For sites with a dual CPE, you must enable at least one WAN link per device to connect to the hub so that OAM traffic can be transmitted.
Device	Use for OAM Traffic	<p>If you've specified that the WAN link is connected to a hub, click the toggle button to enable sending the OAM traffic over the WAN link. Enable this field on at least two WAN links for redundancy.</p> <p>This WAN link is then used to establish the OAM tunnel.</p>
Device	Overlay Tunnel Type	<p>This field is displayed when the Connects to Provider Hubs field is enabled.</p> <p>Select the mesh overlay tunnel type (GRE and GRE_IPSEC) of the tunnel to the hub.</p> <p>MPLS links can have both GRE and GRE_IPSEC as the overlay link type whereas Internet links can have only GRE_IPSEC as the overlay link type.</p>
Device	Overlay Peer Interface	<p>This field is displayed when the Connects to Provider Hubs field is enabled.</p> <p>Select the interface name of the hub device to which the WAN link of the site is connected.</p>
Device	Link Priority	<p>Enter a value in the range 1-255. A lower value indicates a more preferred link. A value of 1 indicates highest priority and a value of 255 indicates lowest priority. If you do not enter a value, the link priority is considered as 255.</p>
Device	Add LAN Segment	<p>Add the LAN segment by specifying the Name, Department, Gateway Address/Mask, and CPE Ports.</p>

3. Click **Finish** to add the site.

If you selected a service while adding the device, the Site Status on the Site Management page changes to Provisioned. If you did not select a service, then the Site Status remains in the Managed state until you apply the service. You can edit the site and add the service. After you add the service, the Site Status changes to Provisioned.

NOTE: In Release 6.1.0, CSO moves a site to the PROVISIONED state when at least one of the WAN links obtains the IP address and is activated. You can activate the remaining DHCP WAN links later.

Some of the other site states are as follows:

- Created—Indicates that the site was added but not configured.
- Configured—Indicates that the site was configured but not activated.
- Maintenance—Indicates that the site upgrade is in progress; any deployments that might occur because of other jobs are skipped when the site status is under Maintenance.

Add an SD-WAN Branch Site

1. From the main menu, go to the Site Management page (**Resources > Site Management**), click **Add**, and select **Branch Site (Manual)**.

The Add Branch Site page opens.

2. Complete the configuration settings according to these guidelines:

Tab	Field	Action
General	Site Name	Enter a unique name for the site. You can use alphanumeric characters and hyphen (-); the maximum length allowed is 32 characters.
General	Device Host Name	The device host name is auto-generated and uses the format <i>tenant-name.host-name</i> . You cannot change the tenant-name part in the device host name. Use alphanumeric characters and hyphen(-); the maximum length allowed is 32 characters.

(Continued)

Tab	Field	Action
General	Site Capabilities	<p>NOTE: Device Management, enabled by default, allows you to create a site with only device management capability (without any services) and add services later.</p> <p>To add an SD-WAN capability for this site, choose one of the following SD-WAN service types:</p> <ul style="list-style-type: none"> Secure SD-WAN Essentials—(Available for tenants with SD-WAN Essentials service level) Provides basic SD-WAN services. You can upgrade an SD-WAN Essentials site to an SD-WAN Advanced site by editing the site information. The SD-WAN Essentials service provides a subset of the features provided by the SD-WAN Advanced service. As such, it does not support multihoming, dynamic mesh tunnels, cloud breakout profiles, SLA-based steering profiles, pool based source NAT rules, IPv6, MAP-E, or underlay BGP. Secure SD-WAN Advanced—(Available for tenants with SD-WAN Advanced service level) Provides the complete SD-WAN services. You cannot downgrade an SD-WAN Advanced site to an SD-WAN Essentials site.
Device	Device Series	Select the device family that your CPE device belongs to—SRX, NFX150, or NFX250.
Device	Device Template	<p>Select a device template for the CPE device.</p> <p>For example, for an SRX300 device, select SRX as SD-WAN CPE (or a modified version of that template) as the device template.</p>

(Continued)

Tab	Field	Action
Device	Use for Fullmesh	<p>Click the toggle button to enable the WAN link to be part of a full-mesh topology.</p> <p>You typically implement a full-mesh topology to connect remote offices within an organization. A full-mesh topology is not commonly used to connect separate organizations because it allows each site to communicate directly with other sites.</p> <p>NOTE: A site with a single-CPE device can have a maximum of three WAN links enabled for meshing. A site with dual-CPE devices can have a maximum of four WAN links enabled for meshing.</p> <p>Configure the two additional fields that appear:</p> <ul style="list-style-type: none"> Mesh Overlay Link Type: Keep the default selection (GRE over IPsec) as the type of encapsulation to be used for the overlay tunnels in the full-mesh topology. <p>NOTE: For links with public IP addresses, we recommend that you use GRE over IPsec as the mesh overlay link type.</p> <ul style="list-style-type: none"> Mesh Tags: Select a mesh tag for the WAN link. <p>NOTE: You can select only one mesh tag, so ensure that you select the correct mesh tag.</p> <p>The tunnels between the enterprise hub and the branch site or between two branch sites are added based on matching mesh tags.</p>
Device	Enable Local Breakout	<p>Click the toggle button to enable local breakout on the WAN link. By default, local breakout is disabled.</p> <p>NOTE:</p> <ul style="list-style-type: none"> If you enable this option, the WAN link can be used for local breakout. You must enable local breakout on at least one WAN link for a single CPE connection plan and at least two WAN links for a dual CPE connection plan. Otherwise, the local breakout is disabled for the site.
Device	Preferred Breakout Link	<p>Click the toggle button to enable the WAN link as the most preferred breakout link.</p> <p>If you disable this option, the breakout link is chosen using ECMP from the available breakout links.</p>

(Continued)

Tab	Field	Action
Device	Connects to Provider Hubs	<p>NOTE: The Connects to Provider Hubs field is available only if you have selected a provider hub.</p> <p>Click the toggle button to specify that the WAN link of the site connects to a provider hub.</p> <p>NOTE:</p> <ul style="list-style-type: none"> For sites with a single CPE, you must enable at least one WAN link to connect to the hub so that OAM traffic can be transmitted. For sites with a dual CPE, you must enable at least one WAN link per device to connect to the hub so that OAM traffic can be transmitted.
Device	Use for OAM Traffic	<p>If you have specified that the WAN link is connected to a hub, click the toggle button to enable sending the OAM traffic over the WAN link. Enable this field on at least two WAN links for redundancy.</p> <p>This WAN link is then used to establish the OAM tunnel.</p>
Device	Overlay Tunnel Type	<p>This field is displayed when the Connects to Provider Hubs field is enabled.</p> <p>Select the mesh overlay tunnel type (GRE and GRE_IPSEC) of the tunnel to the hub.</p> <p>MPLS links can have both GRE and GRE_IPSEC as the overlay link type whereas Internet links can have only GRE_IPSEC as the overlay link type.</p>
Device	Overlay Peer Interface	<p>This field is displayed when the Connects to Provider Hubs field is enabled.</p> <p>Select the interface name of the hub device to which the WAN link of the site is connected.</p>
Device	Link Priority	<p>Enter a value in the range 1-255. A lower value indicates a more preferred link. A value of 1 indicates highest priority and a value of 255 indicates lowest priority. If you do not enter a value, the link priority is considered as 255.</p>

3. Click **Finish** to add the site.

If you selected a service while adding the device, the Site Status on the Site Management page changes to Provisioned. If you did not select a service, then the Site Status remains in the Managed state until you apply the service. You can edit the site and add the service. After you add the service, the Site Status changes to Provisioned. To know about some of the other site states, see the step 3 in the Add an Enterprise Hub Site section.

NOTE: In Release 6.1.0, CSO moves a site to the PROVISIONED state when at least one of the WAN links obtains the IP address and is activated. You can activate the remaining DHCP WAN links later.

Upload and Push the Device License

1. From the main menu, go to the Device License Files page (**Administration > Licenses > Device Licenses**) and click **+**.
The Add License page opens.
2. Click **Browse** to select the license file, and click **Open**.
The License File field displays the license file that you selected.

NOTE: A license file can contain only one license key.

3. Click **OK**.
CSO parses the license file and verifies whether the license file format is valid. If the format is valid, CSO uploads the license file and you're redirected to the Device License Files page.
4. Select the license that you added. Click **Push License** and select **Push**.
The Push License page opens.
5. Select the device to which you want to push the license, and click **OK**.
CSO initiates a job to push the license to the device. When the job completes, the license is pushed to the device.

Install the Signature Database

The signature database contains intrusion detection prevention (IDP) and intrusion prevention system (IPS) signature definitions of predefined attack objects and groups. CSO uses IDP and IPS signatures to detect known attack patterns and protocol anomalies within the network traffic. You'll need to install the signature database on one or more of your network devices. Juniper Networks downloads this database to CSO.

Here's how to install the signature database:

1. From the main menu, go to the Signature Database page (**Administration > Signature Database**) and click **Install Signatures**.
The Install Signatures page opens displaying the signature database version and the devices that you can install the signature database on.
2. Select the check boxes corresponding to the devices that you want to install the signature database on. You can also search for, filter, or sort the devices displayed in the table.
3. For the **Type** field, select one of the following options:
 - **Run now**—To immediately trigger the signature database installation on the selected devices
 - **Schedule at a later time**—To install the signature database later and specify a date and the time you want to trigger the installation
4. Click **OK**.
The signature database is installed on your devices.

Add and Deploy a Firewall Policy

A firewall policy enforces rules for transit traffic, in terms of what traffic can pass through the firewall, and the actions that need to take place on traffic as it passes through the firewall. You can deploy a firewall policy to all sites or specific sites.

Here's how to add and deploy a firewall policy:

1. From the main menu, go to the Firewall Policy page (**Configuration > Firewall > Firewall Policy**), and click the firewall policy that you want to add the firewall policy intent to.

The *Firewall-Policy-Name* page opens.

2. Click **+** to add a firewall policy intent.

The options to add a firewall policy intent appear inline on the *Firewall-Policy-Name* page.

3. Complete the following configuration:

To	Do this
Select the source endpoints you want to apply the firewall policy intent to	Click the add icon (+) to select from the list of addresses, departments, sites, site groups, users, zones, or the Internet
Select the destination endpoints you want to apply the firewall policy intent to	Click the add icon (+) to select from the list of addresses, applications, application groups, departments, services, sites, site groups, zones, or the Internet
Choose whether you want to allow, deny, or reject traffic between the source and destination endpoints	Click the add icon (+) and select one of the following: Allow, Deny, or Reject
Add advanced security features	Click the add icon (+) to select from advanced security features such as unified threat management (UTM) Profiles and IPS Profiles

4. Click **Save** to save the changes to the firewall policy intent.
5. Select the firewall policy intent that you added, and click **Deploy**.

The Deploy page opens.

6. Choose whether you want to deploy the firewall policy intent at the current time (**Run Now**) or schedule the deployment for later (**Schedule at a Later Time**).

To schedule the deployment for later, enter the date (in MM/DD/YYYY format) and the time (in HH:MM:SS 24-hour or AM/PM format) that you want to trigger the deployment. Be sure to specify the time in the local time zone where you access the CSO GUI.

7. Click **Deploy**.

The firewall policy is deployed.

Deploy SD-WAN Policy Intents

NOTE: If your SD-WAN Essentials service deployment doesn't involve hubs, you need to:

- Create a Local Breakout (Underlay) profile. See [Adding Breakout Profiles](#).
- Create an SD-WAN policy intent specifying the source and application (Any), and the breakout profile. See [Creating SD-WAN Policy Intents](#).

SD-WAN policy intents optimize how the network uses WAN links and distributes traffic. CSO provides predefined SD-WAN policy intents for tenants.

Here's how to deploy an SD-WAN policy intent:

1. From the main menu, go to the SD-WAN Policy page (**Configuration > SD-WAN > SD-WAN Policy**), select the SD-WAN policy intent that you want to deploy, and click **Deploy**.

The Deploy page opens.

2. Choose whether you want to deploy the SD-WAN policy intent at the current time (**Run Now**) or schedule the deployment for later (**Schedule at a Later Time**).

To schedule the deployment for later, enter the date (in MM/DD/YYYY format) and the time (in HH:MM:SS 24-hour or AM/PM format) that you want to trigger the deployment. Be sure to specify the time in the local time zone where you access the CSO GUI.

3. Click **OK**.

The SD-WAN policy intent is deployed.

Deploy the NGFW or Security Services (Tenant Administrator)

IN THIS SECTION

- [Add an NGFW \(Security Services\) Site | 28](#)
- [Upload and Push the Device License | 29](#)
- [Install the Signature Database | 30](#)
- [Add and Deploy a Firewall Policy | 30](#)

Before you add an NGFW (Security Services) site:

- Ensure that the required ports are open on the network. Here are the ports that must be open for your NGFW device:

Device Model	NAT/Firewall
SRX3xx, SRX550M, SRX1500, SRX4100, and SRX4200	443, 500 or 4500, 514 or 3514, 6514, 7804, 8060 (needed if using PKI authentication to validate CRL)

NOTE: When you configure the SRX Series device, ensure that you configure either the first port (ge-0/0/0) or the last port (ge-0/0/7 or ge-0/0/15 based on the model) for Internet connectivity.

Add an NGFW (Security Services) Site

1. From the main menu, go to the Site Management page (**Resources > Site Management**), click **Add**, and select **Branch Site (Manual)**.

The Add Branch Site page opens.

2. Configure the settings. The following table lists the mandatory fields. You'll find more details [here](#).

After you complete the configuration in each of the tabs, click **Next**.

Tab	Field	Action
General	Site Name	Give the NGFW site a unique name. You can use alphanumeric characters and hyphen (-); the maximum length allowed is 32 characters. Example: Ngfw-1
General	Device Host Name	The device host name is auto-generated and uses the format <i>tenant-name.host-name</i> . You cannot change the tenant-name part in the device host name. Use alphanumeric characters and hyphen(-); the maximum length allowed is 32 characters.
General	Site Capabilities	Select Security Services . NOTE: You can choose to either onboard a device with security services (NGFW) configured on it or configure the service later.
Device	Device Template	Select the device template for your SRX Series device. For example, select SRX_Standalone_Pre_Staged_ZTP (or a modified version of that template) as the device template.

(Continued)

Tab	Field	Action
Device	In-band Management Port	Select the port that you want to configure as management interface and connect it to the management device. You can configure any of the ge-0/0/x ports, where x ranges from 0 to 14, as in-band management interfaces.
Device	Import Policy Configuration	<p>Click the toggle button to automatically import firewall and NAT policies from the NGFW device to CSO. To use this, you need to disable zero-touch provisioning (ZTP). CSO doesn't provision NGFW devices (that are already configured and operational) through ZTP. By default, the Import Policy Configuration option is disabled.</p> <p>If you don't see this toggle button, you can select the firewall policy and NAT policy that you want to deploy from the Firewall Policies drop-down list and the NAT Policies drop-down list respectively. Select None if you want to deploy the policies after you add the site.</p>

3. Click **OK** to add the NGFW site.

If you selected a service while adding the device, the Site Status on the Site Management page changes to Provisioned. If you did not select a service, then the Site Status remains in the Managed state until you apply the service. You can edit the site and add the service. After you add the service, the Site Status changes to Provisioned.

Upload and Push the Device License

- From the main menu, go to the Device License Files page (**Administration > Licenses > Device Licenses**) and click **+**. The Add License page opens.
- Click **Browse** to select the license file, and click **Open**. The License File field displays the license file that you selected.

NOTE: A license file can contain only one license key.

3. Click **OK**.

CSO parses the license file and verifies whether the license file format is valid. If the format is valid, CSO uploads the license file and the Device License Files page opens.

4. Select the license that you added and click **Push License > Push**.

The Push License page opens.

5. Select the device that you want to push the license to, and click **OK**.

CSO initiates a job to push the license to the device. When the job completes, the license is pushed to the device.

Install the Signature Database

The signature database contains intrusion detection prevention (IDP) and intrusion prevention system (IPS) signature definitions of predefined attack objects and groups. CSO uses IDP and IPS signatures to detect known attack patterns and protocol anomalies within the network traffic. You'll need to install the signature database on one or more of your network devices. Juniper Networks downloads this database to CSO.

See ["Install the Signature Database" on page 25](#).

Add and Deploy a Firewall Policy

A firewall policy enforces rules for transit traffic, in terms of what traffic can pass through the firewall, and the actions that need to take place on traffic as it passes through the firewall. You can deploy a firewall policy to all sites or specific sites.

See ["Add and Deploy a Firewall Policy" on page 26](#).

Step 3: Keep Going

IN THIS SECTION

- [What's Next? | 30](#)
- [Additional Resources | 31](#)

What's Next?

Now that you've done the initial configuration, here are some things you can do next:

If you want to view	Then visit	With the user role
Details of all jobs	Jobs page (Monitor > Jobs)	OpCo Administrator Tenant Administrator
Traffic logs from different sites	Traffic Logs page (Monitor > Traffic Logs)	Tenant Administrator
Alerts generated to identify issues in your network	Alerts page (Monitor > Alerts and Alarms)	OpCo Administrator Tenant Administrator

(Continued)

If you want to view	Then visit	With the user role
System-generated alarms to identify conditions that might prevent a device from operating normally	Alarms page (Monitor > Alerts and Alarms)	OpCo Administrator Tenant Administrator
A summary of all security events in your network	Security Events page (Monitor > Security Events > All Events)	Tenant Administrator
Information (such as sessions, bandwidth consumed, and risk levels) about the applications on your network	Application Visibility page (Monitor > Application Visibility)	Tenant Administrator

Additional Resources

Here are some additional resources that we've chosen for your specific needs:

If you want to	Then
Download, activate, and manage your software licenses to unlock additional features for CSO	See Activate CSO Licenses in the Licensing Guide
See all documentation available for CSO	Visit the Contrail Service Orchestration (CSO) Documentation page in the TechLibrary
Stay up to date with new and changed features, limitations, and known and resolved issues in CSO	See the CSO Release Notes for the latest release
Understand more about CSO SD-WAN	Watch the Contrail SD-WAN 15 Features in 15 Minutes Introduction
Reach out to us	Visit the Juniper Networks Support page

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. Copyright © 2022 Juniper Networks, Inc. All rights reserved. Rev. 01, July 2021.