JUNIPER NETWORKS | Engineering Simplicity

Day One+

Contrail Service Orchestration (SaaS)

IN THIS GUIDE

Step 1: Begin

IN THIS SECTION

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 SaaS. In the SaaS version of CSO, Juniper Networks handles the installation, upgrade, and maintenance, and administration of CSO. Based on your role (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.

> **NOTE:** This Day One+ guide assumes that Juniper Networks has activated your license and that you've activated your user account (OpCo Administrator or Tenant Administrator) on CSO SaaS. If you don't have an account, instructions are available here.

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 SaaS has two types of role scopes:

- 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:

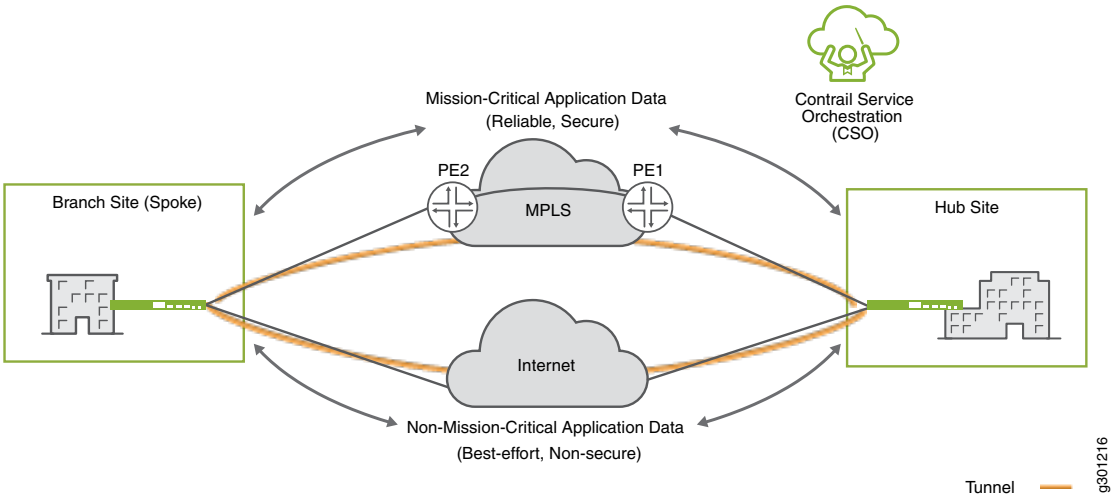
Role	Role Scope	Access Privilege
OpCo Admin	Operating Company	Users with the OpCo Admin role have full access to the OpCo's Administration Portal. OpCo Admins can add users, onboard tenants, and much more. An OpCo Admin is the highest level of administrator available for CSO SaaS.
OpCo Operator	Operating 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.

Role	Role Scope	Access Privilege
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.

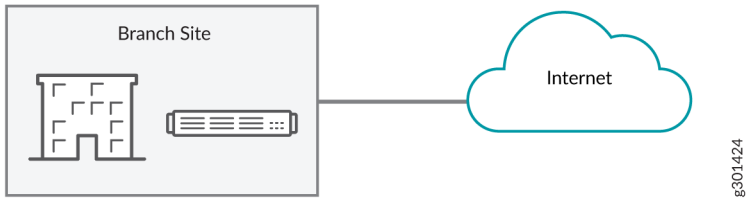
Starting in Release 6.0.0, CSO supports the following SD-WAN services for a site:

- 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). The SD-WAN Essentials service supports a subset of the features provided in Secure SD-WAN Advanced. 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—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.

Log In to CSO

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

   The CSO login page opens.

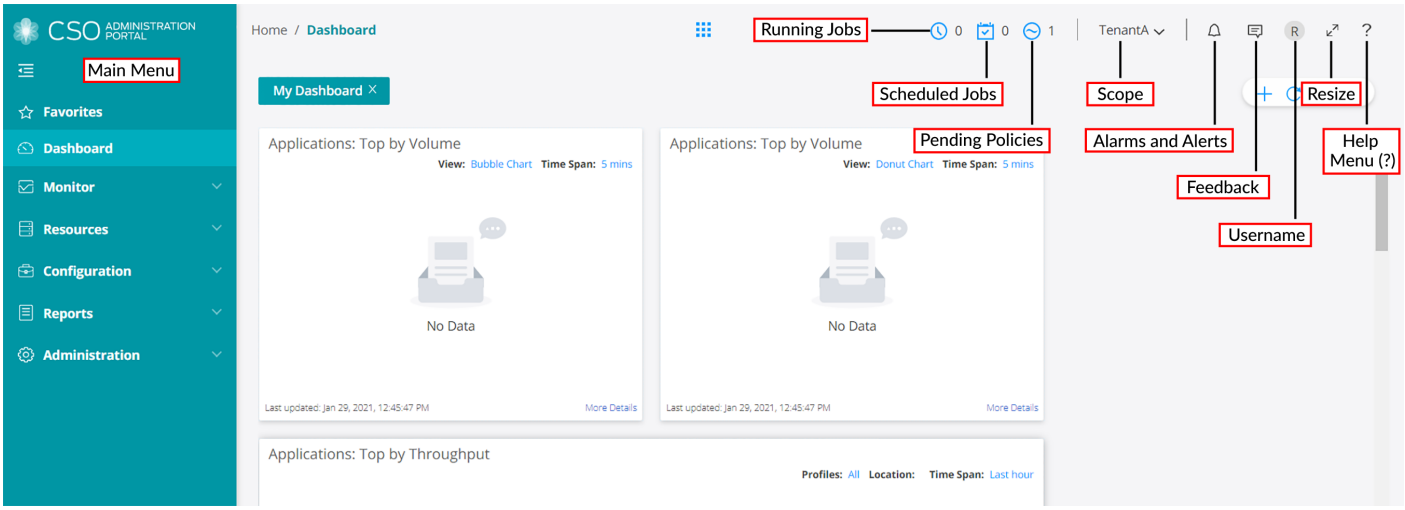
2. Log in with the username (the e-mail address to which the activation e-mail was sent) and the password that you set up.

   If you're an 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.

GUI Element	Description
Alarms and Alerts	Shows the following two tabs: • 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

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

- If you're an OpCo Administrator, add one or more tenants and assign CSO licenses to the tenants. See "Add Tenants (OpCo Administrator)" on page 7 and "Assign the CSO License to the Tenant (OpCo Administrator)" on page 8.
- If you're a Tenant Administrator, deploy the SD-WAN or NGFW service. See "Deploy the SD-WAN Service (Tenant Administrator)" on page 8 or "Deploy the NGFW or Security Services (Tenant Administrator)" on page 20.

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.

Add Tenants (OpCo Administrator)

Here's how to add a tenant:

1. From the main menu, go to the Tenants page (**Tenants > Tenants View**) and click **+**.

   The Add Tenant page opens.

2. Complete the configuration settings according to the following guidelines:

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.
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: • 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	**NOTE:** This field appears only if you selected SD-WAN in the Services for Tenant field. Choose an SD-WAN service type for the tenant. • 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.

Assign the CSO License to the Tenant (OpCo Administrator)

1. From the main menu, go to the CSO Licenses page (**Administration** > **Licenses** > **CSO Licenses**) and click the **Assign** link corresponding to the license that you want to assign.

   The Assign CSO License page opens.

2. For the Tenants List field, click **+**.

   A row is added in the grid.

3. In the Tenant column, select the tenant that you want to assign the license to. In the Device Quantity column, enter the quantity that you want to assign to the tenant.

   > **NOTE:** The sum of the assigned quantities must be less than or equal to the total quantity.

   Then, click **√** to save your changes.

4. Click **Assign**.

   A job is triggered to assign the licenses to the tenants. When the job completes, the CSO Licenses page displays the updated information in the Available and Assigned columns.

Deploy the SD-WAN Service (Tenant Administrator)

IN THIS SECTION

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
SRX4x00	50, 51, 53, 123, 443, 500 or 4500, 514 or 3514, 7804	**xe-0/0/0** through **xe-0/0/3**
SRX3xx, SRX550M, and vSRX	50, 51, 53, 123, 443, 500 or 4500, 514 or 3514, 7804	**ge-0/0/0** through **ge-0/0/3**
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**

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 the following guidelines:

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

Tab	Field	Action
General	Device Host Name	The device host name is auto-generated and uses the format *tenant-name.host-name*. 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	**NOTE:** Device Management, enabled by default, allows you to create a site with only device management capability (without any services) and add services later. To add an SD-WAN capability for this site, choose one of the following SD-WAN service types: • 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	Select a device template for the SRX Series device. The SRX Series device template contains information for configuring the SRX Series device. For example, for an SRX4100 device, select **SRX4x00 as SD-WAN CPE** (or a modified version of that template) as the device template.

Tab	Field	Action
Device	Use for Fullmesh	Click the toggle button to enable the WAN link to be part of a full-mesh topology. 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. Configure the two additional fields that appear: • 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. 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.
Device	**Enable Local Breakout**	Click the toggle button to enable local breakout on the WAN link. By default, local breakout is disabled. **NOTE:** • 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	Click the toggle button to enable the WAN link as the most preferred breakout link. If you disable this option, the breakout link is chosen using ECMP from the available breakout links.

Tab	Field	Action
Device	**Connects to Provider Hubs**	**NOTE:** The **Connects to Provider Hubs** field is available only if you have selected a provider hub. Click the toggle button to specify that the WAN link of the site connects to a provider hub. **NOTE:** • 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**	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. This WAN link is then used to establish the OAM tunnel.
Device	**Overlay Tunnel Type**	This field is displayed when the **Connects to Provider Hubs** field is enabled. Select the mesh overlay tunnel type (GRE and GRE_IPSEC) of the tunnel to the hub. MPLS links can have both GRE and GRE_IPSEC as the overlay link type. However, Internet links can have only GRE_IPSEC as the overlay link type.
Device	**Overlay Peer Interface**	This field is displayed when the **Connects to Provider Hubs** field is enabled. Select the interface name of the hub device to which the WAN link of the site is connected.
Device	Link Priority	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.
Device	Add LAN Segment	Add the LAN segment by specifying the **Name**, **Department**, **Gateway Address/Mask**, and **CPE Ports**.

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.

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.
- Partially-Provisioned– Indicates that one or more DHCP WAN links of the site does not have an IP address after ZTP is complete.
- 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 the following 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 *tenant-name.host-name*. You cannot change the tenant-name part in the device host name. Use alphanumeric characters and hyphen(-); the maximum length allowed is 32 characters.

Tab	Field	Action
General	Site Capabilities	**NOTE:** Device Management, enabled by default, allows you to create a site with only device management capability (without any services) and add services later. To add an SD-WAN capability for this site, choose one of the following SD-WAN service types: • 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 Secure SD-WAN Advanced services. 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 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	Select a device template for the CPE device. For example, for an SRX300 device, select **SRX as SD-WAN CPE** (or a modified version of that template) as the device template.

Tab	Field	Action
Device	Use for Fullmesh	Click the toggle button to enable the WAN link to be part of a full-mesh topology. 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. **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. Configure the two additional fields that appear: • 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. **NOTE:** For links with public IP addresses, we recommend that you use GRE over IPsec as the mesh overlay link type. • Mesh Tags: Select a mesh tag for the WAN link. **NOTE:** You can select only one mesh tag, so ensure that you select the correct one. The tunnels between the enterprise hub and the branch site or between two branch sites are added based on matching mesh tags.
Device	**Enable Local Breakout**	Click the toggle button to enable local breakout on the WAN link. By default, local breakout is disabled. **NOTE:** • 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	Click the toggle button to enable the WAN link as the most preferred breakout link. If you disable this option, the breakout link is chosen using ECMP from the available breakout links.

Tab	Field	Action
Device	**Connects to Provider Hubs**	**NOTE:** The **Connects to Provider Hubs** field is available only if you have selected a provider hub. Click the toggle button to specify that the WAN link of the site connects to a provider hub. **NOTE:** • 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**	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. This WAN link is then used to establish the OAM tunnel.
Device	**Overlay Tunnel Type**	This field is displayed when the **Connects to Provider Hubs** field is enabled. Select the mesh overlay tunnel type (GRE and GRE_IPSEC) of the tunnel to the hub. MPLS links can have both GRE and GRE_IPSEC as the overlay link type where as Internet links can have only GRE_IPSEC as the overlay link type.
Device	**Overlay Peer Interface**	This field is displayed when the **Connects to Provider Hubs** field is enabled. Select the interface name of the hub device to which the WAN link of the site is connected.
Device	Link Priority	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.

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 Step 3 in the Add an Enterprise Hub Site section.

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 on which you can install the signature database.

2. Select the check boxes corresponding to the devices on which you want to install the signature database. 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 installation of the signature database on the devices that you selected.

- **Schedule at a later time**—To install the signature database later and specify a date and the time at which 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 to which you want to add the firewall policy intent.

   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 for which you want to apply the firewall policy intent	Click the add icon (**+**) to select from the list of addresses, departments, sites, site groups, users, zones, or the Internet
Select the destination endpoints for which you want to apply the firewall policy intent	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 does not involve hubs, you'll 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 wish 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

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

Tab	Field	Action
General	Device Host Name	The device host name is auto-generated and uses the format *tenant-name.host-name*. 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.
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	Click the toggle button to automatically import firewall and NAT policies from the NGFW device to CSO. For this zero-touch provisioning (ZTP) has to be disabled because CSO does not provision brownfield NGFW devices (devices which are already configured and operational) by using ZTP. By default, the Import Policy Configuration option is disabled. If you do not 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.

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

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 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 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.

See "Install the Signature Database" on page 17.

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 18.

Step 3: Keep Going

IN THIS SECTION

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
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
Use CSO to implement SD-WAN in an enterprise network	See In Focus: How to Deploy SD-WAN by Using CSO

If you want to	Then
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