JUNIPER NETWORKS | Engineering Simplicity

In Focus

Contrail Service Orchestration: How to Deploy SD-WAN

IN THIS GUIDE

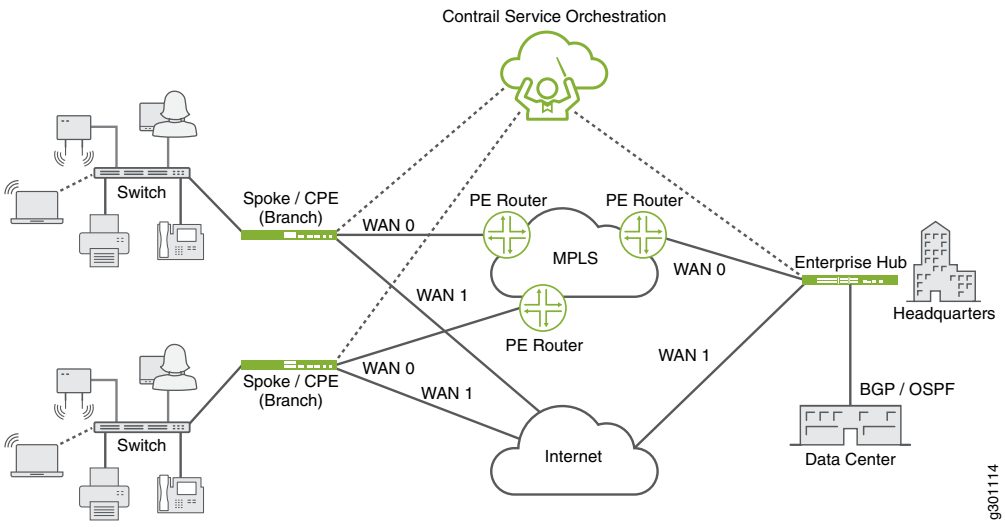
About This In Focus Use Case

Use Case	Use Contrail Service Orchestration (CSO) to implement SD-WAN in an enterprise network.
Audience	Enterprise users who want to learn how to use CSO to implement SD-WAN. Managed services provider (MSP) users who want to understand how to implement SD-WAN for their customers' enterprise networks.
Knowledge Level	Familiarity with routing, software-defined networking, branch networking, and cloud computing.

Benefits	• Save time by automating branch deployment. • Optimize usage of WAN links and performance of applications. • Reduce operational complexity by monitoring and configuring using an intuitive GUI.
Products Used	CSO Release 5.3.0 Refer to "Supported Devices, and Ports and Protocols to Open" on page 45 for details of the devices that you can use.

This In Focus guide provides a high-level overview of software-defined WAN (SD-WAN) and explains the tasks required to configure SD-WAN in an enterprise scenario using CSO Software as a Service (SaaS), which refers to the CSO version hosted by Juniper Networks. Figure 1 displays an SD-WAN enterprise topology for this use case.

Figure 1: SD-WAN Enterprise Topology



The enterprise has one headquarters, which we model as an enterprise hub site in CSO, and two branches, which we model as two SD-WAN on-premise spoke sites. Each site has two WAN links (one Internet and one MPLS) that are meshed based on matching mesh tags. In addition, the enterprise is connected to a data center and is reachable by using a dynamic route; in CSO, we model this by using a dynamically routed LAN segment.

In this guide, we provide step-by-step instructions for configuring the enterprise hub site and the SD-WAN spoke sites by using the CSO GUI. The configuration includes the workflow to add and provision the sites, and the different tasks that you need to perform after the sites are successfully provisioned. We also cover how to break out traffic directly from a site to the Internet by using an SD-WAN policy.

WHAT'S NEXT

See "SD-WAN Overview" | 3 to get a high-level understanding of SD-WAN and how it is implemented by using CSO.

SD-WAN Overview

IN THIS SECTION

In simple terms, software-defined WAN (SD-WAN) refers to the application of software-defined networking (SDN) principles to the WAN. In SD-WAN, the path for the application traffic can be dynamically controlled and selected based on specified service-level agreement (SLA) criteria. Thus, SD-WAN enables you to identify the best path for an application's traffic and to then forward the traffic on that path.

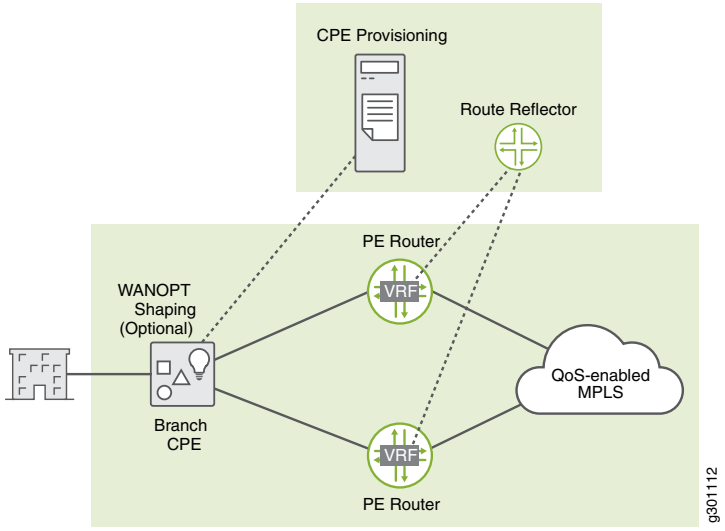
According to Gartner, SD-WAN has the following characteristics:

- Support for multiple WAN connection types (such as MPLS, Internet, LTE) simultaneously.
- Ability to select the traffic path dynamically, which allows for load sharing of traffic across WAN connections.
- Ability to simplify the management and monitoring of WANs.
- Support for VPNs and other third-party services, such as gateways and firewalls.

Branch Management Without and With SD-WAN

Figure 2 displays a topology in which a branch is managed without SD-WAN. In this scenario, the service provider (SP) maintains the quality-of-service-enabled (QoS-enabled) network and the branch, and manages the traffic (including route announcements), and VPN. In Figure 2, the area bounded by the shaded rectangles indicates the what the service provider manages and maintains.

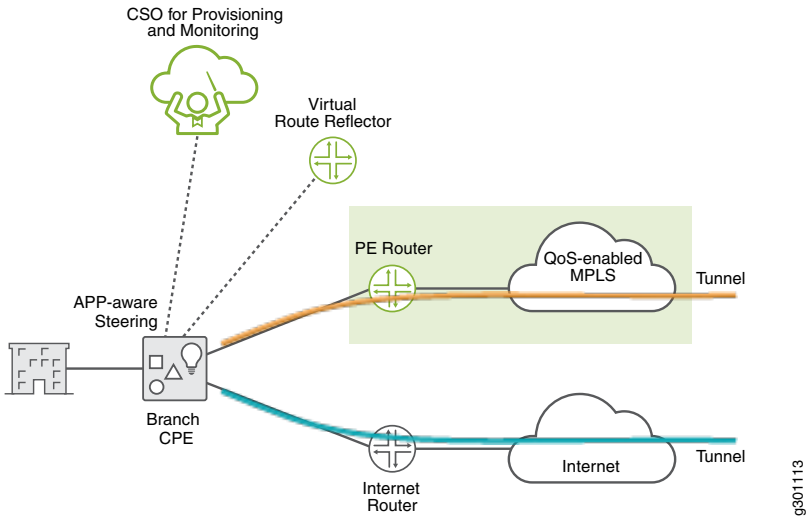
Figure 2: Branch Management Without SD-WAN



The branch customer sends traffic, which is directed over one of the two redundant links to one of the two provider edge (PE) routers, where the traffic is forwarded inside the virtual routing and forwarding (VRF) instance. Typically, the PE routers are configured in an active-backup mode (for redundancy), where traffic flows only through one router at any given time. The PE router builds queues for the traffic and the queues are respected inside the QoS-enabled MPLS network meant for that branch customer. Additionally, bandwidth might be reserved for applications that need a guaranteed bandwidth. Optionally, the service provider can provide WAN optimization, where the traffic is marked using differentiated services code point (DSCP) values and the DSCP values are adhered to downstream in the network.

Figure 3 displays the topology for managing a branch with SD-WAN. In this scenario, the service provider provides the PE router and the MPLS network and *can* be the provider for the Internet network. However, the enterprise has an option to add a different network (for example, broadband Internet) instead of using the service provider's network, and the enterprise can manage the customer premises equipment (CPE) device.

Figure 3: Branch Management With SD-WAN



To build a VPN, the traffic must be tunneled through the different networks. So, instead of sending traffic through the underlay, you use the underlay to build tunnels through the networks to the next element (node). To dynamically select the traffic path, you need to have application-aware (also called app-aware) traffic steering that identifies the application, monitors the tunnel (path) that the traffic is on, and decides the tunnel on which to send the traffic. If a tunnel degrades, the SD-WAN controller can move the traffic to a different tunnel. In the SD-WAN scenario, both the tunnels are active simultaneously.

Therefore, in the SD-WAN scenario, you don't squeeze traffic into queues; instead, you identify the traffic and select the tunnel on which to send the traffic. Services provided throughout the network (such as route reflection) can be moved to the top as shown in Figure 3.

> **NOTE:** In branch management with SD-WAN, you can have redundant PE routers in the topology, if needed. (This is not shown in Figure 3.)

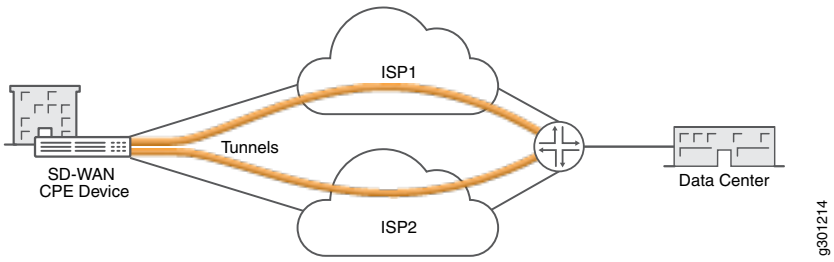
SD-WAN Overlay Tunnels

In SD-WAN, the overlay tunnels (see Figure 4) are transport-agnostic, which means that they are built independent of the underlying transport technology (such as MPLS or Internet) of the network. Tunnels are built based on the IP addresses assigned to the WAN interfaces, and can be between one spoke (branch) and another, or between a spoke and a hub (headquarters).

In CSO, you can build GRE tunnels or GRE tunnels with IPsec for additional security. When CSO identifies the application, it creates inner DSCP markings that are written to the outside tunnel so that the forwarding queues that might exist in the outside network are respected.

> **NOTE:** In CSO, the term MPLS refers to a QoS-engineered path and is used to designate the network. Therefore, CSO doesn't create MPLS frames on the underlay and only creates Ethernet frames.

Figure 4: SD-WAN Overlay Tunnels (Transport-Agnostic)



High-Level SD-WAN Architecture

Figure 5 shows an example of a high-level SD-WAN architecture. There are two branch sites connected to SD-WAN gateways (also known as spokes or CPE devices) and one central site (headquarters) connected to another SD-WAN gateway, which could be a hub device. In addition, an SD-WAN controller controls the SD-WAN gateways using a single UI, manages the devices, the creation of tunnels, and so on.

Figure 5: Example of SD-WAN Architecture

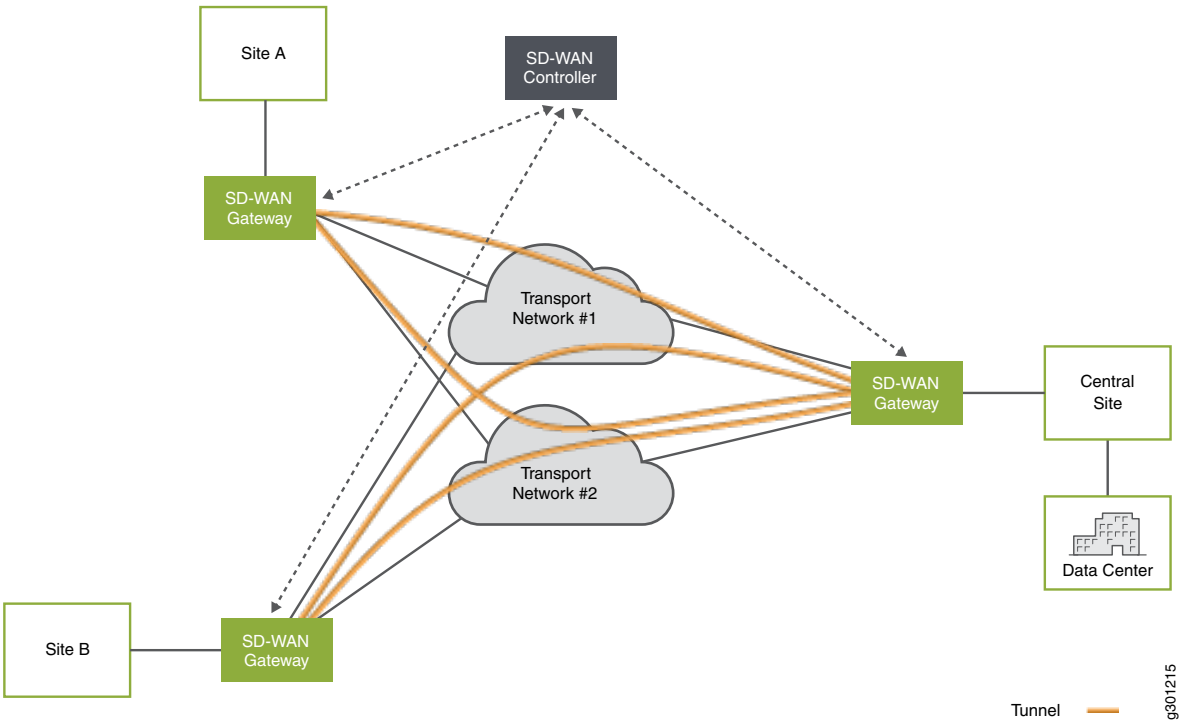
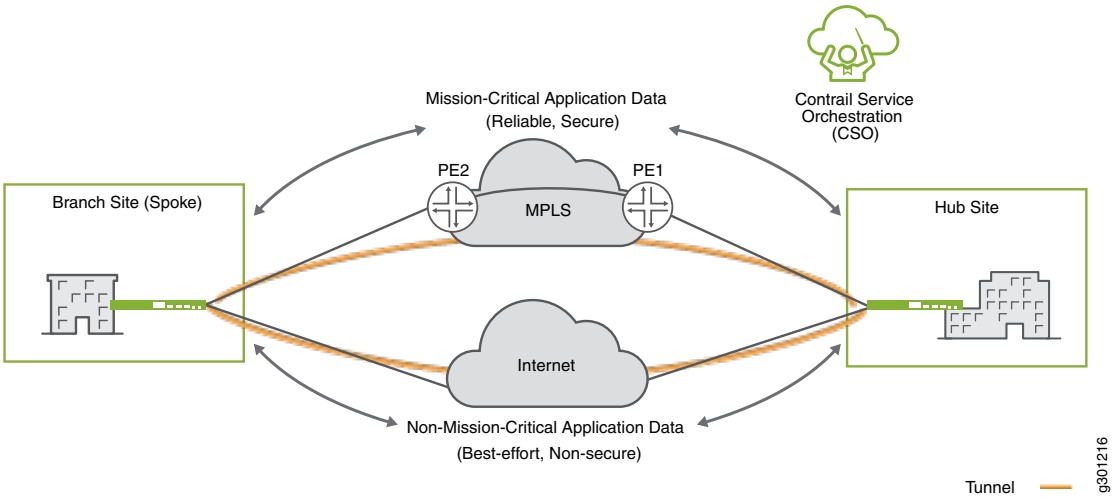


Figure 6 shows how SD-WAN is applied using CSO in a topology that has one branch site and one hub site. CSO builds one tunnel for the WAN links going over the MPLS network and a second tunnel for the WAN links going over the Internet. When you configure SD-WAN, you can ensure that mission-critical application 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).

Figure 6: Example of a CSO SD-WAN Topology



Additional Information

For more information about CSO SD-WAN, watch the Contrail SD-WAN Demos—15 Features in 15 Minutes video.

WHAT'S NEXT

See "SD-WAN Configuration Workflow" | 7 for an overview of the tasks that you must perform to configure SD-WAN.

SD-WAN Configuration Workflow

The following is the workflow for configuring SD-WAN in the enterprise topology (shown in Figure 1) by using CSO:

NOTE: The first two steps must be performed by an operating company (OpCo) Administrator user; an OpCo is like a managed services provider.

1. Log in to the CSO Administration Portal. See "Log in to the CSO Administration Portal" on page 8.
2. Add a tenant. See "Add a Tenant" on page 9.
3. Switch to tenant scope, or log in as tenant administrator. See "Switch Scope or Log in as Tenant Administrator" on page 11.

4. Configure an enterprise hub site. See "Configure Enterprise Hub Site" on page 12.

5. Configure the SD-WAN spoke sites. See "Configure SD-WAN Spoke Sites" on page 33.

6. Monitor sites and devices. See "Monitor Sites and Devices" on page 43.

WHAT'S NEXT

Before you begin configuring SD-WAN, see the "Before You Begin" | 8 topic.

Before You Begin

Before you configure SD-WAN:

- Ensure that you have a valid user account (OpCo Administrator or Tenant Administrator) on CSO SaaS (https://cso.juniper.net/). If you don't have an account, contact your assigned Juniper Networks account manager or get in touch with Juniper through the How to Buy page.
- Decide which devices you want to use for the enterprise hub and the two SD-WAN spoke sites (see "Supported Devices, and Ports and Protocols to Open" on page 45).
- Ensure that you have root access to the hub and spoke devices because you might need to access the Junos OS CLI.
- Ensure that you have the requisite licenses for CSO.
- Decide whether you want to break out traffic locally from the branches, from the enterprise hub, or both.

WHAT'S NEXT

Log in to CSO to start configuring SD-WAN.

Log in to the CSO Administration Portal

To log in to the CSO Administration Portal:

1. Open the link to the CSO portal (for example, https://cso.juniper.net/) in a Web browser.

2. Enter your username and password and click **Log In**.

   The Welcome page appears.

3. Click the close icon (**X**) or click **Go to Dashboard** to go the Dashboard page.

WHAT'S NEXT

After successfully logging in, you must add the tenant for which you are configuring SD-WAN.

Add a Tenant

In CSO, a tenant is a logical representation of a customer. Tenants enable the separation and isolation of resources (such as sites) and traffic of different customers from one another.

To add a tenant:

1. From the CSO menu, select **Tenants**.

   The Tenants page appears.

2. Click the Add (**+**) icon.

   The Add Tenants wizard appears, displaying the General settings to be configured.

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

3. Configure the General settings as explained in Table 1, and click **Next**.

   You are taken to the Deployment Info section of the wizard.

4. Configure the Deployment Info settings as explained in Table 2, and click **Next**.

   You are taken to the Tenant Properties section of the wizard.

5. Configure the Tenant Properties settings as explained in Table 3, and click **Next**.

   You are taken to the Summary section of the wizard, where a summary of the settings that you configured is listed.

6. Review the configuration in the Summary section and, if needed, modify the settings.

NOTE: You can download the tenant settings that you configured as a JavaScript Object Notation (JSON) file by clicking the **Download as JSON** link at the bottom of the Summary section.

7. Click **Finish**.

   You are returned to the Tenants page, and CSO triggers a job to add the tenant and displays a confirmation message. Click the link in the message to view the details of the job. Alternatively, you can check the status of the job on the Jobs (**Resources > Jobs**) page.

   After the job finishes successfully, the tenant that you added is displayed on the Tenants page.

   If an SMTP server is configured. an e-mail is sent to the tenant, which includes a URL to access Customer Portal. The URL is active for only 24 hours and is valid only for the first login.

Table 1: General Settings (Add Tenant)

Field	Guideline
Basic Information	
Name	Enter a unique name for the tenant. The name can contain alphanumeric characters, underscores, and hyphens, and must be less than 15 characters long. For example, Ent_Tenant.
Admin User	You must add an administrator user that can perform the administration tasks for that tenant.
First Name	Enter the first name of the administrator user.
Last Name	Enter the last name of the administrator user.
Username (Email)	Enter the e-mail address of the administrator user. The e-mail address will be the username that the administrator user will use to log in to the CSO portal. After the tenant is added successfully, CSO sends an e-mail containing the link to the CSO portal and a link to set the password.
Roles	Select one or more roles (both predefined and custom roles) that you want to assign to the tenant user, and click the right arrow (>) to move the selected role or roles from the Available column to the Selected column.
Password Policy	Specify the duration (in days) after which the password will expire and must be changed. Range: 1 through 365. Default: 180.

Table 2: Deployment Info Settings (Add Tenant)

Field	Guideline
Services	
Services for Tenant	Select the services that you want to be available for the tenant. The types of services that you select for the tenant determine the types of sites that a tenant can add. For example, if you select SD-WAN, a tenant can add only SD-WAN sites. For this use case, select **SD-WAN**.
SD-WAN Mode	If you selected SD-WAN as a service type, this field displays real-time optimized as the supported SD-WAN mode, which means that application quality of experience (AppQoE) is supported. You cannot modify this field.

Table 3: Tenant Properties Settings (Add Tenant)

Field	Guideline
NOTE: In this guide, we discuss only the network segmentation setting. Use the defaults for the rest of the tenant properties. For information about other tenant properties, see the *Adding a Single Tenant* topic in the *Administration Portal User Guide* (available on the CSO Documentation page).	
Network Segmentation	In CSO, network segmentation, which is enabled by default, enables you to isolate the traffic of one department from another. We'll use the default setting for this use case. **NOTE:** • After the tenant is added, you cannot change this setting. • If you disable network segmentation, then the LAN segments (across different sites in a tenant) cannot have overlapping subnets.

WHAT'S NEXT

> After the tenant is added successfully, you must change the scope to that tenant, or log in to Customer Portal and start adding sites for the tenant.

Switch Scope or Log in as Tenant Administrator

After the tenant is added successfully, you must change the scope to the tenant as follows:

- If you are an OpCo Administrator user, you can switch the scope by doing one of the following:

- On the Tenants page, click the ***Tenant-Name*** link.
- Select the tenant name from the scope switcher list that is displayed on the CSO banner.

- Log in to the CSO portal as a Tenant Administrator user.

The Welcome page appears. Click the close icon (**X**) or click **Go to Dashboard** to go the Dashboard page.

WHAT'S NEXT

> The next step is to add an enterprise hub site for the tenant, which represents the headquarters of the enterprise in this use case topology.

Configure Enterprise Hub Site

SUMMARY

In this section, we add an enterprise hub site. After the site is activated, we perform post-provisioning tasks such as uploading and installing device licenses, and adding and deploying policies.

IN THIS SECTION

Explanation of Procedure

The workflow for configuring the enterprise hub site is as follows:

1. Add the enterprise hub site.
2. After the enterprise hub site is provisioned successfully, perform the following post-provisioning tasks:
   a. Upload and install device licenses.
   b. Install the signature database.

c. Add and deploy a firewall policy.

d. Add an SD-WAN breakout profile.

> **NOTE:** In general, adding breakout profiles is optional. If you choose not to break out traffic, you don't need to add a breakout profile. In this use case, we add breakout profiles to show how you can configure local breakout.

e. Add and deploy an SD-WAN policy intent.

Add Enterprise Hub Site

An enterprise hub is an SD-WAN site that is used to carry site-to-site traffic between on-premise spoke sites and to break out backhaul (also called central breakout) traffic from on-premise spoke sites. An enterprise hub typically has a data center department behind it; however, this is not enforced in CSO.

For more information, see the *Enterprise Hubs Overview* topic in the *Customer Portal User Guide* (available on the CSO Documentation page).

> **NOTE:** Before you add the enterprise hub site, 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, and Ports and Protocols to Open" on page 45.

To add an enterprise hub site:

1. Click **Resources > Site Management**.

   The Sites page appears.

2. Click **Add**, and select **Add Enterprise Hub**.

   The Add Enterprise Hub wizard appears, displaying the General settings to be configured.

3. Configure the General settings as explained in Table 4, and click **Next**.

   You are taken to the WAN section of the workflow.

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

4. Configure the WAN settings as explained in Table 5, and click **Next**.

   You are taken to the LAN section of the workflow.

5. Add a LAN segment:

   a. Click the Add (**+**) icon.

      The Create LAN Segment page appears.

   b. Configure the LAN segment settings as explained in Table 6

   c. Click **OK**.

      You are returned to the LAN section of the workflow, and the LAN segment that you added is displayed.

6. Click **Next**.

   You are taken to the Summary section of the workflow.

7. Review the configuration in the Summary section and, if required, modify the settings.

8. Click **Finish**.

   The Site Activation: *Enterprise-Hub-Site-Name* page appears, and the site activation process proceeds through the tasks explained in Table 7.

   > **NOTE:** The time taken for site activation varies depending on the device that CSO is activating.

9. Click **OK** to close the Site Activation page.

   > **NOTE:** If you don't want to wait for the site activation to finish, you can close the Site Activation page and monitor the status of the site activation from the Jobs page (**Monitor > Jobs**).

Table 4: General Information (Add Enterprise Hub)

Field	Guideline
Site Information	
Site Name	Enter a unique name for the site. The name can contain alphanumeric characters and hyphens (-), and cannot exceed 10 characters.

Table 4: General Information (Add Enterprise Hub) *(continued)*

Field	Guideline
Site Group	Use the default setting (None), which indicates that you're not using site groups.
Site Capabilities	Because we're adding an enterprise hub site with only SD-WAN, we select only SD-WAN as the site capability.
WAN Capabilities	Click the SD-WAN card to select SD-WAN as the WAN capability for the enterprise hub site.
Configuration	
Primary Provider Hub	If the OpCo Administrator has configured additional DATA-only provider hubs and you want to have a backup for the enterprise hub, you can select a DATA-only provider hub as the primary provider hub.
Secondary Provider Hub	If you want provider hub redundancy and if the OpCo Administrator has configured additional DATA-only provider hubs, select another DATA-only provider hub as the secondary provider hub.
On-Demand VPN Threshold	Use the defaults for the on-demand VPN thresholds.
Address and Contact Information	Enter the address and contact information in the fields provided. Although it is not mandatory, providing an address lets you visualize where the site is located on a geographical map on the Monitor Overview page.
Advanced Configuration	For the DNS and NTP servers, you can either use the defaults or specify DNS and NTP servers.
Name Server IP List	If needed, specify the IPv4 addresses of one or more DNS servers.
NTP Server	If needed, specify the IP addresses of one or more NTP servers.
Select Timezone	Select a time zone for the site.

Table 5: WAN Settings (Add Enterprise Hub)

Field	Guideline
Device Information	

Table 5: WAN Settings (Add Enterprise Hub) *(continued)*

Field	Guideline
Device Template	Ensure that you select the correct device template from the carousel; the template depends on the device that you are using as the enterprise hub. For example, for an SRX4100 device, select **SRX4x00 as SD-WAN CPE** (or a modified version of that template) as the device template.
Serial Number	Enter the serial number of the device.
Auto Activate	This setting is enabled by default in device templates. Therefore, ensure that automatic activation is enabled.
Boot Image	If you want to upgrade the enterprise hub device with the latest supported Junos OS version, select the boot image from the list. The boot image is used to upgrade the device when CSO starts the zero touch provisioning (ZTP) process. If you don't specify a boot image, which is the default option (**Use Image on Device**) in the list, then the CSO skips the procedure to upgrade the device during ZTP.
WAN Links	You can configure a maximum of four WAN links. In this use case, we configure two WAN links: one Internet and one MPLS.
WAN_0 (*WAN-Interface-Name*)	The first WAN link is enabled by default. Fields marked with an asterisk (*) must be configured to proceed.
Link Type	For the first WAN link, we use the default (**Internet**) for the underlay network type to ensure reachability to the redirect server.
Egress Bandwidth	Enter the maximum egress bandwidth (in megabits per second [Mbps]) that is allowed for the WAN link.
Address Assignment	Displays the method of assigning an IP address to the WAN link (STATIC). You cannot modify this field. You must provide an IP address prefix and the gateway address for the WAN link.
Static IP Prefix	Enter the IPv4 address prefix of the WAN link; for example, 192.0.2.8/24.

Table 5: WAN Settings (Add Enterprise Hub) *(continued)*

Field	Guideline
Gateway IP Address	Enter the IP address of the gateway of the WAN link's service provider.
Public IP Address	**NOTE:** You should provide a public IP address only if the static IP prefix is a private IP address and 1:1 NAT is configured. Enter the public IPv4 address for the link, if needed.
Advanced Settings	Only the settings that need to be configured for this WAN link are included here. Use the defaults for the other settings.
Provider	Enter the name of the WAN link's service provider.
Cost/Month	Leave this as the default because this field is not used in CSO Release 5.3.0.

Table 5: WAN Settings (Add Enterprise Hub) *(continued)*

Field	Guideline
Enable Local Breakout	Click the toggle button to enable the WAN link to be used for local breakout. Local breakout is an SD-WAN feature that enables Internet links to break out traffic directly from a site. For example, if you want to provide guests who visit your enterprise with Internet access, you can use local breakout to break out guest traffic locally from the site directly to the Internet. **NOTE:** If you enable local breakout, this only means that the WAN link *can* be used for local breakout. To enable traffic to break out from the site, you must also configure a breakout profile, reference that profile in an SD-WAN policy intent, and deploy the SD-WAN policy. If you enable local breakout, additional fields appear: • **Breakout Options**: Retain the default setting of using the WAN link for both breakout and WAN traffic. • **Autocreate Source NAT Rule**: When you enable local breakout on a link, this setting is enabled. Retain the default setting. Enabling this setting triggers automatic creation of source NAT rules for the site. **NOTE:** If NAT is not enforced by a separate device in your network (for example, an Internet gateway firewall), then we recommend that you enable this setting because it allows CSO to automatically create a NAT policy for the site. • **Translation**: Select the type of NAT to be used on the traffic on the WAN link. For this use case, retain the default setting (**Interface**). • **Preferred Breakout Link**: Retain the default setting (**Disabled**). • Retain the default settings for the rest of the local breakout parameters.

Table 5: WAN Settings (Add Enterprise Hub) *(continued)*

Field	Guideline
Use for Fullmesh	Click the toggle button to enable the WAN link to be part of a full mesh topology. Configure the two additional fields that appear: • **Mesh Overlay Link Type**: Retain 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 one or more mesh tags for the WAN link. **NOTE:** The tunnels between the enterprise hub site and the on-premise spoke 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 on-premise spoke site, the mesh tags must be the same for both sites.
Use for OAM traffic	Click the toggle button to enable the use of the WAN link for Operation, Administration, and Maintenance (OAM) traffic. The WAN link is then used to establish an OAM tunnel for communication between the enterprise hub site and CSO. **NOTE:** To ensure redundancy, we recommend that you configure at least two WAN links that can be used for OAM traffic.
WAN_1 (*WAN-Interface-Name*)	Click the toggle button to configure a second WAN link. Fields related to the WAN link appear. **NOTE:** Only the fields for which the settings are different from the first WAN link are listed here. For the rest of the fields, see the explanations for the first WAN link.
Link Type	For the second WAN link, select **MPLS** as the link type. Configure the egress bandwidth, static IP prefix, gateway IP address, and (if applicable) public IP address. See the explanations for the first WAN link.
Advanced Settings	

Table 5: WAN Settings (Add Enterprise Hub) *(continued)*

Field	Guideline
Enable Local Breakout	Because we've already enabled local breakout on the first WAN link, retain this as disabled, which means that the WAN link won't be used for local breakout.
Use for Fullmesh	Click the toggle button to enable the WAN link to be part of a full mesh topology. Configure the additional fields that appear, as explained for the first WAN link.
Use for OAM Traffic	To ensure redundancy for OAM tunnels, click the toggle button to enable the WAN link to be used for sending OAM traffic.
Management Connectivity	We recommend that you don't configure this setting (leave the IP Prefix field blank) because management connectivity is handled automatically by CSO.

Table 6: LAN Segment Settings (Enterprise Hub)

Field	Guideline
Name	Enter a unique name for the LAN segment, which can contain alphanumeric characters and underscores (_), and cannot exceed 15 characters.
Type	Because the enterprise hub is connected to a data center, select **Dynamic Routed** to indicate that the LAN segment is not directly connected to the hub device and is reachable by using a dynamic route. If you select this option, you must specify the dynamic routing information.
Department	Click **Create Department** to add a new data center department. On the Add Department page appears, enter a name for the department (for example, DC-Dept), and click **OK** to add the department. The department is added, and the department name is displayed in the Department field.

Table 6: LAN Segment Settings (Enterprise Hub) *(continued)*

Field	Guideline
Protocol	Select the routing protocol (BGP or OSPF) to be used by the data center department to learn routes from the data center. For this use case, we'll select BGP and configure the parameters related to BGP.
Advertise LAN Prefix	Click the toggle button to advertise the LAN prefixes of the SD-WAN spoke sites to the data center through the data center department that is associated with the enterprise hub. By default, this field is disabled. **NOTE:** • Route advertisements from the data center to SD-WAN spoke sites take place irrespective of whether this field is enabled or disabled. • You must avoid overlapping IP addresses between the LAN network of the SD-WAN spoke sites and the data center network.
Gateway Address/Mask	Enter a valid gateway IP address and subnet mask for the LAN segment. This address will be the default gateway for the endpoints in this LAN segment. For example: 192.0.2.8/24.
CPE Ports	Select the port (on the enterprise hub device) that peers with the data center gateway.
BGP Configuration	
Authentication	Select the BGP route authentication method to be used: • None—Indicates that no authentication should be used. This is the default setting. • Use MD5—Indicates that MD5 is to be used for authentication. If you select this option, you must specify an authentication key.
Peer IP Address	Enter the IP address of the BGP neighbor.

Table 6: LAN Segment Settings (Enterprise Hub) *(continued)*

Field	Guideline
Peer AS Number	Enter the autonomous system (AS) number of the BGP neighbor. CSO uses the default AS number 64512. If the AS number of the data center's router is different from CSO's AS number, an external BGP (eBGP) peering session is established. If the AS number is the same, an internal BGP (iBGP) peering session is established.
Auth Key	If you specified that MD5 should be used for authentication, specify an MD5 authentication key (password), which is used to verify the authenticity of BGP packets.

Table 7: Site Activation Tasks and Troubleshooting

Site Activation Tasks	Troubleshooting
Model Site: CSO first models the site to begin the activation process.	
Prestage Device: Depending on the type of device used, you might need to copy the configuration that is generated by CSO and commit the configuration on the device. For such devices, CSO can move to the next step (detecting the device) only after the configuration is committed successfully on the device.	This step typically goes through without problems. However, if you encounter a problem, log in to the device (using a console or a management interface), access the CLI, and verify that the stage-1 configuration was committed on the device.

Table 7: Site Activation Tasks and Troubleshooting *(continued)*

Site Activation Tasks	Troubleshooting

Detect Device: The device reaches out to CSO, and communication with CSO is established.
 	
This task typically takes a few minutes. If the status shows as Pending after about 10 minutes, try the troubleshooting steps.
	If the device is not detected:
	
	1. Check that the correct interfaces on the device are connected.
	2. Log in to the device, and access the CLI.
	3. Check the system time that is configured on the device by executing the **show system uptime** command, and ensure that the system time is accurate. A mismatch in time might mean that the device is unable to connect to the redirect server.
	4. **NOTE:** This step is applicable only for on-premise spoke sites.
	
	Execute the **show interfaces terse** command.
	
	In the command output, verify whether the device received a DHCP IP address. If the device did not receive an IP address, try to reconnect.
	5. If the device has a valid IP address, then verify that the device can reach the Internet by using the **ping** command. For example, **ping www.juniper.net**.
	
	If the **ping** command executes successfully, this means that the device can reach the Internet, and DNS resolution is working.
	6. Verify whether the device has the permissions required for outgoing connections on port 443 by executing the **telnet redirect.juniper.net 443** command.
	
	If the device has the required permissions, you should see an output similar to the following:
	
	`Trying 192.0.2.155...`
	`Connected to telnet-host.example.com.`
	`Escape character is '^]'.`

Table 7: Site Activation Tasks and Troubleshooting *(continued)*

Site Activation Tasks	Troubleshooting

Bootstrap Device:
 	
This task comprises the following sub-tasks:
 	
1. A secure OAM tunnel (using IPsec) from the device to the OAM hub is established.
2. An outbound SSH connection from the device is established with CSO.
3. An Internal BGP (iBGP) peering between the device and the virtual route reflector (VRR) is established.
4. The device sends a Bootstrap Complete message to CSO, which CSO receives and marks the bootstrap as completed.
 	
The device is now managed by CSO.
 	
This task typically takes a few minutes to finish. If the status shows as Pending after about 10 minutes, try the troubleshooting steps.
	If the bootstrap device task does not finish successfully:
	
	1. Verify whether the stage-1 configuration was deployed on the device by executing the **show configuration | display set | match outbound-ssh | match 7804** command.
	If the resulting output is similar to the following sample output, it means that the stage-1 configuration was deployed successfully.
	
	`set system services outbound-ssh client CSO-xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx 192.0.2.100 port 7804`
	
	2. Check if the secure OAM tunnels are up by executing the following commands:
	• **show security ike sa** command. If the State field in the output doesn't display **UP**, it means that port 500 is blocked. Ensure that you open 500 and retry the activation job (from the Jobs page).
	• **show security ipsec sa** command. If the State field in the output doesn't display **UP**, it means that port 4500 is blocked. Open port 4500, and retry the activation job (from the Jobs page).
	3. Verify whether the device has established BGP peering with the VRR by executing the **show bgp summary** command.
	If the State field in the output displays **Establ**, it means that BGP peering is established successfully.
	4. Verify whether the secure OAM session is established by executing the **show security flow session destination-port 7804** command.
	If the resulting output is similar to the following output, it means that the secure OAM session was established successfully.
	
	`Session ID: 430000098, Policy name: default-policy-00/2, Timeout: 1778, Valid In: 192.0.2.10/15190 --> 192.0.2.20/23;tcp, If: ge-7/1/0.0, Pkts: 109, Bytes: 5874, CP Session ID: 430000093 Out: 192.0.2.20/23 --> 192.0.2.10/15190;tcp, If: ge-7/1/1.0, Pkts: 64, Bytes: 4015, CP Session ID: 430000093 Total sessions: 1`

Table 7: Site Activation Tasks and Troubleshooting *(continued)*

Site Activation Tasks	Troubleshooting
Provision Device: The final task in the site activation process is that CSO applies the provisioning configuration on the device. After this task is completed, the device is ready for use. The time taken for this task depends on the type of device. If the status is showing Pending after about 20 minutes, try the troubleshooting steps.	Go to the Jobs page (**Monitor > Jobs**), search for the ZTP job, and check the status. Click the *job-name* link to view the tasks associated with the job and their status. You can drill down further by clicking the *task-name* link. If the status of the job or task is **In Progress**, wait until the job or task finishes. If the job failed, you can retry the job by selecting the job, and clicking the **Retry Job** button.

WHAT'S NEXT

> After the enterprise hub is successfully provisioned, you must carry out the post-provisioning tasks, the first of which is to upload and install device licenses.

Upload and Install Device Licenses

After a site is successfully provisioned, you must upload the required device licenses into CSO, and then install the licenses on the device (that is associated with the site).

To upload and install device licenses:

1. Upload the device license file:

   NOTE: Device license files can be uploaded by the managed services provider (OpCo) Administrator or by the tenant.

   a. Select **Administration** > **Device Licenses**.

      The Device License Files page appears.

   b. Click the Add (+) icon.

      The Add License page appears.

   c. 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.

d. (Optional) Enter a description for the license file in the **Description** field.

e. 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 returns you to the Device License Files page.

If needed, upload additional device license files.

2. Install (push) the license to the device:

a. Select the device license file that you want to push to the device.

b. Click **Push License**, and select **Push**.

The Push License page appears, displaying the sites and devices to which the license can be pushed.

c. 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 and displays a confirmation message. After the job completes successfully, the license is pushed to the device. You can view the status of the job on the Jobs page (**Monitor > Jobs**).

WHAT'S NEXT

The next step after installing licenses is to install the signature database on the device.

Install the Signature Database

Because SD-WAN uses application identification, you must install the active signature database (downloaded by the Juniper team to CSO) on the device.

> **TIP:** The signature database also contains intrusion detection prevention (IDP) or intrusion prevention system (IPS) signatures, which are used in CSO's IDP or IPS features. For more information, see the *About the IPS Profiles Page* in the *Customer Portal User Guide* (available at the CSO Documentation page).

To install the active signature database:

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

   The Signature Database page appears.

2. Click **Install Signatures**.

   The Install Signatures page appears, displaying the signature database version and the devices on which you can install the signature database.

3. 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 that are displayed.

4. From the **Type** field:
   - Select **Run now** to trigger the installation of the signature database immediately.
   - Select **Schedule at a later time** to install the signature database later, and specify a date and time at which you want the installation to be triggered.
5. Click **OK**.
   - If you specified that the database must be installed immediately, a job is triggered. In the Job Tasks page that appears, the tasks associated with the signature database installation are displayed. Click **OK** to exit and return to the Signature Database page.
   - If you specified that the database must be installed 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.

WHAT'S NEXT

> After the signature database is installed successfully, you must add a firewall policy to allow traffic.

Add and Deploy Firewall Policy

Because Juniper's SD-WAN devices are tightly integrated with security features, you must configure a firewall policy to allow traffic that traverses zones. By default, traffic between one site and another site, and traffic from a site to the Internet is *not allowed* and must be explicitly allowed by using a firewall policy. CSO supports intent-based policies, which makes it simple for you to configure firewall policies.

To add and then deploy a firewall policy:

1. Add a firewall policy:
   a. Select **Configuration > Firewall > Firewall Policy**.

      The Firewall Policy page appears.

   b. Click the Add (**+**) icon.

      The Add Firewall Policy page appears.

   c. Complete the configuration according to the guidelines provided in Table 8.

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

   d. Click **OK**.

      The firewall policy is added and displayed in the grid.

2. Add one or more firewall policy intents to the policy:
   a. Click the ***Firewall-Policy-Name*** link.

      The *Firewall-Policy-Name* page appears.

   b. Click the Add (**+**) icon.

      The fields for adding an intent are displayed inline.

   c. Complete the configuration according to the guidelines provided in Table 9.

   d. Click **Save**.

      The intent is saved, and a confirmation message is displayed.

3. Deploy the firewall policy:
   a. Click the **Deploy** button.

      The Deploy page appears.

   b. From the **Choose Deployment Time** field:
      - Select **Run now** to trigger the deployment of the policy immediately.
      - Select **Schedule at a later time** to schedule the deployment for later.

        If you schedule the deployment for later, enter the date (in MM/DD/YYYY format) and time (in HH:MM:SS 24-hour or AM/PM format) at which you want the deployment to be triggered. You specify the time in the local time zone of the client from which you access the CSO GUI.

You are returned to the Firewall Policy page, and a job to deploy the policy is triggered. You can check the status of the deployment on the Jobs page (**Monitor > Jobs)**.

Table 8: Add Firewall Policy Settings

Field	Guideline
Name	Enter a unique name for the firewall policy.
Description	(Optional) Enter a description for the firewall policy.
All Sites	Select the **Enable** check box to apply the firewall policy to all sites.
Select Sites	To apply the firewall policy only to specific sites, select the sites from the Available column, and click the right arrow icon (**>**).

Table 9: Add Firewall Policy Intent Settings

Field	Guideline
Name	Enter a name for the policy intent or use the name generated by CSO.
Description	(Optional) Enter a description for the policy intent.
Source	From the Site category, select the name of the site as the source. You can select one or more sites in the Source field. **NOTE:** You can select other options for the source (for example, a department). For more information, see *Adding Firewall Policy Intents* in the *Customer Portal User Guide* (available at the CSO Documentation page).
Action	Select **Permit** as the action to allow traffic.
Destination	From the Address category (Addr), select **Any** to specify that traffic to any Internet address or to a data center department is allowed. **NOTE:** Selecting **Any** does not mean that site-to-site traffic is allowed. To allow site-to-site traffic, you must explicitly add intents to allow such traffic. For example, if you want traffic from Site A to Site B to be allowed in both directions (from A to B and from B to A), you must add two intents: one allowing traffic from Site A to Site B and another allowing traffic from Site B to Site A.

WHAT'S NEXT

Because we enabled local breakout on the WAN links (Internet) of the enterprise hub and the SD-WAN on-premise spoke sites, the next step is to add an SD-WAN breakout profile.

Add SD-WAN Breakout Profile

> **NOTE:** You can use one breakout profile for the enterprise hub site and a different profile (or two different profiles) for the SD-WAN spoke sites, or you can use one breakout profile for all three sites.

As explained previously, if you enable a site's WAN link for local breakout, the WAN link *can* be used for local breakout. However, the decision of whether traffic breaks out locally from the site depends on the breakout profile that is referenced in the SD-WAN policy intent. So, for traffic to break out locally, you must:

1. Add an SD-WAN breakout profile.
2. Add an SD-WAN policy intent that references the breakout profile.
3. Deploy the SD-WAN policy.

To learn about breakout and breakout profiles in CSO, see *Breakout and Breakout Profiles Overview* in the *Customer Portal User Guide* (available at the CSO Documentation page).

To add an SD-WAN breakout profile:

1. Select **Configuration > SD-WAN > Breakout Profiles**.

   The Breakout Profiles page appears.

2. On the Breakout Profiles tab, click the Add (**+**) icon.

   The Add Breakout Profile page appears.

3. Complete the configuration according to the guidelines provided in Table 10.

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

4. Click **OK**.

   You are returned to the Breakout Profiles page, and a message confirming that the breakout profile was added is displayed. The page refreshes to display the breakout profile that you added.

Table 10: Fields on the Add Breakout Profile Page

Field	Guideline
Type	Select **Local Breakout (Underlay)** because we want traffic to break out locally (on the underlay) from the site.
Name	Enter a unique name for the breakout profile. You can use alphanumeric characters and hyphens (-); the maximum length is 15 characters.

Table 10: Fields on the Add Breakout Profile Page *(continued)*

Field	Guideline
Description	Enter a description for the breakout profile.
Traffic Type Profile	Select a traffic type profile to apply class of service (CoS) parameters to the breakout traffic.
Preferred Path	Because we've enabled only Internet WAN links (on the previously configured sites) to be used for breakout traffic, select **Internet** as the preferred path to be used for breaking out the traffic.
Advanced Configuration	You can optionally configure parameters for rate limiting the breakout traffic for cacheable applications. By default, rate limiting is disabled.

WHAT'S NEXT

> The next step is to add an SD-WAN policy intent that references the breakout profile.

Add and Deploy SD-WAN Policy Intent

After you add an SD-WAN breakout profile, you must add an SD-WAN policy intent, and then deploy the SD-WAN policy intent to ensure that traffic breaks out locally from the WAN link that you configured for local breakout.

To add and deploy an SD-WAN policy intent:

1. Add the SD-WAN policy intent:
   a. Select **Configuration > SD-WAN > SD-WAN Policy**.

      The SD-WAN Policy page appears.

   b. Click the Add icon (**+**).

      The parameters for an SD-WAN policy intent appear inline on the SD-WAN Policy page.

   c. Enter the policy intent information according to the guidelines provided in Table 11.

   d. Click **Save**.

      The SD-WAN policy intent is added, and a confirmation message is displayed. The Undeployed field is incremented by one, indicating that the policy intent must be deployed.

2. Deploy the SD-WAN policy intent:

   a. Click the **Deploy** button.

      The Deploy page appears.

   b. From the **Choose Deployment Time** field:

      - Select **Run now** to deploy the policy immediately.
      - Select **Schedule at a later time** to schedule the deployment for later.

        If you schedule the deployment for later, enter the date (in MM/DD/YYYY format) and time (in HH:MM:SS 24-hour or AM/PM format) at which you want the deployment to be triggered. You specify the time in the local time zone of the client from which you access the CSO GUI.

   You are returned to the SD-WAN Policy page, and a job to deploy the policy is triggered. You can check the status of the deployment on the Jobs page (**Monitor > Jobs)**.

   After the SD-WAN policy is successfully deployed, traffic can break out directly from the site.

Table 11: SD-WAN Intent Policy Settings

Field	Guideline
Name	Enter a name for the policy intent, or use the name generated by CSO.
Description	(Optional) Enter a description for the policy intent.
Source	If the SD-WAN policy intent is: • For the enterprise hub, select the name of the enterprise hub site. • For the on-premise spoke, select the name of the on-premise spoke site. **NOTE:** You can select other options for the source (for example, a department). For more information, see *Creating SD-WAN Policy Intents* in the *Customer Portal User Guide* (available at the CSO Documentation page).
Application	Select the applications for which you want to break out traffic locally. **NOTE:** You can also select **Any**, which means that this policy intent is applicable to all applications. However, you'd typically do this if you were matching on a guest department (that is the Source would be the guest department) where you want all guest traffic to break out to the Internet through the underlay.
Traffic Steering Profile	Click inside the text box, and select the local breakout profile that you added earlier.

If you haven't yet configured the SD-WAN spoke sites, the next step is to do so; see "Configure SD-WAN Spoke Sites" | 33.

If you have finished configuring the SD-WAN spoke sites, see "Monitor Sites and Devices" | 43.

Configure SD-WAN Spoke Sites

SUMMARY

In this section, we'll add two SD-WAN spoke sites. After the sites are activated, perform post-provisioning tasks such as uploading and installing device licenses, and adding and deploying policies.

IN THIS SECTION

Explanation of Procedure

The high-level workflow for configuring the SD-WAN spoke sites is as follows:

1. Add two SD-WAN on-premise spoke sites.

2. After the two SD-WAN spoke sites are provisioned successfully, perform post-provisioning tasks as explained in "Post-Provisioning Tasks for the On-Premise Spoke Sites" on page 42

Add On-Premise Spoke (SD-WAN CPE) Sites

An on-premise spoke represents an endpoint, like the customer premises equipment (CPE) device at a physical location, such as a branch office. Typically, these sites are connected using overlay connections to hub sites.

NOTE: Before you add the SD-WAN spoke sites, check the cable connections, review the NAT and firewall ports and protocols, and check the Junos OS version of the SD-WAN CPE device. For details, see "Supported Devices, and Ports and Protocols to Open" on page 45.

In this use case, we have two branches in our topology. So, you need to add two on-premise spoke sites.

To add on-premise spoke sites with SD-WAN capability:

1. Click **Resources > Site Management**.

   The Sites page appears.

2. Click **Add**, and select **Add On-Premise Spoke (Manual)**.

   The Add On-Premise Spoke Site wizard appears, displaying the General settings to be configured.

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

3. Configure the General settings as explained in Table 12, and click **Next**.

   You are taken to the WAN section of the workflow.

4. Configure the WAN settings as explained in Table 14, and click **Next**.

   You are taken to the LAN section of the workflow.

5. Add a LAN segment:

   a. Click the Add (**+**) icon.

      The Add LAN Segment page appears.

   b. Configure the LAN segment settings as explained in Table 15.

   c. Click **OK**.

      You are returned to the LAN section of the workflow and the LAN segment that you added is displayed.

6. Click **Next**.

   You are taken to the Summary section of the workflow.

7. Review the configuration in the Summary section and, if required, modify the settings.

8. Click **Finish**.

   The Site Activation: *Spoke-Site-Name* page appears. The activation of the site proceeds through the tasks as previously explained in Table 7.

   > **NOTE:** The time taken for site activation varies depending on the device that CSO is activating.

9. Click **OK** to close the Site Activation page.

> **NOTE:** If you don't want to wait for the site activation tasks to finish, you can close the Site Activation page, and monitor the status of the site activation from the Jobs page.

10. Repeat the steps starting from Step 2 for the second on-premise spoke site.

Table 12: General Information (Add On-Premise Spoke)

Field	Guideline
Site Information	
Site Name	Enter a unique name for the site. The name can contain alphanumeric characters, and hyphens (-) and cannot exceed 10 characters.
Site Group	Use the default setting (None), which indicates that you're not using site groups.
Site Capabilities	
WAN Capabilities	Click the SD-WAN card to select SD-WAN as the WAN capability for the on-premise spoke site.
Configuration	You must configure at least one hub to which the on-premise spoke site must connect. The combinations supported are listed in Table 13
Primary Enterprise Hub	Select the enterprise hub site that you previously configured. **NOTE:** Because the SD-WAN enterprise topology includes only one enterprise hub, we're configuring only the primary enterprise hub for the on-premise spoke site.
On-Demand VPN Threshold	Use the defaults for the on-demand VPN thresholds.
Address and Contact Information	Enter the address of the on-premise spoke site and contact information in the fields provided. Although it is not mandatory, providing an address lets you visualize where the site is located on the geographical map on the Monitor Overview page.
Advanced Configuration	For the DNS and NTP servers, you can either use the defaults or specify DNS and NTP servers.

Table 12: General Information (Add On-Premise Spoke) *(continued)*

Field	Guideline
Domain Name Server (DNS)	Specify the IPv4 addresses of one or more DNS servers.
NTP Server	If needed, specify the IP addresses of one or more NTP servers.
Select Timezone	Select a time zone for the site.

Table 13: Supported Combinations of Provider and Enterprise Hubs

Provider Hubs Specified	Enterprise Hubs Specified
Primary	None
Primary	Primary
Primary	Primary and Secondary
Primary and Secondary	None
Primary and Secondary	Primary
Primary and Secondary	Primary and Secondary
None	Primary
None	Primary and Secondary

Table 14: WAN Settings (Add On-Premise Spoke)

Field	Guideline
Device Template	
Device Series	Select the device series of the CPE device; for example, SRX. Based on the device series that you selected, the supported device templates are displayed. Ensure that you select the correct device template from the carousel. For example, for an SRX300 device, select **SRX as SD-WAN CPE** (or a modified version of that template) as the device template.

Table 14: WAN Settings (Add On-Premise Spoke) *(continued)*

Field	Guideline
Device Information	
Serial Number	Enter the serial number of the device.
Auto Activate	This setting is enabled by default in device templates, so verify that automatic activation is enabled.
Boot Image	If you want to upgrade the enterprise hub device with the latest supported Junos OS version, select the boot image from the list. The boot image is used to upgrade the device when CSO starts the ZTP process. If you don't specify a boot image, which is the default selection (**Use Image on Device**) in the list, then CSO skips the procedure to upgrade the device during ZTP.
WAN Links	You can configure a maximum of four WAN links. In this use case, we'll configure two WAN links: one Internet and one MPLS.
WAN_0 (*WAN-Interface-Name*)	The first WAN link is enabled by default. **NOTE:** Fields marked with an asterisk (*) must be configured to proceed. Only the fields relevant to this use case are documented here; use the default settings for the rest of the fields.
Link Type	Like we did for the enterprise hub site, for the first WAN link, we use the default (**Internet**) for the underlay network type to ensure reachability to the redirect server.
Access Type	Select **Ethernet** as the access type.
PPPoE	Use the default setting, which is to disable PPPoE for the WAN link.
Egress Bandwidth	Enter the maximum egress bandwidth (in Mbps) allowed for the WAN link.

Table 14: WAN Settings (Add On-Premise Spoke) *(continued)*

Field	Guideline

Address Assignment	Select the method for assigning an IP address to the WAN link:
	• If you select **DHCP**, the IP address is provided by using the DHCP server of the WAN link's service provider.
	• If you select **STATIC**, you must provide the IP address prefix and the gateway address for the WAN link.
	  ◦ **Static IP Prefix**—Enter the IPv4 address prefix of the WAN link; for example, 192.0.2.8/24.
	  ◦ **Gateway IP Address**—Enter the IP address of the gateway of the WAN link's service provider.

Advanced Settings	Only the settings that need to be configured for this WAN link are included here.
Provider	Enter the name of the WAN link's service provider.
Cost/Month	Leave this as the default because this field is not used in CSO Release 5.3.0.

Table 14: WAN Settings (Add On-Premise Spoke) *(continued)*

Field	Guideline
Enable Local Breakout	Click the toggle button to enable the WAN link to be used for local breakout. Local breakout is an SD-WAN feature that enables Internet links to break out traffic directly from a site. For example, if you want to provide guests who visit your enterprise with Internet access, you can use local breakout to break out guest traffic locally from the site directly to the Internet. **NOTE:** If you enable local breakout, the WAN link *can* be used for local breakout. To enable traffic to break out from the site, you must also configure a breakout profile, reference that profile in an SD-WAN policy intent, and deploy the SD-WAN policy. If you enable local breakout, additional fields appear: • **Breakout Options**: Retain the default setting of using the WAN link for both breakout and WAN traffic. • **Autocreate Source NAT Rule**: When you enable local breakout on a link, this setting is enabled. Retain the default setting. Enabling this setting triggers automatic creation of source NAT rules for the site. If NAT is not enforced by a separate device in your network (for example, an Internet gateway firewall), then we recommend that you enable this setting because it allows CSO to automatically create a NAT policy for the site. • **Translation**: Select the type of NAT to be used on the traffic on the WAN link. For this use case, retain the default setting (**Interface**). • **Preferred Breakout Link**: Retain the default setting (**Disabled**). • Retain the default settings for the rest of the local breakout parameters.

Table 14: WAN Settings (Add On-Premise Spoke) *(continued)*

Field	Guideline
Use for Fullmesh	Click the toggle button to enable the WAN link to be part of a full mesh topology. Configure the two additional fields that appear: • **Mesh Overlay Link Type**: Retain 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:** For on-premise spoke sites, you can select only one mesh tag, so ensure that you select the correct mesh tag. The tunnels between the enterprise hub and the on-premise spoke site or between two on-premise spoke sites are added based on matching mesh tags.
Use for OAM traffic	Click the toggle button to enable the use of the WAN link for OAM traffic. The WAN link is then used to establish an OAM tunnel for communication between the enterprise hub site and CSO. Like we did with the enterprise hub site, to ensure redundancy, we recommend that you configure at least two WAN links that can be used for OAM traffic.
WAN_1 (*WAN-Interface-Name*)	Click the toggle button to configure a second WAN link. Fields related to the WAN link appear. **NOTE:** Only the fields for which the settings are different from the first WAN link are listed here. For the rest of the fields, see the explanations for the first WAN link.
Link Type	For the second WAN link, select **MPLS** as the link type.
Egress Bandwidth	Configure this field similar to the way that you did for the first WAN link.
Address Assignment	Similar to what you configured for the first WAN link, select a method for assigning an IP address to the WAN link.
Advanced Settings	

Table 14: WAN Settings (Add On-Premise Spoke) *(continued)*

Field	Guideline
Provider	Enter the name of the WAN link's service provider.
Cost/Month	Leave this as the default because this field is not used in CSO Release 5.3.0.
Enable Local Breakout	Because we've already enabled local breakout on the first WAN link, click the toggle button to disable the second WAN link from being used for local breakout.
Use for Fullmesh	Click the toggle button to enable the WAN link to be part of a full mesh topology. Configure the fields that appear, as explained for the first WAN link.
Use for OAM Traffic	To ensure redundancy for OAM tunnels, click the toggle button to enable the WAN link to be used for sending OAM traffic.
Management Connectivity	We recommend that you don't configure this setting (leave the IP Prefix field blank) because management connectivity is handled automatically by CSO.

Table 15: LAN Segment Settings (Add On-Premise Spoke)

Field	Guideline
Name	Enter a unique name for the LAN segment, which can contain alphanumeric characters and underscores (_), and cannot exceed 15 characters.
Department	Select a department to which the LAN segment is assigned. Alternatively, click **Create Department** to add a new department. On the Add Department page appears, enter a name for the department (for example, IT-Dept), and click **OK** to add the department. The department is added and the department name is displayed in the Department field.

Table 15: LAN Segment Settings (Add On-Premise Spoke) *(continued)*

Field	Guideline
Gateway Address/Mask	Enter a valid gateway IP address and subnet mask for the LAN segment. This address will be the default gateway for the endpoints in this LAN segment. For example: 192.0.2.8/24.
DHCP	Click the toggle button to enable the DHCP sever running on the CPE device to assign IPv4 addresses to the LAN segment. When you enable DHCP, you must configure the additional fields that appear on the page: • **Address Range Low**—Enter the starting IP address in the range of IP addresses that can be allocated by the DHCP server to the LAN segment. • **Address Range High**—Enter the ending IP address in the range of IP addresses that can be allocated by the DHCP server to the LAN segment. • **Maximum Lease Team**—Specify the maximum duration (in seconds) for which a client can request for and hold a lease on the DHCP server. • **Name Server**—Specify one or more IPv4 addresses of the DNS server.
CPE Ports	Select the ports (on the CPE device) that you want to include as part of the LAN segment.

WHAT'S NEXT

After the SD-WAN spoke sites are successfully provisioned, you must perform the post-provisioning tasks.

Post-Provisioning Tasks for the On-Premise Spoke Sites

After the two SD-WAN on-premise spoke sites are successfully provisioned, perform the following post-provisioning tasks:

1. Upload and install device licenses. See “Upload and Install Device Licenses” on page 25.
2. Install the signature database. See “Install the Signature Database” on page 26.
3. Add and deploy a firewall policy. See “Add and Deploy Firewall Policy” on page 27.

4. Add an SD-WAN breakout profile for local Internet breakout. See "Add SD-WAN Breakout Profile" on page 30.

> **NOTE:** As explained previously, adding breakout profiles is optional. If you choose not to break out traffic, you don't need to add a breakout profile. In this use case, we add breakout profiles to show how you can configure local breakout.

5. Add and deploy an SD-WAN policy intent. See "Add and Deploy SD-WAN Policy Intent" on page 31.

WHAT'S NEXT

> After completing the post-provisioning tasks for the two SD-WAN sites, you can monitor the sites and devices; see "Monitor Sites and Devices" | 43.

Monitor Sites and Devices

After configuring the enterprise hub and the two SD-WAN spoke sites, you can do the following monitoring tasks:

- On the Overview page (**Monitor > Overview**), you can view the sites that you configured on a geographical map, and the site status and connections between the sites.

  You can filter based on sites, connections, or both, and zoom in to the map.
- On the *Site-Name* page (**Resources > Site Management > *Site-Name***), you can view general information about the site, WAN overlay and underlay links, policies, and devices.
- On the *Device-Name* page (**Resources > Devices > *Device-Name***), you can view general information about the device, and view recent alerts and alarms.
- On the Generated Alerts page (**Monitor > Alerts**), you can view the alerts generated by the SD-WAN CPE or enterprise hub devices.
- On the Alarms page (**Monitor > Alarms**), you can view the alarms raised by the SD-WAN CPE or enterprise hub devices.
- On the *Tenant-Name* SLA Performance page (**Monitor > Application SLA Performance**). you can view the SLA performance of the tenant's sites that have met and not met the defined SLA values.
- On the Application Visibility page (**Monitor > Application Visibility**, you can view information about your applications such as sessions, bandwidth consumed, and risk levels.
- On the User Visibility page (**Monitor > User Visibility**), you can view information about the devices (such as top 50 devices accessing high bandwidth-consuming applications and establishing higher number of sessions) on your network.
- On the Traffic Logs page (**Monitor > Traffic Logs**), you can view the traffic logs from different sites.

Summary

In this use case, you used CSO SaaS to configure SD-WAN in an enterprise scenario consisting of one headquarters (modelled as an enterprise hub site) and two branches (modelled as two on-premise spoke sites), with the headquarters connected to a data center. You also added an SD-WAN policy to enable traffic to break out locally directly from the sites to the Internet.

Even though the enterprise scenario that we've used is generic, it gives you an understanding of the underlying principles of how to implement SD-WAN in your network. In addition, this use case demonstrates how the CSO GUI simplifies the implementation of SD-WAN and demonstrates CSO's powerful secure SD-WAN capabilities.

While the tasks for configuring SD-WAN in your own network depend on the complexity of your network and the functionality that you want to implement, you can use the underlying principles explained in this use case to configure SD-WAN in your own, unique network.

> **NOTE:** In CSO SaaS, there are several tasks that are handled by the Juniper team, such as onboarding a provider hub for OAM connectivity, and SMTP server configuration. If you use the on-premise version of CSO, which means that you install CSO on your own infrastructure, the service provider (SP) administrator must handle these tasks.

WHAT'S NEXT

More Breakout Options—Now that you know how to use an SD-WAN policy intent to implement local breakout, you can use intents to route traffic from specific applications to use local breakout.
You can also use intents to route traffic from specific applications over a Zscaler overlay (cloud breakout), if you have a Zscaler account. For more information, see *Adding Cloud Breakout Settings* in the *Customer Portal User Guide* (available at the CSO Documentation page).

Path-Based Traffic Steering—You can add a path-based traffic steering profile that enables you to specify the path that traffic should take and add an SD-WAN policy intent that references the profile, which enables CSO to reroute traffic from specific applications over the overlay (MPLS or Internet) specified in the profile. For more information, see *Adding Path-Based Steering Profiles* in the *Customer Portal User Guide* (available at the CSO Documentation page).

SLA-Based (Dynamic) Traffic Steering—You can add an SLA-based traffic steering profile that enables you to set SLA criteria (such as latency, packet loss, and jitter) and add an SD-WAN policy intent that references the profile, which enables CSO to dynamically select the path on which to route traffic from specific applications based on the SLA criteria specified in the profile. For more information, see *Adding SLA-Based Steering Profiles* in the *Customer Portal User Guide* (available at the CSO Documentation page).

Appendix

IN THIS SECTION

Supported Devices, and Ports and Protocols to Open

Table 16 lists the enterprise hub and CPE device models that are supported by CSO and the list of ports or protocols that must be opened for these devices.

> **NOTE:** During the site activation process for SRX4100, SRX4200, and vSRX 3.0, you must copy the stage-1 configuration (generated automatically by CSO) to the device, and commit the configuration on the device.

Before you add the enterprise hub site or the on-premise spoke site:

- Connect cables to the device according to your network design, and power on the device. For more information, see the hardware documentation links in Table 16.

  > **NOTE:** We assume that the on-premise spoke (SD-WAN CPE) devices will obtain the DHCP IP address (if DHCP is configured as the address assignment method) and will have Internet connectivity along with DNS resolution, when connected according to the network design.

- Ensure that the NAT and firewall ports and protocols listed in Table 16 are open on the network.
- Ensure that the devices are running the recommended version of Junos OS. For information about the supported Junos OS versions in a CSO release, refer to the CSO Release Notes for that release (available at the CSO Documentation page).
- Before you initiate ZTP for the enterprise hub, ensure that the hub device can connect to CSO.

Table 16: Supported Enterprise Hub and SD-WAN CPE Devices, and NAT and Firewall Ports to Open

Device Model	Supported Site Type	NAT and Firewall Protocols or Ports	WAN Link Ports	Hardware Documentation Links
NFX150	On-premise (SD-WAN) spoke	IP Protocol 50 IP Protocol 51 TCP Port 443 UDP Port 500 TCP and UDP Ports 4500 TCP Port 8060	heth-0-0 heth-0-5 heth-0-2 heth-0-3	NFX150 Chassis
NFX250	On-premise (SD-WAN) spoke	IP Protocol 50 IP Protocol 51 TCP Port 443 UDP Port 500 TCP and UDP Ports 4500 TCP Port 7804 TCP Port 8060	ge-0/0/10 ge-0/0/11 xe-0/0/12 xe-0/0/13	NFX250 Chassis
SRX300 SRX320 SRX340 SRX345	On-premise (SD-WAN) spoke	IP Protocol 50 IP Protocol 51 TCP Port 443 UDP Port 500 TCP and UDP Ports 4500 TCP Port 8060	ge-0/0/0 ge-0/0/1 ge-0/0/2 ge-0/0/3	SRX300 Chassis SRX320 Chassis SRX340 Chassis SRX345 Chassis

Table 16: Supported Enterprise Hub and SD-WAN CPE Devices, and NAT and Firewall Ports to Open *(continued)*

Device Model	Supported Site Type	NAT and Firewall Protocols or Ports	WAN Link Ports	Hardware Documentation Links
SRX550M	On-premise (SD-WAN) spoke	IP Protocol 50 IP Protocol 51 TCP Port 443 UDP Port 500 TCP and UDP Ports 4500 TCP Port 8060	ge-0/0/0 ge-0/0/1 ge-0/0/2 ge-0/0/3	SRX550 HM Chassis
SRX1500	Enterprise hub On-premise (SD-WAN) spoke	IP Protocol 50 IP Protocol 51 TCP Port 443 UDP Port 500 TCP and UDP Ports 4500 TCP Port 8060	ge-0/0/7 ge-0/0/8 xe-0/0/18 xe-0/0/19	SRX1500 Chassis
SRX4100 SRX4200	Enterprise hub On-premise (SD-WAN) spoke	IP Protocol 50 IP Protocol 51 TCP Port 443 TCP Port 500 TCP and UDP Ports 4500 TCP Port 8060	xe-0/0/0 xe-0/0/1 xe-0/0/2 xe-0/0/3	SRX4100 Chassis SRX4200 Chassis

Table 16: Supported Enterprise Hub and SD-WAN CPE Devices, and NAT and Firewall Ports to Open *(continued)*

Device Model	Supported Site Type	NAT and Firewall Protocols or Ports	WAN Link Ports	Hardware Documentation Links
vSRX	Enterprise hub On-premise (SD-WAN) spoke	IP Protocol 50 IP Protocol 51 TCP Port 443 UDP Port 500 TCP and UDP Ports 4500 TCP Port 8060	ge-0/0/0 ge-0/0/1 ge-0/0/2 ge-0/0/3	vSRX Deployment Guides

Additional Documentation

Table 17 lists the additional CSO documentation that you can see for more information about CSO's SD-WAN features.

Table 17: Additional CSO Documentation

Documentation	Link
Deployment Guide	Getting Started section of the CSO Documentation page
Administration Portal User Guide Customer Portal User Guide	User Guides section of the CSO Documentation page
Release Notes	Release Notes section of the CSO Documentation page
Monitoring and Troubleshooting Guide	System Administration section of the CSO Documentation page