

Contrail Service Orchestration Quick Start Guide

Published
2020-11-20

Release
5.4.0

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Contrail Service Orchestration Quick Start Guide
Release 5.4.0
Copyright © 2020 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <https://support.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About the Documentation | iv

Documentation and Release Notes | iv

Documentation Conventions | iv

Documentation Feedback | vii

Requesting Technical Support | vii

Self-Help Online Tools and Resources | viii

Creating a Service Request with JTAC | viii

1

Quick Start Guide

Quick Start Guide for Contrail Service Orchestration, Release 5.4.0 | 10

2

SD-WAN

SD-WAN Sites | 12

Add an Enterprise Hub Site for SD-WAN Deployments | 12

Add an SD-WAN On-Premises Spoke Site | 16

3

Next Generation Firewall

Next-Generation Firewall Sites | 24

Add an On-Premises Spoke Site for Next Generation Firewall | 24

4

Tenant Management

Add a Tenant | 29

5

Provider Hub

Add a Provider Hub (DATA_ONLY Capability) | 31

6

Device Activation

Activate a Device | 36

About the Documentation

IN THIS SECTION

- Documentation and Release Notes | iv
- Documentation Conventions | iv
- Documentation Feedback | vii
- Requesting Technical Support | vii

This document provides information about the essential steps for an enterprise (tenant) administrator or a managed service provider (OpCo) administrator to quickly get started with Contrail Service Orchestration.

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <https://www.juniper.net/documentation/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <https://www.juniper.net/books>.

Documentation Conventions

[Table 1 on page v](#) defines notice icons used in this guide.

Table 1: Notice Icons







Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page v defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i> >;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

GUI Conventions

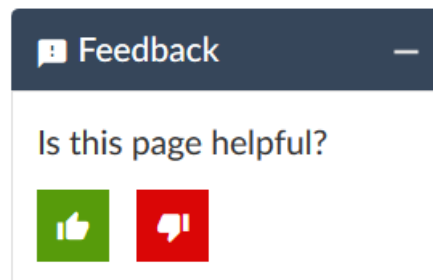
Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are

covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://entitlementsearch.juniper.net/entitlementsearch/>

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://myjuniper.juniper.net>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <https://support.juniper.net/support/requesting-support/>.

1

CHAPTER

Quick Start Guide

Quick Start Guide for Conrail Service Orchestration, Release 5.4.0 | **10**

Quick Start Guide for Contrail Service Orchestration, Release 5.4.0

Contrail Service Orchestration (CSO) Release 5.4.0 is a Juniper Networks-hosted public cloud-based Software as a Service (SaaS) solution.

This topic lists the essential steps for an enterprise (tenant) administrator or a managed service provider (OpCo) administrator to quickly get started with Contrail Service Orchestration. For details about CSO administrator roles, see [CSO documentation](#).

After you receive the account activation credentials e-mail, start with the following steps:

1. Log in to the CSO portal by using the link provided in the activation mail.
2. If you are an OpCo administrator setting up a tenant, perform the following tasks:
 1. [Add one or more tenants on page 29](#)
 2. Optionally, "[Add a Provider Hub \(DATA_ONLY Capability\)](#)" on [page 31](#)
3. If you are a tenant administrator add one or more on-premises spoke sites to enable the following services:
 - [SD-WAN on page 12](#)
 - [Next-Generation Firewall on page 24](#)

2

CHAPTER

SD-WAN

SD-WAN Sites | 12

SD-WAN Sites

A typical SD-WAN site topology includes an on-premises spoke site and a hub site. A hub site can be an enterprise hub site, which is an SD-WAN site that is used to carry site-to-site traffic between on-premises spoke sites and to break out backhaul (central breakout) traffic from on-premises spoke sites.

An on-premises spoke site represents an endpoint that is part of a customer premises equipment (CPE) at some physical location such as a branch office or a point-of-sale (PoS) location. Typically, these points are connected using overlay connections to hub sites.

You can [“Add an Enterprise Hub Site for SD-WAN Deployments” on page 12](#) and one or more of the following on-premise spoke sites for SD-WAN:

- [SD-WAN On-Premise Spoke Site on page 16](#)

Add an Enterprise Hub Site for SD-WAN Deployments

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 (central breakout) traffic from on-premise spoke sites.

To add an enterprise hub:

1. On the Sites page (**Resources > Site Management**) of the CSO portal, click **Add**, and select **Enterprise Hub**.

The **Add enterprise hub for *Tenant-Name*** page appears.

2. Complete the configuration settings according to the guidelines provided in [Table 3 on page 12](#).
3. Click **OK**.

When the site is successfully created, the Site Status on the Sites page changes to Provisioned.

If you did not enter serial number while creating the enterprise hub site, you must manually enter the serial number after adding the enterprise hub site, in order to activate the site. See *Add Enterprise Hubs with SD-WAN Capability* for more information.

Table 3: Enterprise Hub Site Settings

Field	Description
General	

Table 3: Enterprise Hub Site Settings (*continued*)

Field	Description
Site Name	Enter a unique name for the site. You can use alphanumeric characters and hyphen (-); the maximum length is 32 characters.
Site Capabilities	SD-WAN capability is selected by default. You cannot clear the selection.
WAN	
Device Series	Select the device series to which the CPE device belongs—SRX, NFX150, or NFX250.
Device Template	Select a device template for the selected device series. The device template contains information for configuring a device.
Serial Number	Enter the serial number of the CPE device. You can also add the enterprise hub site but activate the site later. If you do not enter the serial number of the CPE device when creating the enterprise hub site, you must enter it while activating the site, using the Activate Site link. See <i>Add Enterprise Hubs with SD-WAN Capability</i> for more information.
Auto Activate	If the selected device template supports auto authorization, Auto Activate is enabled. When Auto Activate is enabled, zero-touch provisioning of the device is automatically triggered when the site is added. The Activation Code field appears if the selected device template does not support auto authorization or if you disable the Auto Activate option. In such cases, specify the activation code of the device to manually activate a device. For information about manually activating a device, see “Activate a Device” on page 36 .
IP Prefix	Enter the IPv4 prefix to be used for the management network. This IP address must be unique across the entire management network. <ul style="list-style-type: none"> For NFX150 and NFX250 devices, if the USE_SINGLE_SSH_TO_NFX parameter is disabled in the device template, then enter the IP address prefix as /29 or lower based on the number of VNFs. For all other devices, enter the IP address prefix as /32.
WAN Links	

Table 3: Enterprise Hub Site Settings (*continued*)

Field	Description
WAN_0	<p>This field is enabled by default.</p> <p>You can configure up to 4 WAN links as required.</p>
Link Type	<p>Select whether the link would be an MPLS link or Internet link.</p> <p>NOTE: If the enterprise hub and the SD-WAN branch site are not in the same network, that is if these devices are not directly reachable, select one link as Internet and assign a public IP to the Internet-type link.</p>
Egress Bandwidth	<p>Enter the maximum bandwidth, in Mbps, allowed on the WAN link.</p> <p>Range: 1 through 10,000.</p>
Address Assignment	<p>Select the method of assigning an IP address to the WAN link—DHCP or STATIC.</p> <p>If you select STATIC, you must provide the IP address prefix and the gateway address for the WAN link.</p>
Static IP Prefix	<p>If you configured the address assignment method as STATIC, enter the IP address prefix of the WAN link.</p> <p>NOTE: If the enterprise hub and the SD-WAN branch site are not in the same network, assign a public IP to the Internet-type link</p>
Gateway IP Address	<p>If you configured the address assignment method as STATIC, enter the IP address of the gateway of the WAN service provider.</p>
Advanced Settings	
Use For Fullmesh	<p>Click the toggle button to specify whether the WAN link can be a part of a full mesh topology.</p> <p>A site can have a maximum of three links enabled for meshing.</p>
Add LAN Segment	
Name	<p>Enter a name for the LAN segment.</p> <p>The name for a LAN segment should be a unique string of alphanumeric characters and some special characters (. -). No spaces are allowed and the maximum length is 15 characters.</p>

Table 3: Enterprise Hub Site Settings (*continued*)

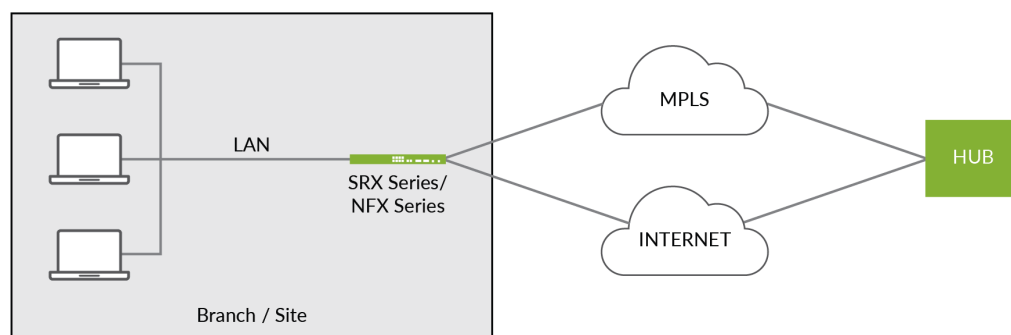
Field	Description
Type	<p>Select the type of LAN segment:</p> <ul style="list-style-type: none"> • Directly Connected—Indicates that the LAN segment is directly connected to the site. This is the default. • Dynamic Routed—Indicates that the LAN segment is not directly connected to the site and is reachable by using a dynamic route. If you select this option, you must specify the dynamic routing information.
Department	<p>Select a department to which the LAN segment is to be assigned.</p> <p>Alternatively, click the Create Department link to create a new department and assign the LAN segment to it. See <i>Add a Department</i> for details.</p> <p>You group LAN segments as departments for ease of management and for applying policies at the department-level. For LAN segments that are dynamically routed, you can assign only a data center department.</p>
Gateway Address/Mask	Enter a valid gateway IP address and mask for the LAN segment; for example, 192.0.2.8/24.
CPE Ports	Select the ports from the Available column and click the right-arrow to move the ports to the Selected column.

SEE ALSO

[Add an SD-WAN On-Premises Spoke Site](#) | 16

Add an SD-WAN On-Premises Spoke Site

The following illustration shows a simple SD-WAN topology.



Before you add an on-premise spoke site:

- Add an [“enterprise hub site”](#) on page 12.
- Connect cables to the device according to your network design and power on the device.

NOTE:

This task assumes that the device will get DHCP IP address and will have Internet connectivity along with DNS resolution when connected according to the network design.

For more information about connecting the cables and connecting the device to a console, see the documentation for the CPE device as listed in [Table 4 on page 17](#).

- Ensure that ESP protocol traffic is allowed on the network.
- Ensure that the ports listed in [Table 4 on page 17](#) are open on the network.

NOTE: Ensure that the devices are running the recommended version of Junos OS. For information about the supported Junos OS versions, see the *Release Notes* for that release.

Table 4: CPE Devices, Port Information, and Documentation Links

Device Model	NAT/Firewall Ports	CPE WAN Link Ports	Hardware Documentation
SRX4x000 devices	50	xe-0/0/0	SRX4100
	51	xe-0/0/1	• SRX4100
	53	xe-0/0/2	SRX4200
	123	xe-0/0/3	• SRX4200
	443		
	500		
	4500		
SRX3xx devices, SRX550M, and vSRX devices	50	ge-0/0/0	SRX300
	51	ge-0/0/1	• https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/srx300-chassis.html
	53	ge-0/0/2	
	123	ge-0/0/3	SRX320
	443		• https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/srx320-chassis.html
	500		
	4500		SRX340
			• https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/srx340-chassis.html
			SRX345
			• https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/srx345-chassis.html
			SRX550M
			• https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/srx550-hm-chassis.html

Table 4: CPE Devices, Port Information, and Documentation Links (*continued*)

Device Model	NAT/Firewall Ports	CPE WAN Link Ports	Hardware Documentation
NFX250	50	ge-0/0/10	NFX250 <ul style="list-style-type: none"> https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/nfx250-chassis.html
	51	ge-0/0/11	
	443	xe-0/0/12	
	500	xe-0/0/13	
	514		
	2216		
	3514		
	4500		
	7804		
NFX150	50	heth4	NFX150 <ul style="list-style-type: none"> https://www.juniper.net/documentation/en_US/release-independent/junos/topics/reference/specifications/chassis-nfx150-physical.html
	51	heth5	
	443	heth2	
	500	heth3	
	4500		

- If you are using a GRE-only overlay between an SRX CPE and a hub device, ensure that GRE Traffic is enabled between CPE and the hub device.

To add an on-premises spoke site for SD-WAN:

1. From the Sites page (**Resources > Site Management**) of the CSO portal, click **Add** and select **On-Premises Spoke Site**.

The **Add Site** wizard appears.

2. Complete the settings as explained in [Table 5 on page 19](#).
3. Click **OK** to add the site.

When the site is successfully created, the Site Status in the Sites page changes to Provisioned.

If you did not enter serial number while creating the on-premises spoke site, you must manually enter the serial number after adding the spoke site, in order to activate the site. See *Add an On-Premises Spoke Site with SD-WAN Capability* for more information.

Table 5: SD-WAN On-Premises Spoke Site Settings

Field	Description
General	
Site Name	Enter a unique name for the site. You can use alphanumeric characters and hyphen (-); the maximum length is 32 characters.
Site Capabilities	Select SD-WAN .
Primary Hub	Select an enterprise hub site as the primary hub from the list of available hub sites. If there is only one hub site available, that one is selected by default.
WAN	
Device Series	Select the CPE device.
Device Template	Select a device template for the CPE device.
Serial Number	<p>Enter the serial number of the CPE device.</p> <p>You can also add the on-premises spoke site but activate the site later. If you do not enter the serial number of the CPE device when creating the on-premises spoke site, you must enter it while activating the site, using the Activate Site link.</p> <p>See <i>Add an On-Premises Spoke Site with SD-WAN Capability</i> for more information.</p>
Auto Activate	<p>If the selected device template supports ZTP, Auto Activate is enabled. When Auto Activate is enabled, zero-touch provisioning of the device is automatically triggered when the site is added.</p> <p>The Activation Code field appears if the selected device template does not support ZTP or if you disable the Auto Activate option.</p> <p>In such cases, specify the activation code of the device to manually activate a device. For information about manually activating a device, see “Activate a Device” on page 36.</p>
Link Type	Select whether the link is an MPLS link or Internet link.

Table 5: SD-WAN On-Premises Spoke Site Settings (*continued*)

Field	Description
Access Type	<p>Select the access type for the underlay link:</p> <ul style="list-style-type: none"> • If you've selected Internet as the link type, you can select Ethernet (default), LTE, ADSL, or VDSL as the access type. • If you've selected MPLS as the link type, you can select Ethernet (default) or LTE as the access type. <p>You can select the LTE, ADSL, or VDSL access type only for one WAN link.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • You cannot configure LTE, ADSL, or VDSL as the access type if you are using the Dual SRX and Dual NFX device templates; Ethernet is configured as the access type for the underlay link. • SRX300 does not support LTE and ADSL access types. • On SRX300 line of Services Gateways (except SRX300 devices) and NFX150 devices, the LTE WAN link is supported through a SIM card that is inserted in the SIM slot of the Mini-Physical Interface Module (Mini-PIM). On NFX250 devices, the LTE WAN link is supported through a USB dongle (Vodafone K5160 dongle) that is plugged into the USB port of the CPE device.
PPPoE/PPP	<p>Click the toggle button to enable authenticated address assignment for the WAN link by using PPPoE (Point-to-Point Protocol over Ethernet) or PPP (Point-to-Point Protocol). By default, this toggle button is disabled.</p> <p>PPPoE works with Ethernet, ADSL, and VDSL access types while PPP works with the LTE access type.</p> <p>NOTE: This toggle button is not available for Internet links with LTE as the access type.</p> <p>If you've enabled this toggle button, you must specify the PPPoE or PPP parameters (username, password, and authentication protocol) for the PPPoE or PPP server, respectively. The PPPoE or PPP server assigns an IP address to the WAN link after successful authentication.</p> <p>If you've disabled this toggle button, select a method (DHCP or STATIC) to assign an IP address to the WAN link from the Address Assignment list.</p>

Table 5: SD-WAN On-Premises Spoke Site Settings (*continued*)

Field	Description
Access Point Name (APN)	<p>If you choose to use a private APN with the current LTE service provider or to use a different LTE service provider, enter the APN for the CPE device (as specified by the service provider).</p> <p>This field is displayed only if you have enabled PPPoE/PPP for MPLS links with LTE as the access type. If you have disabled PPPoE/PPP for these links, CSO uses the default APN settings.</p>
Egress Bandwidth	<p>Specify the maximum bandwidth allocated for the WAN link.</p> <p>NOTE: This option is not available for Internet and MPLS links with LTE access type.</p>
Address Assignment	<p>Specify whether to use DHCP or Static addresses.</p> <p>If you select Static, specify a Static IP Prefix and Gateway IP Prefix.</p> <p>This field is displayed only if you have disabled the PPPoE/PPP toggle button.</p>
Service Provider	Enter the name of the service provider.
Cost per month	Enter the per month cost of the link. This information is used to identify the least expensive link when link switch occurs.
LAN Segment	
Add LAN Segment	Click to add a LAN segment.
Name	Enter a unique name for the LAN segment.
Gateway Address/Mask	Enter a valid gateway IP address and mask for the LAN segment; for example, 192.0.2.8/24.
Department	<p>Select a department from the list; if no department is available, click Create Department and add one.</p> <p>A department is a grouping of LAN segments within a site. You use departments to apply specific policies to LAN segments that are members of a department.</p>
CPE Port	Select at least one CPE port.

After the site is provisioned, you can complete the following tasks as required:

- Upload and install licenses. For example, **Administration > Licenses**.
- Install signatures. For example, **Administration > Signature Database**.
- Add, edit, and deploy an SD-WAN policy. For example, **Configuration > SD-WAN Policy**.
- Create and generate reports. For example, **Reports > Report Definitions > SD-WAN**.
- Monitor alerts and alarms, SLA performance of tenants, and jobs. For example, **Monitor > Jobs**.

For more information about these tasks, see the Contrail Service Orchestration user guide at https://www.juniper.net/documentation/product/en_US/contrail-service-orchestration.

3

CHAPTER

Next Generation Firewall

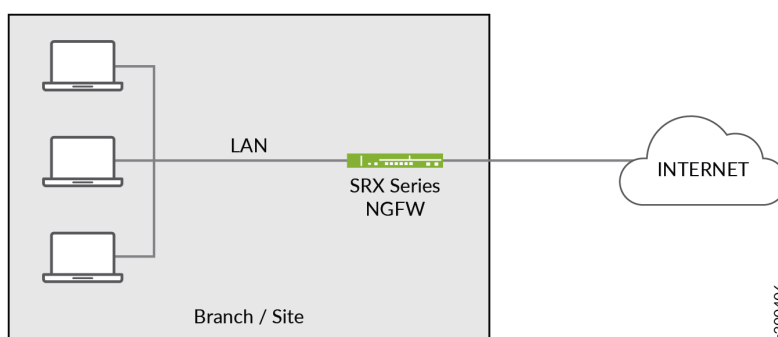
[Next-Generation Firewall Sites](#) | 24

Next-Generation Firewall Sites

You can add a next-generation firewall site to manage a standalone SRX device that is configured as a firewall device. You can also create a next-generation firewall site for branch networks to manage an SRX firewall device. This topic explains how you can, [“Add an On-Premises Spoke Site for Next Generation Firewall” on page 24.](#)

Add an On-Premises Spoke Site for Next Generation Firewall

The following image shows a simple network topology for a standalone next-generation firewall site.



Complete the connections as shown in the topology diagram and power up the device.

This task assumes that the device will get DHCP IP address and will have Internet connectivity along with DNS resolution when connected according to the network design.

NOTE: When you configure the SRX 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 SRX model) for Internet connectivity.

For more information about connecting the cables and connecting a console to the device, see the documentation for the firewall device. Links to the hardware documentation for the supported models are provided in [Table 6 on page 25.](#)

NOTE: Ensure that the devices are running the recommended version of Junos OS. For information about the supported Junos OS versions, see the *Release Notes* for that Release.

Table 6: Next Generation Firewall Devices, Port Information, and Documentation Links

Device Model	NAT/Firewall	Hardware Documentation
SRX3xx devices, SRX550M, SRX1500, SRX4100, and SRX4200	443	SRX340
	444 (not needed for CSO SaaS instances)	<ul style="list-style-type: none"> https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/srx340-chassis.html
	514	SRX345
	6514	<ul style="list-style-type: none"> https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/srx345-chassis.html
	7804	SRX550M
	8060 (needed if using PKI authentication to validate CRL)	<ul style="list-style-type: none"> https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/srx550-hm-chassis.html
		SRX1500
		<ul style="list-style-type: none"> https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/srx1500-chassis.html
		SRX4100
		<ul style="list-style-type: none"> https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/srx4100-chassis.html
		SRX4200
		<ul style="list-style-type: none"> https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/srx4200-chassis.html

To add a next-generation firewall site:

1. From the Sites page (**Resources > Site Management**) of the CSO portal, click **Add** and select **On-Premise Spoke Site**.

The **Add Site** wizard appears.

2. Complete the configuration as explained in [Table 7 on page 26](#).
3. Click **Next** to review the settings and then, click **OK** to add the site.

When the site is successfully created, the Site Status in the Sites page changes to Provisioned.

If you did not enter serial number while creating the next-generation firewall site, you must manually enter the serial number after adding the firewall site, in order to activate the site. See *Add a Standalone Next Generation Firewall Site* for more information.

Table 7: SD-WAN On-Premises Spoke Site Settings

Field	Description
General	
Site Name	Enter a unique name for the site. You can use alphanumeric characters and hyphen (-); the maximum length is 32 characters.
Site Capabilities	Select Next Gen Firewall .
WAN	
Serial Number	<p>Enter the serial number of the device.</p> <p>You can also add the Next-Generation Firewall site but activate the site later. If you choose to not enter the serial number of the CPE device when creating the Next-Generation Firewall site, you must enter it while activating the site, using the Activate Site link.</p> <p>See <i>Add a Standalone Next Generation Firewall Site</i> for more information.</p>
Auto Activate	Auto Activate is enabled by default. When Auto Activate is enabled, the device activation is automatically triggered when the site is added. The Activation Code field appears if you disable the Auto Activate option. In such cases, specify the activation code of the device to manually activate a device. For information about manually activating a device, see “Activate a Device” on page 36 .
Zero Touch Provisioning	Zero Touch Provisioning is enabled by default. When Zero Touch Provisioning is enabled, zero-touch provisioning of the device is automatically triggered when the site is added. Note that the SRX device must support phone home client for ZTP to work. If the device does not support phone home client, disable Zero Touch Provisioning and manually copy-paste the stage-1 configuration from the device CLI.

After you add the site, you can complete the following tasks as required:

NOTE: The device must be activated before you install licenses or signatures, or deploy policies.

- Upload and install licenses. For example, **Administration > Licenses**.
- Install signatures. For example, **Administration > Signature Database**.
- Add, modify, and deploy firewall policies. For example, **Configuration > Firewall Policy**.
- Monitor alerts, alarms, and jobs. For example, **Monitor > Jobs**.

For more information about these tasks, see the Contrail Service Orchestration documentation at https://www.juniper.net/documentation/product/en_US/contrail-service-orchestration.

4

CHAPTER

Tenant Management

[Add a Tenant](#) | **29**

Add a Tenant

To add a tenant to the OpCo portal, follow these steps:

1. From the CSO portal, go to the **Tenants** page and click **+**.

The Add Tenant wizard appears.

2. Configure the settings as explained in [Table 8 on page 29](#).

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

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

An Add Tenant job is created, and when the job is successfully completed, the tenant is listed in the Tenants page. When a new tenant is added, an account activation e-mail is sent to the tenant.

Table 8: Add Tenant Settings

Field Name	Description
Name	Enter a unique name for the tenant. The name can contain alphanumeric characters and underscore and should not exceed 32 characters.
First Name	Enter the first name of the tenant administrator user.
Last Name	Enter the last name of the tenant administrator user.
Username (Email)	Enter the e-mail address of the tenant administrator user to set as the user name for the tenant administrator.
Roles	Select one or more of the available roles to assign that to the tenant administrator user.
Service for Tenant	<p>Select one or more of the following services that the tenants can manage by using CSO:</p> <ul style="list-style-type: none"> • SD-WAN—Enables tenants to manage sites that have up to four WAN links with intelligent, SLA-based traffic routing among the WAN links. • Next-Generation Firewall—Enables the tenants to manage next generation firewall devices and firewall policies. <p>When tenants add sites, they can implement any of the services that you selected.</p>

5

CHAPTER

Provider Hub

Add a Provider Hub (DATA_ONLY Capability) | 31

Add a Provider Hub (DATA_ONLY Capability)

You can add an SRX Series services gateway or a vSRX instance as a provider hub device. The device template that is currently supported for provider hub devices is SRX as SD-WAN Hub. You can configure a provider hub with the DATA_ONLY capability.

Ensure that the ports listed are open on the provider hub device:

- For communication with an OAM hub or CSO—50, 51, 443, 500, and 4500
- For DNS resolution and NTP—53 and 123

To add a provider hub device with DATA_ONLY capability:

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

The Provider Hub Devices page appears.

2. Click the add icon (+).

The Add Provider Hub page appears.

3. Complete the configuration according to the guidelines provided in [Table 9 on page 31](#).

4. Click **Ok**. If you want to discard your changes, click **Cancel** instead.

If you click **Ok**, the provider hub device is added. The information about the new provider hub device appears on the Provider Hub Devices page.

Table 9: Fields on the Add Provider Hub Page

Field	Description
Name	<p>Enter the name of the provider hub device.</p> <p>You can use alphanumeric characters, including special character(-). The maximum length is 15 characters.</p> <p>Example: SRX-hub</p>
Management Region	<p>Displays the regional server with which the device communicates. The management region name is populated based on the information from the device template.</p> <p>Example: regional</p>

Table 9: Fields on the Add Provider Hub Page (*continued*)

Field	Description
POP	<p>Select the POP where the hub device needs to be added.</p> <p>Example: pop_blue</p>
Site Capability	<p>Select the site capability of the provider hub device as DATA_ONLY, which indicates that the hub transmits only the data traffic.</p> <p>A secure connection is established between the provider hub with data capability and the provider hub (with OAM capability) that are owned and managed by the Juniper Network team that hosts CSOaaS.</p>
Authentication Type	Select the authentication method—Preshared Key (PSK) or Public Key Infrastructure (PKI).
Advanced Configuration	
Name Server IP List	<p>Specify one or more IPv4 addresses of the DNS server. To enter more than one DNS server address, type the address, press Enter, and then type the next address, and so on.</p> <p>DNS servers are used to resolve hostnames into IP addresses.</p>
NTP Server	<p>Specify the fully qualified domain names (FQDNs) or IP addresses of one or more NTP servers.</p> <p>Example: ntp.example.net</p> <p>The site must have DNS reachability to resolve the FQDN during site configuration.</p>
Select Timezone	Select the time zone of the site.
Device Template	
Device Series	Select the device series to which the provider hub belongs—SRX.
Device Template	<p>Select a device template for the selected device series.</p> <p>The device template contains information for configuring a device.</p>
Device Information	

Table 9: Fields on the Add Provider Hub Page (*continued*)

Field	Description
Serial Number	<p>Enter the serial number of the provider hub device.</p> <p>The serial number is a 12-digit number present on the rear panel of the device. Serial numbers are case-sensitive.</p> <p>You can also add the provider hub site but activate the site later. If you do not enter the serial number of the device when creating the provider hub site, you must enter it while activating the site, using the Activate Site link.</p>
Auto Activate	<p>Click the toggle button to enable or disable automatic activation of the provider hub device.</p> <p>When you enable this field, zero-touch provisioning (ZTP) of the provider hub device is automatically triggered after the site is added to CSO.</p> <p>The device template that you select determines whether this option is enabled or disabled by default.</p>
Boot image	<p>Select the boot image from the drop-down list if you want to upgrade the image for the provider hub device.</p> <p>The boot image is the latest build image uploaded to the image management system. The boot image is used to upgrade the device when the CSO starts the ZTP process.</p> <p>If the boot image is not provided, then the device skips the procedure to upgrade the device image. The boot image (NFX or SRX) is populated based on the device template that you have selected while creating a site. .</p>
Management Connectivity	
Loopback IP Prefix	<p>By default, CSO assigns the IPv4 address prefix for the loopback interface on the device. If you prefer to use a specific loopback address contact the Juniper Networks team.</p>
WAN Links	

Table 9: Fields on the Add Provider Hub Page (*continued*)

Field	Description
WAN_0	Select a WAN link to enable it. After selecting the link, specify the following information: <ul style="list-style-type: none"> • WAN Interface—Displays the interface name configured in the device template. You cannot modify this field. Example: ge-0/0/0 • Link Type—Select the link type (MPLS or Internet) configured in the device template. Example: Internet • Address Assignment—Select STATIC to assign a static IP address. • Static IP Prefix—Enter a private IPv4 address from the subnet • Gateway IP Address—Enter the gateway IP address of the default route. • Data VLAN ID—(Optional) Enter the VLAN ID that is associated with the data link. A data VLAN identifier is an integer in the range 0–65,535. Example: 201
WAN_1	
WAN_2	
WAN_3	

After you add the provider hub device:

- If you have enabled the Auto Activate field, the provider hub device gets automatically activated.
- If you have disabled the Auto Activate field, select the provider hub device on the **Resources > Provider Hub Devices** page and click **Activate Device**.

During activation, the provider hub device is discovered and the required details are stored in CSO.

6

CHAPTER

Device Activation

Activate a Device | 36

Activate a Device

To manually activate a device, follow these steps:

1. From the Customer Portal, click **Sites**.

The **Sites** page appears.

2. Click the site with which the device that you want to activate is associated.

The *Site* page for the selected site appears.

3. Go to the **Devices** tab of the *Site* page.

4. Select the device that you want to activate and click **Activate Device**.

The **Activate Device** page appears.

5. On the **Activate Device** page, enter the activation code for the device. The activation code must match the activation code that was provided during the site addition workflow.

6. Click **Next**.

The progress of the device activation task is displayed.

7. Click **OK** when the device activation is complete.

The sites page appears. The status of the device is set to PROVISIONED if the device is successfully activated. Once the device is provisioned, you can use the device to route traffic.

RELATED DOCUMENTATION

[Add an SD-WAN On-Premises Spoke Site | 16](#)

[Add an On-Premises Spoke Site for Next Generation Firewall | 24](#)