JUNIPER NETWORKS | Engineering Simplicity

Contrail Service Orchestration Quick Start Guide

Published
2020-11-05

Release
5.1.1

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 5.1.1
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 | v

Documentation and Release Notes | **v**

Documentation Conventions | **v**

Documentation Feedback | **viii**

Requesting Technical Support | **viii**

- Self-Help Online Tools and Resources | **ix**
- Creating a Service Request with JTAC | **ix**

1 **Quick Start Guide**

Quick Start Guide for Contrail Service Orchestration, Release 5.1.1 | 11

2 **SD-WAN**

SD-WAN Sites | 13

- Add an Enterprise Hub Site for SD-WAN Deployments | **13**
- Add an Enterprise Hub Site with SD-WAN and LAN Capabilities | **16**
- Add an SD-WAN On-Premise Spoke Site | **21**
- Add an SD-WAN On-Premise Spoke Site with LAN for Branch Networks | **26**

3 **Hybrid WAN**

Add an On-Premise Spoke Site with Hybrid WAN Capability | 34

4 **Next Generation Firewall**

Next-Generation Firewall Sites | 40

- Add an On-Premise Spoke Site for Next Generation Firewall | **40**
- Add an On-Premise Spoke Site with Next-Generation Firewall and LAN Capabilities | **43**

5 **LAN**

LAN Sites | 49

- Add an On-Premise Spoke Site for LAN | **50**
- Add an Enterprise Hub Site with SD-WAN and LAN Capabilities | **59**
- Add LAN Capabilities to an Existing Site by Using a Switch | **64**

Enabling Integration with Mist Access Points | 66

6 **Tenant Management**

Add a Tenant | 68

7 **SMTP Configuration**

Configure SMTP Settings | 71

8 **Provider Hub**

Add a Provider Hub (DATA_ONLY Capability) | 73

9 **Device Activation**

Activate a Device | 78

About the Documentation

IN THIS SECTION

- Documentation and Release Notes | v
- Documentation Conventions | v
- Documentation Feedback | viii
- Requesting Technical Support | viii

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 vi 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 vi 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`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*

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

Convention	Description	Examples
Italic text like this	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** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• 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 *metric*>;**
| (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** **(*string1* | *string2* | *string3*)**
# (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 [*community-ids*]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		

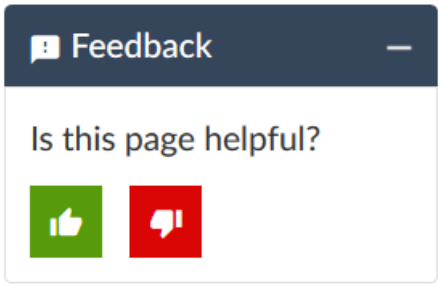
Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• 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/.

CHAPTER 1

Quick Start Guide

Quick Start Guide for Contrail Service Orchestration, Release 5.1.1

Contrail Service Orchestration (CSO) Release 5.1.1 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. Configure SMTP settings on page 71
   2. Add one or more tenants on page 68
   3. Optionally, "Add a Provider Hub (DATA_ONLY Capability)" on page 73
3. If you are a tenant administrator add one or more on-premise spoke sites to enable the following services:
   - SD-WAN on page 13
   - Hybrid WAN on page 34
   - Next-Generation Firewall on page 40
   - LAN on page 49

2

CHAPTER

SD-WAN

SD-WAN Sites | **13**

SD-WAN Sites

A typical SD-WAN site topology includes an on-premise 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-premise spoke sites and to break out backhaul (central breakout) traffic from on-premise spoke sites.

An on-premise spoke site represents an endpoint that is part of a customer premise 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.

CSO supports SD-WAN sites that contain an EX Series switch for the branch network along with the CPE device.

You can "Add an Enterprise Hub Site for SD-WAN Deployments" on page 13 and one or more of the following on-premise spoke sites for SD-WAN:

- SD-WAN On-Premise Spoke Site on page 21
- SD-WAN On-Premise Spoke Site with LAN for Branch Networks on page 26

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.

> **NOTE:** You can add enterprise hubs only if the SD-WAN mode is set to real-time optimized.

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 14.

3. Click **OK**.

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

Table 3: Enterprise Hub 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 10 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.
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 78. **NOTE:**
IP Prefix	Enter the IPv4 prefix to be used for the management network. This IP address must be unique across the entire management network. • 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	
WAN_0	This field is enabled by default. You can configure up to 4 WAN links as required.

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

Field	Description
Link Type	Select whether the link would be an MPLS link or Internet link. **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.
Egress Bandwidth	Enter the maximum bandwidth, in Mbps, allowed on the WAN link. Range: 1 through 10,000.
Address Assignment	Select the method of assigning an IP address to the WAN link—DHCP or STATIC. If you select STATIC, you must provide the IP address prefix and the gateway address for the WAN link.
Static IP Prefix	If you configured the address assignment method as STATIC, enter the IP address prefix of the WAN link. **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
Gateway IP Address	If you configured the address assignment method as STATIC, enter the IP address of the gateway of the WAN service provider.
Advanced Settings	
Use For Fullmesh	Click the toggle button to specify whether the WAN link can be a part of a full mesh topology. A site can have a maximum of three links enabled for meshing.
Add LAN Segment	
Name	Enter a name for the LAN segment. 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.

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

Field	Description
Type	Select the type of LAN segment: • 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	Select a department to which the LAN segment is to be assigned. Alternatively, click the **Create Department** link to create a new department and assign the LAN segment to it. See *Adding a Department* for details. 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.
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.

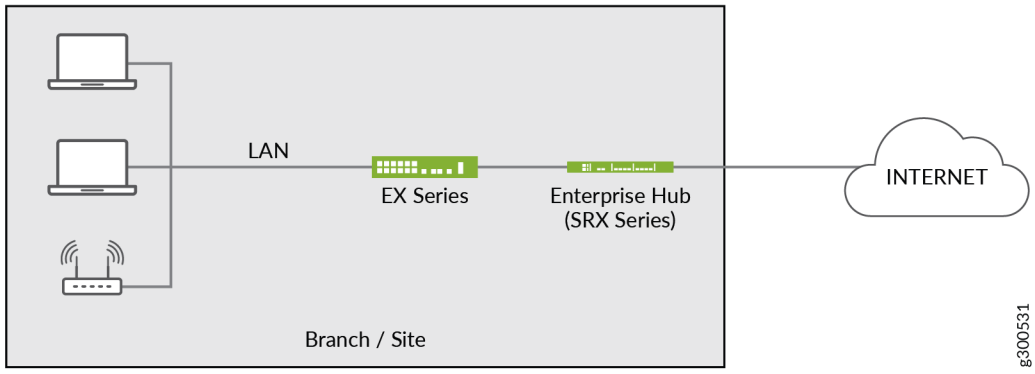
SEE ALSO

Add an SD-WAN On-Premise Spoke Site | 21
Add an SD-WAN On-Premise Spoke Site with LAN for Branch Networks | 26

Add an Enterprise Hub Site with SD-WAN and LAN Capabilities

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. You can add an EX Series switch for branch network as part of the enterprise hub site. The following illustration shows a

simple topology that contains an enterprise hub and an EX Series switch.



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 4 on page 18.

3. Click **OK**.

   The site activation job is initiated and the Site Activation: Site-Name page appears displaying the progress of the steps executed for activating the devices in the site.

4. - If the Zero Touch Provisioning (ZTP) toggle button is enabled (default), CSO pushes the stage-1 and stage-2 configurations and provisions the switch.

     This process occurs immediately after the activation process, for which you entered the activation code or selected auto-activation.

     > **NOTE:** Stage-1 configuration is the initial configuration that allows basic connectivity to a device, which is pushed to the device.
     >
     > The configuration that is pushed to the device after it has connected to CSO is called stage-2 configuration.

   - If you disabled the Zero Touch Provisioning (ZTP) toggle button, you must manually configure the stage-1 configuration (as provided by CSO) on the switch.

To manually configure the stage-1 configuration:

a. On the **Site Activation: *Site-Name*** page, the **Click to copy stage-1 configuration** link appears after the Prestage Device step completes successfully.

b. Click the **Click to copy stage-1 configuration** link.

   The stage-1 configuration page appears displaying the stage-1 configuration to be copied to the EX Series device.

c. Copy the stage-1 configuration and log in to the console of the EX Series switch.

d. Enter the configuration mode, paste, and commit the configuration.

   After the stage-1 configuration is committed, the switch has the outbound SSH configuration to connect with CSO.

   CSO then provisions the switch.

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

Table 4: Enterprise Hub 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 10 characters.
Site Capabilities	SD-WAN capability is selected by default. You cannot clear the selection. If you want to include LAN capabilities in the enterprise hub site, select **LAN**.
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.

Table 4: Enterprise Hub Site Settings *(continued)*

Field	Description
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 78. **NOTE:**
IP Prefix	Enter the IPv4 prefix to be used for the management network. This IP address must be unique across the entire management network. • 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	
WAN_0	This field is enabled by default. You can configure up to 4 WAN links as required.
Link Type	Select whether the link would be an MPLS link or Internet link.
Egress Bandwidth	Enter the maximum bandwidth, in Mbps, allowed on the WAN link. Range: 1 through 10,000.
Address Assignment	Select the method of assigning an IP address to the WAN link—DHCP or STATIC. If you select STATIC, you must provide the IP address prefix and the gateway address for the WAN link.
Static IP Prefix	If you configured the address assignment method as STATIC, enter the IP address prefix of the WAN link.
Gateway IP Address	If you configured the address assignment method as STATIC, enter the IP address of the gateway of the WAN service provider.
Advanced Settings	

Table 4: Enterprise Hub Site Settings *(continued)*

Field	Description
Use For Fullmesh	Click the toggle button to specify whether the WAN link can be a part of a full mesh topology. A site can have a maximum of three links enabled for meshing.
LAN **NOTE:** This tab is enabled only if you select **LAN** from the Site Capabilities options in General Settings.	
Device Profile	
Device Name	Enter a name for the switch. You can use alphanumeric characters and hyphen (-). The maximum length allowed is 15 characters.
Device Type	Select the type of switch—EX2300, EX3400, or EX4300 When you change the default device type, a carousel for device template appears.
Device Model	Select the model for the switch you specified in the Device Type. The models vary in the number and type of ports the switch contains. For example, If you selected EX3400, select a model such as EX3400-24P, EX3400-48P, EX3400-24T among others.
CPE Settings	
Trunk Ports	Select at least two trunk ports on the CPE device to connect with the switch. The trunk ports are used for carrying the following: • LAN traffic between the switch and the CPE • Management traffic for in-band management of the switch.
Switch Management Subnet	Specify the subnet that the DHCP can use to assign IP addresses to the switch and the access devices connected to the switch.
Switch Details	
Serial Number	Specify the serial number of the switch.

Table 4: Enterprise Hub Site Settings *(continued)*

Field	Description
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 78. **NOTE:** You must physically connect the switch to the CPE and power it on for the switch to be automatically activated when the auto activate option is enabled.

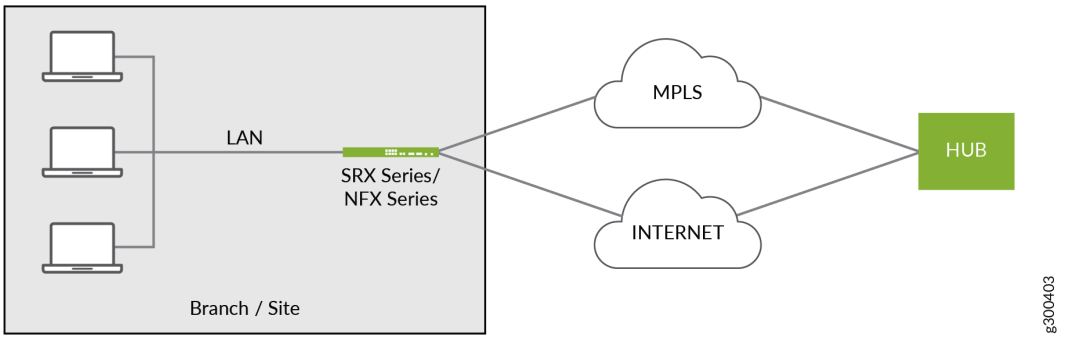
SEE ALSO

On-premise spoke site for LAN | 50

Next-generation firewall site with LAN for branch networks | 43

Add an SD-WAN On-Premise 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 13.
- 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 5 on page 22. .

- Ensure that ESP protocol traffic is allowed on the network.
- Ensure that the ports listed in Table 5 on page 22 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 in a release, see the *Release Notes* for that release..

Table 5: CPE Devices, Port Information, and Documentation Links

Device Model	NAT/Firewall Ports	CPE WAN Link Ports	Hardware Documentation
SRX4x000 devices	443 500 4500	**xe-0/0/0** **xe-0/0/1** **xe-0/0/2** **xe-0/0/3**	SRX4100 • SRX4100 SRX4200 • SRX4200

Table 5: CPE Devices, Port Information, and Documentation Links *(continued)*

Device Model	NAT/Firewall Ports	CPE WAN Link Ports	Hardware Documentation
SRX3xx devices, SRX550M, and vSRX devices	443 500 4500	**ge-0/0/0** **ge-0/0/1** **ge-0/0/2** **ge-0/0/3**	SRX300 • https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/srx300-chassis.html SRX320 • https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/srx320-chassis.html 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
NFX250	443 500 4500 7804	**ge-0/0/10** **ge-0/0/11** **xe-0/0/12** **xe-0/0/13**	NFX250 • https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/nfx250-chassis.html

Table 5: CPE Devices, Port Information, and Documentation Links *(continued)*

Device Model	NAT/Firewall Ports	CPE WAN Link Ports	Hardware Documentation
NFX150	443 500 4500	**heth4** **heth5** **heth2** **heth3**	NFX150 • https://www.juniper.net/documentation/en_US/release-independent/junos/topics/reference/specifications/chassis-nfx150-physical.html

- 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-premise spoke site for SD-WAN:

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 settings as explained in Table 6 on page 24.

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

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

   Table 6: SD-WAN On-Premise 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 10 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.

Table 6: SD-WAN On-Premise Spoke Site Settings *(continued)*

Field	Description
Serial Number	Enter the serial number of the CPE device.
Auto Activate	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. The **Activation Code** field appears if the selected device template does not support ZTP 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 78.
Link Type	Specify whether the link is an Internet link or an MPLS link. If you select **Internet** as the Link Type, select the Access Type. The access type options available for Internet link are: **Ethernet**, **LTE**, **ADSL**, and **VDSL**.
Egress Bandwidth	Specify the maximum bandwidth allocated for the WAN link.
Address Assignment	Specify whether to use DHCP or Static addresses. If you select Static, specify a Static IP Prefix and Gateway IP Prefix.
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 andmask for the LAN segment; for example, 192.0.2.8/24.
Department	Select a department from the list; if no department is available, click Create Department and add one. 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.

Table 6: SD-WAN On-Premise Spoke Site Settings *(continued)*

Field	Description
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**.

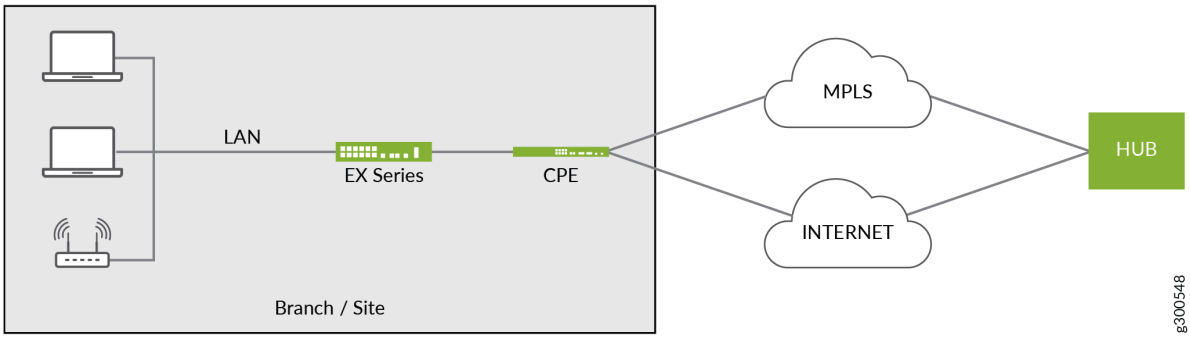
For more information about these tasks, see the Contrail Service Orchestration user guide at https://www.juniper.net/ documentation/product/en_US/contrail-service-orchestration.

SEE ALSO

Add an SD-WAN On-Premise Spoke Site with LAN for Branch Networks | **26**

Add an SD-WAN On-Premise Spoke Site with LAN for Branch Networks

The following image illustrates a simple network topology that contains a CPE and an EX Switch. The CPE can be an SRX Series device or an NFX250 device.



After you connect the devices as shown in the topology diagrams and power on the devices, log into the CSO portal and add an SD-WAN site.

Before you add an on-premise spoke site:

- Add an “enterprise hub site” on page 13.
- Connect cables to the device according to your network design and power on the device.

  NOTE:

  This task assumes that the CPE 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 to the device console, see the documentation for the CPE device. The port numbers including the WAN link ports for each of the supported CPE device models and the NAT and firewall ports that need to be enabled and links to the hardware documentation for the supported models are provided in Table 7 on page 27.
- Ensure that ESP protocol traffic is allowed on the network.
- Ensure that the ports listed in Table 7 on page 27 are open.

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

Table 7: CPE Devices, Port Information, and Documentation Links

Device Model	NAT/Firewall Ports	CPE WAN Link Ports	Hardware Documentation
SRX4x00 devices	443 500 4500	**xe-0/0/0** **xe-0/0/1** **xe-0/0/2** **xe-0/0/3**	SRX4100 • https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/srx4100-chassis.html SRX4200 • https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/srx4200-chassis.html

Table 7: CPE Devices, Port Information, and Documentation Links *(continued)*

Device Model	NAT/Firewall Ports	CPE WAN Link Ports	Hardware Documentation
SRX3xx devices, SRX550M, and vSRX devices	443 500 4500	**ge-0/0/0** **ge-0/0/1** **ge-0/0/2** **ge-0/0/3**	SRX300 • https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/srx300-chassis.html SRX320 • https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/srx320-chassis.html 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
NFX250	443 500 4500 7804	**ge-0/0/10** **ge-0/0/11** **xe-0/0/12** **xe-0/0/13**	NFX250 • https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/nfx250-chassis.html
LAN Switches			
EX2300	—	—	https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/ex2300-system-overview.html
EX3400	—	—	https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/ex3400-chassis.html

Table 7: CPE Devices, Port Information, and Documentation Links *(continued)*

Device Model	NAT/Firewall Ports	CPE WAN Link Ports	Hardware Documentation
EX4300	—	—	https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/ex4300-system-overview.html

NOTE:
- Only EX Series devices running 18.4R2.7 firmware support ZTP.
- EX4600 and EX4650 switches do not support Phone-Home client. You must disable ZTP and manually configure the stage-1 configuration on the switches.

- 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 SD-WAN site with a CPE device and a LAN device:

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

   The Add On-premise Spoke Site for *Tenant-Name* page appears.

2. Complete the configuration according to the guidelines provided in Table 8 on page 30.

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

3. Review the configuration from the **Summary** tab and click **OK**.

   (Optional) click the Edit links within the summary to go directly to a specific page of the wizard and modify the configured settings.

   After you click OK, site activation is initiated and the **Site Activation: *Site-Name*** page appears.

4. - If the Zero Touch Provisioning (ZTP) toggle button is enabled (default), CSO pushes the stage-1 and stage-2 configurations and provisions the switch.

     This process occurs immediately after the activation process, for which you entered the activation code or selected auto-activation.

> **NOTE:** Stage-1 configuration is the initial configuration that allows basic connectivity to a device, which is pushed to the device.
>
> The configuration that is pushed to the device after it has connected to CSO is called stage-2 configuration.

- If you disabled the Zero Touch Provisioning (ZTP) toggle button, you must manually configure the stage-1 configuration (as provided by CSO) on the switch.

  To manually configure the stage-1 configuration:

  a. On the **Site Activation: *Site-Name*** page, the **Click to copy stage-1 configuration** link appears after the Prestage Device step completes successfully.

  b. Click the **Click to copy stage-1 configuration** link.

     The stage-1 configuration page appears displaying the stage-1 configuration to be copied to the EX Series device.

  c. Copy the stage-1 configuration and log in to the console of the EX Series switch.

  d. Enter the configuration mode, paste, and commit the configuration.

     After the stage-1 configuration is committed, the switch has the outbound SSH configuration to connect with CSO.

     CSO then provisions the switch.

Table 8: SD-WAN On-Premise 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 10 characters.
Site Capabilities	Select **SD-WAN** and **LAN**.
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	

Table 8: SD-WAN On-Premise Spoke Site Settings *(continued)*

Field	Description
Device Series	Select the CPE device.
Device Template	Select a device template for the CPE device.
Device Name	Enter a unique name for the CPE device.
Serial Number	Enter the serial number of the CPE device.
Auto Activate	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. The **Activation Code** field appears if the selected device template does not support ZTP 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 78.
Link Type	Specify whether the link is an Internet link or an MPLS link. If you select **Internet** as the Link Type, select the Access Type. The access type options available for Internet link are: **Ethernet**, **LTE**, **ADSL**, and **VDSL**.
Egress Bandwidth	Specify the maximum bandwidth allocated for the WAN link.
Address Assignment	Specify whether to use DHCP or static addresses.
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	
Device Name	Enter a unique name for the device.
Device Type	Select the type of the device.
Serial Number	Specify the serial number of the switch.

Table 8: SD-WAN On-Premise Spoke Site Settings *(continued)*

Field	Description
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 78.

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

> **NOTE:** If **Auto Activate** is not enabled for the devices, ensure that device is activated before you install licenses or signatures, or deploy policies.

- If the EX Series switch has Mist access points associated with that, you could integrate the Mist access points with CSO. For more information about integrating Mist access points with CSO, see "Enabling Integration with Mist Access Points" on page 66.
- Upload and install licenses. For example, **Administration** > **Licenses**.
- 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 documentation at https://www.juniper.net/ documentation/product/en_US/contrail-service-orchestration.

SEE ALSO

Add an SD-WAN On-Premise Spoke Site | 21

3
CHAPTER

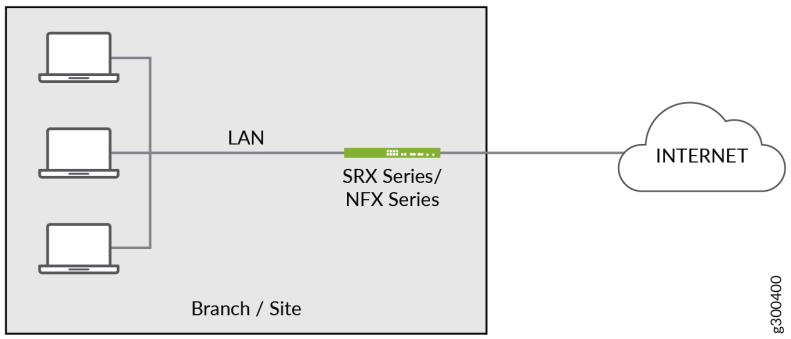
Hybrid WAN

Add an On-Premise Spoke Site with Hybrid WAN Capability | 34

Add an On-Premise Spoke Site with Hybrid WAN Capability

You add an on-premise spoke site with Hybrid WAN capability from the **Sites** page. The Hybrid WAN sites can have a maximum of two WAN links (one of the links functions as a backup) and run network services from the CPE device.

The following image illustrates a simple Hybrid WAN topology.



Before you add an on-premise spoke site with Hybrid WAN capability:

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

  NOTE: This task assumes that the firewall 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 a console to the device, see the documentation for the CPE device. Links to the hardware documentation for the supported models are provided in Table 9 on page 35.

- Ensure that ESP protocol traffic is allowed on the network.
- Ensure that the ports listed in Table 9 on page 35 are open.

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

Table 9: Ports for Hybrid WAN

Device Model	NAT/Firewall Ports	CPE WAN Link Ports	
SRX 4x000 devices	443 500 4500	**xe-0/0/0** **xe-0/0/1** **xe-0/0/2** **xe-0/0/3**	SRX4100 • https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/srx4100-chassis.html SRX4200 • https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/srx4200-chassis.html
SRX 3xx devices, SRX 550M and vSRX devices	443 500 4500	**ge-0/0/0** **ge-0/0/1**	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
NFX 250	443 500 4500 7804	**ge-0/0/8**	NFX250 • https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/nfx250-chassis.html

Table 9: Ports for Hybrid WAN *(continued)*

Device Model	NAT/Firewall Ports	CPE WAN Link Ports	
NFX 150	443 500 4500	**heth4** and LTE	NFX150 • https://www.juniper.net/documentation/en_US/release-independent/junos/topics/reference/specifications/chassis-nfx150-physical.html

To add a hybrid WAN site:

1. From the **Add** list of the **Sites** page, click **On-Premise Spoke Site**.

   The **Add Site** wizard appears.

2. Complete the configuration settings in the General and WAN sections according to the guidelines provided in Table 10 on page 36.

3. Review the configuration and modify the settings, if needed, from the **Summary** tab.

4. 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.

Table 10: Fields on the Add OSpoke Site Page

Field	Description
General	
Site Information	
Site Name	Enter a site name. You can use any number of alphanumeric characters, including special characters. The maximum length is 10 characters.
Site Capabilities	
WAN Capabilities	Select **Hybrid WAN** to include Hybrid WAN capability in the on-premise spoke site.
Device Profile	

Table 10: Fields on the Add OSpoke Site Page *(continued)*

Field	Description
Device Series	Select the device series to which the CPE 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.
Device Information	
Serial Number	Enter the serial number of the CPE device.
Auto Activate	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. The **Activation Code** field appears if the selected device template does not support ZTP 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 78.
CPE Info	
CPE AS Number	Specify the autonomous system(AS) number.
Access Info	
Router Name	Specify the router name.
Router AS Number	Specify the AS number for the router.
Management Connectivity	
OAM Traffic Information	Select this option to set up an OAM link with CSO.

Table 10: Fields on the Add OSpoke Site Page *(continued)*

Field	Description
IP Prefix	Enter the IPv4 prefix to be used for the management network. This IP address must be unique across the entire management network. • For NFX150 and NFX250 devices, if the USE_SINGLE_SSH_TO_NFX parameter is disabled in the device template,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.
Gateway IP	If you configured the address assignment method as STATIC, enter the IP address of the gateway of the WAN service provider.
WAN links One of the two links functions as a backup link.	
WAN_0	
Link Type	Select whether the link would be an MPLS link or Internet link.
VLAN ID	Specify the identifier for the Layer 2 VLAN for the CPE device.
VRF Name	Specify the name of the virtual routing and forwarding (VRF) instance.
IPsec Concentrator Name	Specify the name of the IPsec concentrator device.
Internet Gateway IP	If you specified that the device is an IPsec concentrator, then specify the IPv4 address of the Internet gateway.
WAN_1	Refer to the fields described for WAN_0 for an explanation of the fields.

4

CHAPTER

Next Generation Firewall

Next-Generation Firewall Sites | 40

Next-Generation Firewall Sites

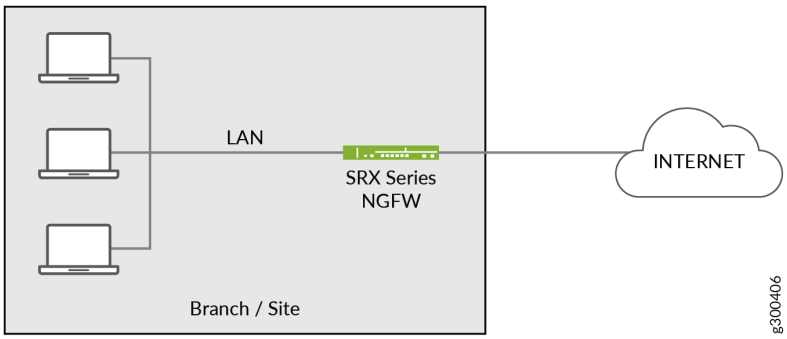
You can add a next-generation firewall site to manage a standalone SRX device that is configured as a firewall device. You can also create a next-generation firewall site with LAN for branch networks to manage an SRX firewall device and an EX Series switch.

This topic explains how you can:

- Add an On-Premise Spoke Site for Next Generation Firewall on page 40
- Add an On-Premise Spoke Site with Next-Generation Firewall and LAN Capabilities on page 43

Add an On-Premise 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 11 on page 41.

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

Table 11: Next Generation Firewall Devices, Port Information, and Documentation Links

Device Model	Hardware Documentation
SRX3xx device and SRX550M	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 SRX3400 • https://www.juniper.net/documentation/en_US/release-independent/junos/topics/concept/chassis-srx3400.html SRX3600 • https://www.juniper.net/documentation/en_US/release-independent/junos/topics/concept/chassis-srx3600.html SRX550M • https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/srx550-hm-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 12 on page 42.

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.

Table 12: SD-WAN On-Premise 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 10 characters.
Site Capabilities	Select **Next Gen Firewall**.
WAN	
Serial Number	Enter the serial number of the device.
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 78.
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**.

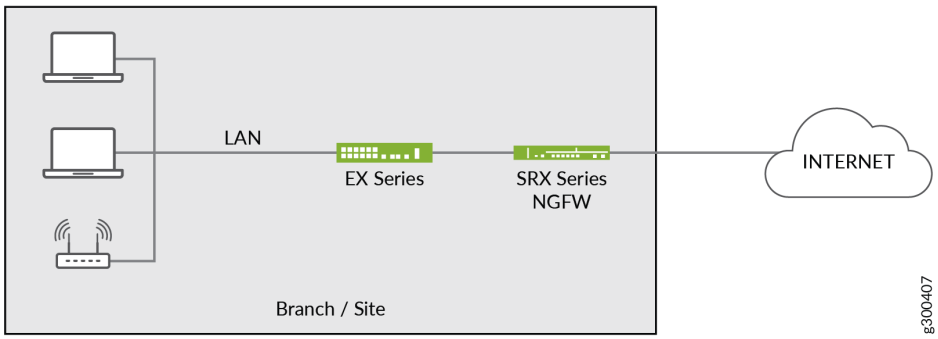
For more information about these tasks, see the Contrail Service Orchestration documentation at https://www.juniper.net/ documentation/product/en_US/contrail-service-orchestration.

SEE ALSO

Add an On-Premise Spoke Site with Next-Generation Firewall and LAN Capabilities

You can add a next-generation firewall site with LAN capabilities to manage an SRX device that is configured as a firewall device along with an EX series switch that is configured for the LAN network.

The following image shows a simple network topology for an on-premise spoke site with next-generation firewall and LAN capabilities.



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

This task assumes that the firewall 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 13 on page 44.

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

Table 13: Documentation Links for the Supported Hardware Devices

Device Model	Hardware Documentation
SRX3xx devices and SRX550M	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
LAN Switches	
EX2300	https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/ex2300-system-overview.html
EX3400	https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/ex3400-chassis.html
EX4300	https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/ex4300-system-overview.html

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 14 on page 45.

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

4. • If the Zero Touch Provisioning (ZTP) toggle button is enabled (default), CSO pushes the stage-1 and stage-2 configurations and provisions the switch.

   This process occurs immediately after the activation process, for which you entered the activation code or selected auto-activation.

> **NOTE:** Stage-1 configuration is the initial configuration that allows basic connectivity to a device, which is pushed to the device.
>
> The configuration that is pushed to the device after it has connected to CSO is called stage-2 configuration.

- If you disabled the Zero Touch Provisioning (ZTP) toggle button, you must manually configure the stage-1 configuration (as provided by CSO) on the switch.

  To manually configure the stage-1 configuration:

  a. On the **Site Activation: *Site-Name*** page, the **Click to copy stage-1 configuration** link appears after the Prestage Device step completes successfully.

  b. Click the **Click to copy stage-1 configuration** link.

     The stage-1 configuration page appears displaying the stage-1 configuration to be copied to the EX Series device.

  c. Copy the stage-1 configuration and log in to the console of the EX Series switch.

  d. Enter the configuration mode, paste, and commit the configuration.

     After the stage-1 configuration is committed, the switch has the outbound SSH configuration to connect with CSO.

     CSO then provisions the switch.

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

Table 14: SD-WAN On-Premise 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 10 characters.
Site Capabilities	Select **Next Gen Firewall**.
WAN	
Serial Number	Enter the serial number of the device.

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

Field	Description
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 78.
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.
In Band Management	Use the same port that you have configured for Internet connectivity for in-band management. Based on the SRX device, the port can be the first port (**ge-0/0/0**) or the last port (**ge-0/0/7** or **ge-0/0/15**.
LAN	
Device Name	Enter a unique name for the device.
Device Type	Select the type of the device.
Trunk Ports	Select at least two trunk ports on the CPE device to connect with the switch.
Switch Management Subnet	Specify the subnet that the DHCP can use to assign IP addresses.
Serial Number	Enter the serial number of the device.
Auto Activate	If the selected device 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. The **Activation Code** field appears if the selected device template does not support ZTP 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 78.

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.

- If the EX Series switch has Mist access points associated with that, you could integrate the Mist access points with CSO. For more information about integrating Mist access points with CSO, see "Enabling Integration with Mist Access Points" on page 66.
- 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** .
- Create and generate reports. For example, **Reports** > **Report Definitions** > .

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

SEE ALSO

Add an On-Premise Spoke Site for Next Generation Firewall | 40

5
CHAPTER

LAN

LAN Sites | **49**

Enabling Integration with Mist Access Points | **66**

LAN Sites

You can add an on-premise spoke site to provision, manage, and monitor EX Series switches by using CSO. You can either add an on-premise spoke site to manage a standalone EX Series switch or add an EX Series switch along with a CPE, a next-generation firewall device, or an enterprise hub. The EX Series switch can be added when you create an on-premise spoke site or enterprise hub. Alternatively, you can add the switch to an existing SD-WAN site, a next-generation firewall site, or an enterprise hub.

You can create one or more of the following sites to manage EX series switches:

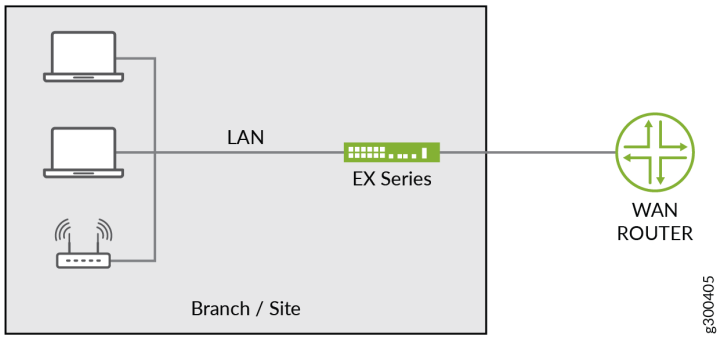
- On-premise spoke site for LAN on page 50
- On-premise spoke site for SD-WAN and LAN capabilities on page 26
- On-premise spoke site for next-generation firewall and LAN capabilities on page 43
- Add an Enterprise Hub Site with SD-WAN and LAN Capabilities on page 16

Alternatively, you can also add an EX Series switch to one of the existing sites as explained in the "Add LAN Capabilities to an Existing Site by Using a Switch" on page 64 topic.

If the EX Series switch has Mist access points associated with that, you could integrate the Mist access points with CSO. For more information about integrating Mist access points with CSO, see “Enabling Integration with Mist Access Points” on page 66.

Add an On-Premise Spoke Site for LAN

Adding an on-premise spoke site for LAN enables you to provision, manage, and monitor EX Series switches (physical and Virtual Chassis) by using CSO. The following image illustrates a simple topology of LAN for branch networks.



Connect the devices as shown in the topology diagram and power on the devices.

> **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.

> **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 Contrail Service Orchestration Release 5.1.1.

For information about connecting the device and connecting a console to the device, see the hardware documentation for your LAN device:

- EX2300
- EX3400
- EX4300
- EX4600
- EX4650

To add an on-premise spoke site for LAN:

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

   The Add On-premise Spoke Site for *Tenant-Name* page appears.

2. Complete the configuration as explained in Table 15 on page 53.

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

3. Review the configuration from the **Summary** tab.

   (Optional) Click the Edit links within the summary to go directly to a specific page of the wizard and modify the configured settings.

4. Click **OK** to add the site.

   The site activation job is initiated and the **Site Activation: *Site-Name*** page appears displaying the progress of the steps executed for activating the switch.

5. - If the Zero Touch Provisioning (ZTP) toggle button is enabled (default), CSO pushes the stage-1 and stage-2 configurations and provisions the switch.

     This process occurs immediately after the activation process, for which you entered the activation code or selected auto-activation.

     NOTE: Stage-1 configuration is the initial configuration that allows basic connectivity to a device, which is pushed to the device.

     The configuration that is pushed to the device after it has connected to CSO is called stage-2 configuration.

   - If you disabled the Zero Touch Provisioning (ZTP) toggle button, you must manually configure the stage-1 configuration (as provided by CSO) on the switch.

     To manually configure the stage-1 configuration:

     a. On the **Site Activation: *Site-Name*** page, the **Click to copy stage-1 configuration** link appears after the Prestage Device step completes successfully.

     b. Click the **Click to copy stage-1 configuration** link.

        The stage-1 configuration page appears displaying the stage-1 configuration to be copied to the EX Series device.

     c. Copy the stage-1 configuration and log in to the console of the EX Series switch.

     d. Enter the configuration mode, paste, and commit the configuration.

After the stage-1 configuration is committed, the switch has the outbound SSH configuration to connect with CSO.

CSO then provisions the switch.

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

Table 15: Settings for an On-Premise Spoke Site with LAN Capabilities

Field	Description
General	
Site Name	Enter a unique name for the site. You can use alphanumeric characters and hyphen (-); the maximum length is 10 characters.
Site Capabilities	Select **LAN**.
LAN	
Device Name	Enter a unique name for the device.
Device Type	Select the type of switch—EX2300, EX3400, EX4300, EX4600, and EX4650.
Device Model	Select the model for the switch you specified in the Device Type field. The models vary in the number and type of ports the switch contains. For example, If you selected EX3400, select a model such as EX3400-24P, EX3400-48P, EX3400-24T among others.
Virtual Chassis	Click the toggle button to enable or disable (default) adding the switch as a Virtual Chassis. If you enable this toggle button, you must select the method of provisioning the Virtual Chassis. **NOTE:** • Before you add a Virtual Chassis in CSO, ensure that the Virtual Chassis is setup. See "Step-by-Step Procedure" on page 57 for information about setting up a Virtual Chassis. • In Release 5.1.1, you cannot add a new member or change the roles assigned to the members after you onboard a Virtual Chassis. To change the roles, you must delete the Virtual Chassis, form a new Virtual Chassis, and then, onboard the new Virtual Chassis.

Table 15: Settings for an On-Premise Spoke Site with LAN Capabilities *(continued)*

Field	Description
Method	Select the method of provisioning the Virtual Chassis: • Auto Provisioning: The Virtual Chassis automatically determines the roles (primary, backup, and line card) of the member devices. If you select this option, you must enter only the serial number of the primary device in the Primary Serial Number field that appears. • Pre Provisioning: You can determine the roles (primary, backup, and line card) of the member devices in the Virtual Chassis. If you select this option, you must provide the serial number, device model, device type, and role of all the member devices of the Virtual Chassis in the fields that appear. **NOTE:** In the case of preprovisioning, the Primary device must always be designated as Member 0. For both these methods, ensure that: • The devices in the Virtual Chassis are fully installed and ready to be configured in the site. In addition, all members must be powered on. This means that the output of the show virtual-chassis status command must display all the member devices of the Virtual Chassis and the devices must be in Present (**Prsnt**) state. **NOTE:** If you do not have access to the serial console port for preprovisioning, only the primary device must be powered on first. • The primary and backup member devices have internet access to the Juniper redirect server and CSO. • All members in the Virtual Chassis are running the same firmware (either JUNOS 18.4R2.7 or 18.4R3.3). • For EX3400, EX4300, EX4600, and EX4650 devices to act as a Virtual Chassis, all the corresponding member devices are interconnected through Virtual Chassis ports (VCPs). For EX2300 devices to act as a Virtual Chassis, the 10-Gbps Ethernet ports are configured as VCPs manually and the member devices are interconnected.

Table 15: Settings for an On-Premise Spoke Site with LAN Capabilities *(continued)*

Field	Description
Master Serial Number	If you selected Auto Provisioning, enter the serial number of the Primary (from the fully-formed Virtual Chassis). To obtain the serial number, log in to the CLI of any device that is part of the fully-formed Virtual Chassis, in operational mode, and enter **show virtual-chassis**. The list of the member devices in the Virtual Chassis, along with the serial number and role appear. The primary device is indicated as **Master** under **Role**. Alternatively, you can view the serial number on the barcode sticker, which is on the rear-panel of the switch.
Member *<member-number>*	If you selected Pre Provisioning, enter the serial numbers of all the devices (from the fully-formed Virtual Chassis or based on what roles you decide to assign each Virtual Chassis member), and also select the device type and model from the list. **NOTE:** • If you enable ZTP, you must enter the serial number of the Primary device only in the Member 0 field. • If you do not have access to the serial console port of the virtual chassis, the first member that is powered on is considered the primary. Enter the serial number of this device in the Member 0 field. Click the Add (+) icon to add a member or the Remove (-) icon to remove a member. For information on the number of devices that can be added, see Table 16 on page 56. **NOTE:** The Routing Engine check box corresponding to Member 0 is always selected, indicating that Member 0 always acts as the primary. To select a member as backup, click the Routing Engine check box corresponding to that member; the remaining members act as line cards.
Serial Number	If you disabled the Virtual Chassis toggle button, specify the serial number of the physical switch. To obtain the serial number, log in to the CLI of the switch in operational mode and enter **show chassis hardware**. Alternatively, you can view the serial number on the barcode sticker, which is on the rear-panel of the switch. The serial number is a case-sensitive, alphanumeric string.

Table 15: Settings for an On-Premise Spoke Site with LAN Capabilities *(continued)*

Field	Description
Zero Touch Provisioning	Click the toggle button to enable or disable zero-touch provisioning (ZTP) of the switch through ZTP. If you disable ZTP, you must manually copy and paste the Stage-1 configuration on the switch during site activation. See Step 4 for details. **NOTE:** • Only EX Series switches running 18.4R2.7 or 18.4R3.3 firmware support ZTP. • EX4600 and EX4650 switches do not support Phone-Home client. You must disable ZTP and manually configure the stage-1 configuration on the switches.
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 78.

Table 16 on page 56 lists the supported device types, combinations in the non-mixed mode, and the total number of members, supported by each device type, in a Virtual Chassis.

Table 16: Supported Device Types, Modes, and Number of Members Allowed in a Virtual Chassis

Device Type	Non-mixed Virtual Chassis Support	Number of Members Allowed in the Virtual Chassis
EX2300	Combination of the same or different models of EX2300 switches.	Up to 4 members.
EX3400	Combination of the same or different models of EX3400 switches.	Up to 10 members.
EX4300	Combination of the same or different models of EX4300 switches.	Up to 10 members.
EX4600	Combination of the same or different models of EX4600 switches.	Up to 10 members.
EX4650	Combination of the same or different models of EX4650 switches.	Up to 2 members.

Before you autoprovision or preprovision a Virtual Chassis in CSO, ensure that the Virtual Chassis is setup.

- To setup a Virtual Chassis for autoprovisioning:

  1. Decide the number of member devices in the Virtual Chassis.

  2. If you've added EX3400, EX4300, EX4600, or EX4650 devices as Virtual Chassis, interconnect all the corresponding member devices through Virtual Chassis ports (VCPs).

     If you've added EX2300 devices as Virtual Chassis, configure the 10-Gbps Ethernet ports as VCPs manually (through CLI) and interconnect the member devices.

     > **NOTE:** At this point, do not power on any member devices in the Virtual Chassis.

  3. Decide which member device acts as the r and power on only this device first.

     > **NOTE:**
     > - Remember the serial number of the primary device in the Virtual Chassis. This serial number is required during the site activation workflow to add this Virtual Chassis in CSO.
     > - For ZTP to be successful, the primary device should always be designated as Member 0. You must specify the same serial number in the Member 0 field in CSO.

  4. Wait until the primary device completes booting.

     After booting is complete, the LCD panel on this device displays a menu that includes the JUNOS OS version loaded on the device, status of VCPs, status of power supplies, and so on.

  5. Power on the remaining member devices one after the other.

  6. Wait until all the member devices complete booting.

     After booting is complete, you can confirm that the Virtual Chassis is fully formed when all the LEDs on the VCPs are ON.

  7. Connect the primary and backup device to the Internet through the management port or uplink port.

  8. Verify the connectivity from the primary device to CSO or to any host on the Internet by using **ping** or **telnet** to Juniper redirect server on port 443.

- To setup a Virtual Chassis for preprovisioning:

1. Decide the number of member devices in the Virtual Chassis.

2. If you've added EX3400, EX4300, EX4600, or EX4650 devices as Virtual Chassis, interconnect all the corresponding member devices through Virtual Chassis ports (VCPs).

   If you've added EX2300 devices as Virtual Chassis, configure the 10-Gbps Ethernet ports as VCPs manually and interconnect the member devices.

   > **NOTE:** At this point, do not power on any member devices in the Virtual Chassis.

3. Decide which member device acts as the primary and which member device acts as the backup.

4. Of the two devices, power on the device that you want to select as the primary (Member 0), and wait until it completes booting.

   After booting is complete, the LCD panel on this device displays a menu that includes the JUNOS OS version loaded on the device, status of VCPs, status of power supplies, and so on.

   > **NOTE:**
   > - Remember the serial numbers of all the devices in the Virtual Chassis. These serial numbers will be needed in the site activation workflow to add this Virtual Chassis in CSO.
   > - For ZTP to be successful, the primary should always be designated as Member 0. You must specify the same serial number in the Member 0 field in CSO.

5. Power on the device that you want to select as the backup and wait until it completes booting.

   After booting is complete, the LCD panel on this device displays a menu that includes the JUNOS OS version loaded on the device, status of VCPs, status of power supplies, and so on.

6. Power on the remaining member devices one after the other.

7. Wait until all the member devices complete booting.

   After booting is complete, you can confirm that the Virtual Chassis is fully formed when all the LEDs on the VCPs are ON.

8. Connect the primary and backup device to the Internet through the management port or uplink port.

9. Verify the connectivity from the primary device to CSO or to any host on the Internet by using **ping** or **telnet** to Juniper redirect server on port 443

Now that the Virtual Chassis is setup, proceed to add the Virtual Chassis in CSO. See the **LAN section** in Table 15 on page 53 for details.

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.

- Monitor alerts, alarms, and jobs. For example, **Monitor** > **Jobs**.

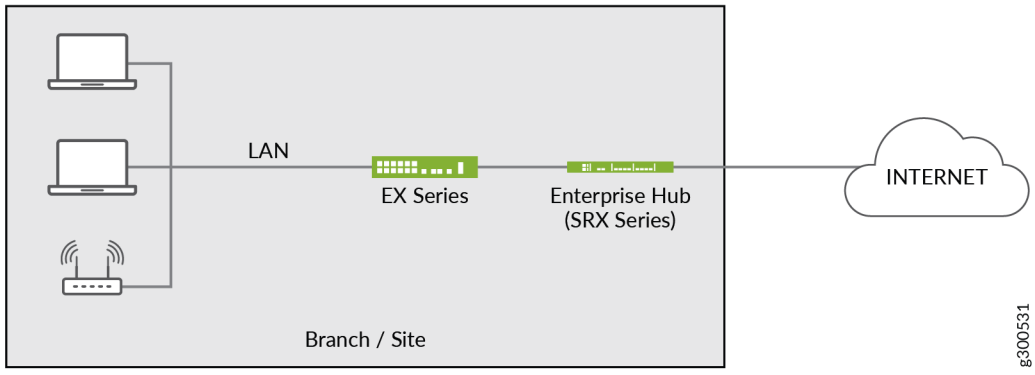
For more information about these tasks, see the Contrail Service Orchestration documentation at https://www.juniper.net/ documentation/product/en_US/contrail-service-orchestration.

SEE ALSO

Add an SD-WAN On-Premise Spoke Site with LAN for Branch Networks | 26

Add an Enterprise Hub Site with SD-WAN and LAN Capabilities

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. You can add an EX Series switch for branch network as part of the enterprise hub site. The following illustration shows a simple topology that contains an enterprise hub and an EX Series switch.



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 4 on page 18.

3. Click **OK**.

   The site activation job is initiated and the Site Activation: Site-Name page appears displaying the progress of the steps executed for activating the devices in the site.

4. - If the Zero Touch Provisioning (ZTP) toggle button is enabled (default), CSO pushes the stage-1 and stage-2 configurations and provisions the switch.

     This process occurs immediately after the activation process, for which you entered the activation code or selected auto-activation.

     > **NOTE:** Stage-1 configuration is the initial configuration that allows basic connectivity to a device, which is pushed to the device.
     >
     > The configuration that is pushed to the device after it has connected to CSO is called stage-2 configuration.

   - If you disabled the Zero Touch Provisioning (ZTP) toggle button, you must manually configure the stage-1 configuration (as provided by CSO) on the switch.

     To manually configure the stage-1 configuration:

     a. On the **Site Activation: *Site-Name*** page, the **Click to copy stage-1 configuration** link appears after the Prestage Device step completes successfully.

     b. Click the **Click to copy stage-1 configuration** link.

        The stage-1 configuration page appears displaying the stage-1 configuration to be copied to the EX Series device.

     c. Copy the stage-1 configuration and log in to the console of the EX Series switch.

     d. Enter the configuration mode, paste, and commit the configuration.

        After the stage-1 configuration is committed, the switch has the outbound SSH configuration to connect with CSO.

CSO then provisions the switch.

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

Table 17: Enterprise Hub 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 10 characters.
Site Capabilities	SD-WAN capability is selected by default. You cannot clear the selection. If you want to include LAN capabilities in the enterprise hub site, select **LAN**.
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.
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 78. **NOTE:**
IP Prefix	Enter the IPv4 prefix to be used for the management network. This IP address must be unique across the entire management network. • 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 17: Enterprise Hub Site Settings *(continued)*

Field	Description
WAN_0	This field is enabled by default. You can configure up to 4 WAN links as required.
Link Type	Select whether the link would be an MPLS link or Internet link.
Egress Bandwidth	Enter the maximum bandwidth, in Mbps, allowed on the WAN link. Range: 1 through 10,000.
Address Assignment	Select the method of assigning an IP address to the WAN link—DHCP or STATIC. If you select STATIC, you must provide the IP address prefix and the gateway address for the WAN link.
Static IP Prefix	If you configured the address assignment method as STATIC, enter the IP address prefix of the WAN link.
Gateway IP Address	If you configured the address assignment method as STATIC, enter the IP address of the gateway of the WAN service provider.
Advanced Settings	
Use For Fullmesh	Click the toggle button to specify whether the WAN link can be a part of a full mesh topology. A site can have a maximum of three links enabled for meshing.
LAN **NOTE:** This tab is enabled only if you select **LAN** from the Site Capabilities options in General Settings.	
Device Profile	
Device Name	Enter a name for the switch. You can use alphanumeric characters and hyphen (-). The maximum length allowed is 15 characters.
Device Type	Select the type of switch—EX2300, EX3400, or EX4300 When you change the default device type, a carousel for device template appears.

Table 17: Enterprise Hub Site Settings *(continued)*

Field	Description
Device Model	Select the model for the switch you specified in the Device Type. The models vary in the number and type of ports the switch contains. For example, If you selected EX3400, select a model such as EX3400-24P, EX3400-48P, EX3400-24T among others.
CPE Settings	
Trunk Ports	Select at least two trunk ports on the CPE device to connect with the switch. The trunk ports are used for carrying the following: • LAN traffic between the switch and the CPE • Management traffic for in-band management of the switch.
Switch Management Subnet	Specify the subnet that the DHCP can use to assign IP addresses to the switch and the access devices connected to the switch.
Switch Details	
Serial Number	Specify the serial number of the switch.
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 78. **NOTE:** You must physically connect the switch to the CPE and power it on for the switch to be automatically activated when the auto activate option is enabled.

SEE ALSO

On-premise spoke site for LAN | 50

Next-generation firewall site with LAN for branch networks | 43

Add LAN Capabilities to an Existing Site by Using a Switch

You can add a switch to an existing SD-WAN site, next-generation firewall site, or an enterprise hub site.

Before you add a switch to an existing site, ensure that you connect the switch to the network as shown in the topology diagrams provided in the following topics. After you connect the switch to the network as required, power on the device.

- SD-WAN site with LAN for branch networks on page 26

  NOTE: You can add a LAN switch to an SD-WAN site only if the CPE is an SRX series device or an NFX250 device.

- Next-generation firewall site with LAN for branch networks on page 43
- Add an Enterprise Hub Site with SD-WAN and LAN Capabilities on page 16

To add a switch to an existing site, follow these steps:

1. From the Sites page (**Resources** > **Site Management**) of the CSO portal, select the site to which you want to add the switch, click **Add**, and select **Add Switch**.

   The Add Switch page appears.

2. Complete the following configuration:
   - Device Name - specify a unique name for the device.
   - Device Type - select the type of device from the Device Type drop-down list.
   - Device Model - select a device model for the switch.
   - Trunk Ports - specify the CPE trunk ports.
   - Switch Management Subnet - specify the subnet that the DHCP can use to assign IP addresses to the switch and the access devices connected to the switch.
   - Serial Number - specify the serial number of the switch.

     NOTE: Based on the device template you selected, the Auto Activate Switch toggle button is enabled or disabled by default. You can click to enable or disable this option. When Auto Activate Switch is enabled, zero-touch provisioning of the switch is automatically triggered when the site is created.

     If you choose to disable the Auto Activate Switch option, you must specify the activation code of the device to “manually activate a device” on page 78.

3. Click **Save**.

   The site activation job is initiated and the Site Activation: Site-Name page appears displaying the progress of the steps executed for activating the devices in the site.

4. - If the Zero Touch Provisioning (ZTP) toggle button is enabled (default), CSO pushes the stage-1 and stage-2 configurations and provisions the switch.

     This process occurs immediately after the activation process, for which you entered the activation code or selected auto-activation.

     > **NOTE:** Stage-1 configuration is the initial configuration that allows basic connectivity to a device, which is pushed to the device.
     >
     > The configuration that is pushed to the device after it has connected to CSO is called stage-2 configuration.

   - If you disabled the Zero Touch Provisioning (ZTP) toggle button, you must manually configure the stage-1 configuration (as provided by CSO) on the switch.

     To manually configure the stage-1 configuration:

     a. On the **Site Activation: *Site-Name*** page, the **Click to copy stage-1 configuration** link appears after the Prestage Device step completes successfully.

     b. Click the **Click to copy stage-1 configuration** link.

        The stage-1 configuration page appears displaying the stage-1 configuration to be copied to the EX Series device.

     c. Copy the stage-1 configuration and log in to the console of the EX Series switch.

     d. Enter the configuration mode, paste, and commit the configuration.

        After the stage-1 configuration is committed, the switch has the outbound SSH configuration to connect with CSO.

        CSO then provisions the switch.

Enabling Integration with Mist Access Points

You can enable integration with the Mist access points to easily access and view Mist access points connected to the branch network. When integration with Mist access point is enabled, the connected access points are listed in the **Devices** tab of the **Resources** > **Site Management** > ***Site Name*** page. You can click the access point name to view the Mist access point details from the Mist portal that is integrated with CSO.

To enable integration with the Mist access point:

1. Select **Administration** > **WiFi Settings**.

   The WiFi Settings page appears.

2. Click the Enable toggle button to enable integration with Mist access points.

   The Login E-mail and Login Password fields appear.

3. In the Login E-mail page, enter the e-mail address that is the username for your Mist account.

4. In the Login Password page, enter the password for your Mist account.

5. Click **Save**.

After you enable integration and enter the login credentials, CSO adds the access point to the list of devices associated with a site. To view details about the access point, **Devices** tab of the **Resources** > **Site Management** > ***Site Name*** page and click the access point name. The Mist portal page for the selected device appears.

6

CHAPTER

Tenant Management

Add a Tenant | **68**

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 18 on page 68.

   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 18: 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 15 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.

Table 18: Add Tenant Settings *(continued)*

Field Name	Description

Service for Tenant	Select one or more of the following services that the tenants can manage by using CSO:
	• SD-WAN—Enables tenants to manage sites that have up to four WAN links with intelligent, SLA-based traffic routing among the WAN links.
	• Hybrid WAN—Enables tenants to manage sites where the network services are run from the CPE device and supports up to WAN links to provide an active/backup model.
	• Next-Generation Firewall—Enables the tenants to manage next generation firewall devices and firewall policies.
	• LAN—Enables the tenants to manage EX Series switches.
	When tenants add sites, they can implement any of the services that you selected. For example:
	• If you select only SD-WAN, tenants can create one or more on-premise spoke site for SD-WAN.
	• If you select only LAN, tenants can create one or more on-premise spoke site for standalone EX Series switches.
	• If you select SD-WAN and LAN, tenants can create one or more of the following sites:
	  ◦ An on-premise spoke site for SD-WAN
	  ◦ An on-premise spoke site for a standalone EX Series switch
	  ◦ An on-premise spoke site for SD-WAN with LAN capabilities

RELATED DOCUMENTATION

Configure SMTP Settings | 71

CHAPTER 7

SMTP Configuration

Configure SMTP Settings | 71

Configure SMTP Settings

Configure an SMTP server for sending e-mail messages.

1. When you log in to the CSO portal for the first time after changing the default password, you are prompted to configure the SMTP server. Click **OK** to open the SMTP page.

   Alternatively, select **Administration** >**SMTP** from the CSO portal.

   The SMTP page appears.

2. Configure the settings as explained in Table 19 on page 71.

3. Click **Save**.

   Table 19: SMTP Settings

Field	Description
Server Address	Enter the hostname for the SMTP server.
Port Number	Enter the port number for the SMTP server. Check with your e-mail service provider for the SMTP port number.
From Name	Enter the name that you want to appear as the from name in the e-mail.
User Name	If you have enabled **SMTP Authentication**, enter the user name that you want to use for authentication.
Password	If you have enabled **SMTP Authentication**, enter and confirm the password that you want to use for authentication.
From Email Address	Enter the e-mail address that you want to appear as the from address in the e-mail.

RELATED DOCUMENTATION

Add a Tenant | 68

8
CHAPTER

Provider Hub

Add a Provider Hub (DATA_ONLY Capability) | 73

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.

To add a provider hub device with DATA_ONLY capability:

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

   The Cloud Hub Devices page appears.

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

   The Add Cloud Hub Device page appears.

3. Complete the configuration according to the guidelines provided in Table 20 on page 73.

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 Cloud Hub Devices page.

Table 20: Fields on the Add Cloud Hub Device Page

Field	Description
Name	Enter the name of the cloud hub device. You can use alphanumeric characters, including special character(-). The maximum length is 15 characters. Example: SRX-cloud-hub
Management Region	Displays the regional server with which the device communicates. The management region name is populated based on the information from the device template. Example: regional
POP	Select the POP where the hub device needs to be added. Example: pop_blue

Table 20: Fields on the Add Cloud Hub Device Page *(continued)*

Field	Description
Site Capability	Select the site capability of the provider hub device as DATA_ONLY, which indicates that the hub transmits only the data traffic. 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 the cloud-based CSO.
Authentication Type	Select the authentication method—Preshared Key (PSK) or Public Key Infrastructure (PKI).
Advanced Configuration	
Name Server IP List	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. DNS servers are used to resolve hostnames into IP addresses.
NTP Server	Specify the fully qualified domain names (FQDNs) or IP addresses of one or more NTP servers. Example: ntp.example.net The site must have DNS reachability to resolve the FQDN during site configuration.
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	Select a device template for the selected device series. The device template contains information for configuring a device.
Device Information	

Table 20: Fields on the Add Cloud Hub Device Page *(continued)*

Field	Description
Serial Number	Enter the serial number of the provider hub device. The serial number is a 12-digit number present on the rear panel of the device. Serial numbers are case-sensitive.
Auto Activate	Click the toggle button to enable or disable automatic activation of the provider hub device. When you enable this field, zero-touch provisioning (ZTP) of the provider hub device is automatically triggered after the site is added to CSO. The device template that you select determines whether this option is enabled or disabled by default.
Boot image	Select the boot image from the drop-down list if you want to upgrade the image for the provider hub device. 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. 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. .
Management Connectivity	
Loopback IP Prefix	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.
WAN Links	

Table 20: Fields on the Add Cloud Hub Device Page *(continued)*

Field	Description
WAN_0 WAN_1 WAN_2 WAN_3	Select a WAN link to enable it. After selecting the link, specify the following information: • 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

After you add the cloud hub device:

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

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

9

CHAPTER

Device Activation

Activate a Device | **78**

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-Premise Spoke Site | 21
- Add an On-Premise Spoke Site for LAN | 50
- Add an SD-WAN On-Premise Spoke Site with LAN for Branch Networks | 26
- Add an On-Premise Spoke Site with Hybrid WAN Capability | 34
- Add an On-Premise Spoke Site for Next Generation Firewall | 40
- Add an On-Premise Spoke Site with Next-Generation Firewall and LAN Capabilities | 43