JUNIPER NETWORKS | Engineering Simplicity

Contrail SD-LAN: Manage Branch and Campus Switching

Published
2020-11-11

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 SD-LAN: Manage Branch and Campus Switching
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 | vi

Documentation and Release Notes | **vi**

Documentation Conventions | **vi**

Documentation Feedback | **ix**

Requesting Technical Support | **ix**

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

1 **Introduction to Contrail SD-LAN**

Contrail SD-LAN Overview | 12

- Contrail SD-LAN implementation in Branch and Campus Networks | **12**

SD-LAN Use Cases | 13

SD-LAN Workflow | 16

2 **Add Profiles for SD-LAN**

SD-LAN Profiles Overview | 20

- Life Cycle of a Port Profile | **22**

Add Authentication Profiles | 23

Add Firewall Filters and Terms | 28

Add Port Profiles | 31

Add RADIUS Server Profiles | 36

Add Access Profiles | 38

3 Onboard Devices to CSO

Add and Provision a Switch Overview | 43

Switch Behind an Internet Gateway Overview | 44

Switch Behind a CPE or Next-Generation Firewall Overview | 45

Add a Switch Behind an Internet Gateway | 47

Add a Switch Behind a CPE | 57

Add a Switch Behind a Next-Generation Firewall | 73

Add Switches to an Existing SD-LAN Site | 80

Add Switches to an Existing SD-WAN Site | 91

4 Configure an EX Series Switch

Configure an EX Series switch Overview | 97

Configure an EX Series Switch by Using Configuration Templates | 97

Configure an EX Series Switch by Using Profiles | 101

Deploy an Access Profile on a Switch | 102

Configure Switch Ports by Using a Port Profile | 102

Configure an EX Series Switch Manually | 104

Enable Ports | 105

5 Integrate CSO with Mist UI and Discover Access Points

Integrate CSO with Mist Portal | 108

Discover Mist Access Points | 109

6 Monitor an EX Series Switch and Connected Access Points

Monitor an EX Series Switch Overview | 111

Monitor Port Level Information | 112

Monitor Chassis-Level Information | 113

Monitor System Health | 116

Monitor Device Level Information | 119

Monitor Mist Access Points | 123

7 Troubleshoot Issues

Gather Troubleshooting Data | 126

Troubleshoot Connectivity Issues Between the Switch and CSO | 127

Virtual Chassis is not Connecting to CSO | 129

Device Activation is Failing When Using ZTP | 131

ZTP of an EX Series Switch is Failing | 132

Device Statistics are not Displayed | 133

Unable to Monitor Ports | 134

Chassis View is not Refreshing | 134

Ports are not Reflecting the Configured Behavior | 135

8 Appendix

Prepare a Virtual Chassis for Onboarding to CSO | 137

- Setting up a Virtual Chassis for Provisioning | 137
- Setup a Virtual Chassis for Autoprovisioning | 138
- Setup a Virtual Chassis for Preprovisioning | 139
- Members Allowed in a Virtual Chassis | 140

Default Configuration Templates For EX Series Switches | 141

Creating a LAN Segment for Discovering Mist Access Points | 142

About the Documentation

IN THIS SECTION

- Documentation and Release Notes | vi
- Documentation Conventions | vi
- Documentation Feedback | ix
- Requesting Technical Support | ix

Use this guide to implement SD-LAN solutions by using Contrail Service Orchestration (CSO).

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 vii 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 vii 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		

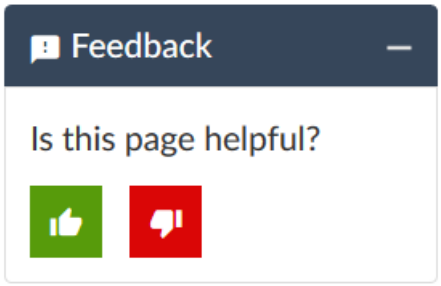
Table 2: Text and Syntax Conventions *(continued)*

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

Introduction to Contrail SD-LAN

Contrail SD-LAN Overview | **12**

SD-LAN Use Cases | **13**

SD-LAN Workflow | **16**

Contrail SD-LAN Overview

SUMMARY

This chapter briefly describes the Contrail SD-LAN solution, the different SD-LAN use cases and the workflow to implement these use cases.

Software-Defined LAN (SD-LAN) uses software-defined networking (SDN) and network function virtualization (NFV) in the access layer of an enterprise network. The access layer comprises devices(for example: LAN switches and wireless LAN (WLAN) access points) which enable end-user devices (for example: laptops) to connect to enterprise networks.

The SD-LAN concept provides a network-wide, policy-based approach to the management of devices in the LAN A controller assigns policies to all the devices in the access layer of the enterprise network. This reduces the provisioning time and centralizes the management of the enterprise network. The controller also continuously monitors the devices and uses policies to enable the devices to react to specific conditions.

By using SD-LAN, you have greater control of the enterprise network down to the application layer and have deeper insight into the networks performance and use.

Juniper Networks' Contrail SD-LAN uses Contrail Service Orchestration (CSO) to deploy, manage and monitor remote LAN devices. By using CSO as the controller to manage the EX Series switches, network administrators can monitor LANs and WLAN access points from remote locations.

By using the Contrail SD-LAN solution, you can easily provision switches to manage LANs, configure LAN virtualization, and apply security policies in the same way that you operate your SD-WAN environments. This automated functionality simplifies operations to reduce costs and leverage the WAN and LAN network for connected security.

Contrail SD-LAN implementation in Branch and Campus Networks

Figure 1 on page 13 shows an example of the implementation of the Contrail SD-LAN solution by using CSO. The branch network has an EX switch behind a CPE or a next-generation firewall. A Mist access point is connected to the switch for wireless connectivity. The EX switch can be an EX Series Virtual Chassis or a physical standalone switch.

The campus network has multiple distribution switches connected to an SRX Series device that acts as an Internet gateway. The distribution switches are connected to access switches.

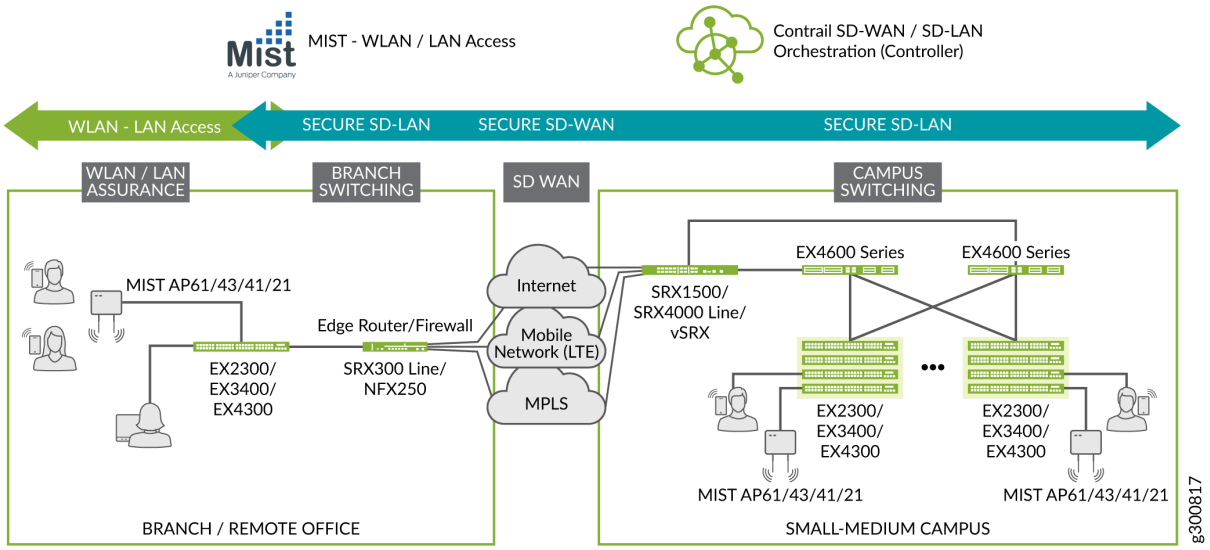
The branch and the campus networks are connected to each other through the Internet, mobile (LTE), or MPLS paths.

CSO manages the following:

- CPE, firewall, switches, and the Internet gateway
- SD-WAN connections between the branch and the campus network
- Connections between the switch and the attached devices (CPE, firewall, and Internet gateway)

You can use MIST portal to manage the access points and wireless LAN within the branch and campus network.

Figure 1: Contrail SD-LAN Implementation



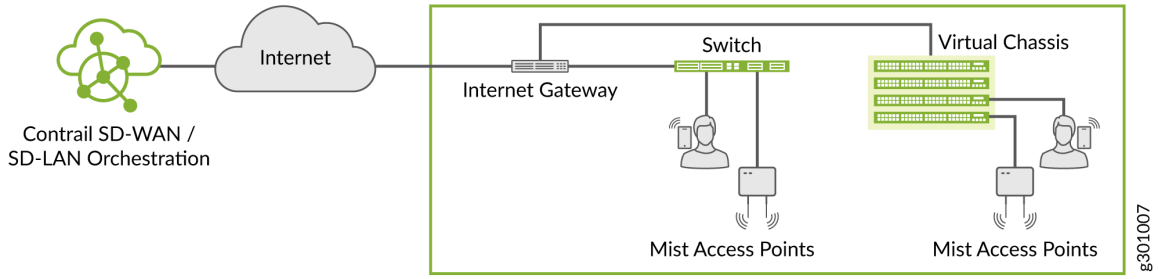
SD-LAN Use Cases

You can implement the Contrail SD-LAN solution in a branch and campus network to mange your switches and access points as follows:

- **EX Behind an Internet Gateway**: In this implementation, you can manage multiple EX Series switches by connecting them to CSO through an Internet Gateway; see Figure 2 on page 14.

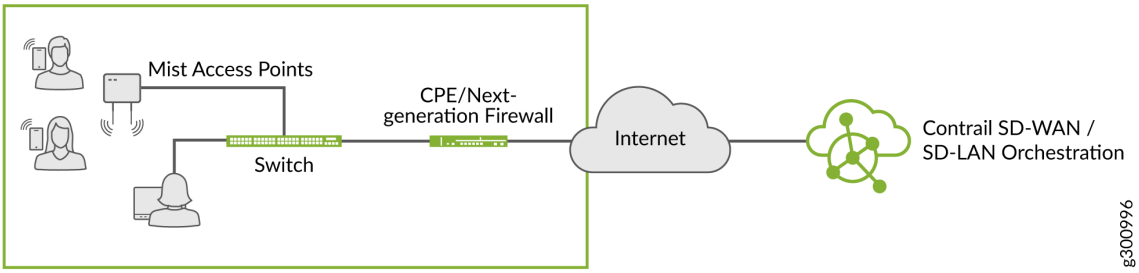
  The Internet gateway device can be a Juniper Networks device or a third-party device.

Figure 2: EX Behind an Internet Gateway



- **EX behind an SD-WAN CPE**: In this implementation, you can manage an EX Series switch by connecting it to CSO through an SD-WAN CPE; see Figure 3 on page 14.
- **EX behind a next-generation firewall**: In this implementation, you can manage an EX Series switch with by connecting it to CSO through a next-generation firewall; see Figure 3 on page 14.

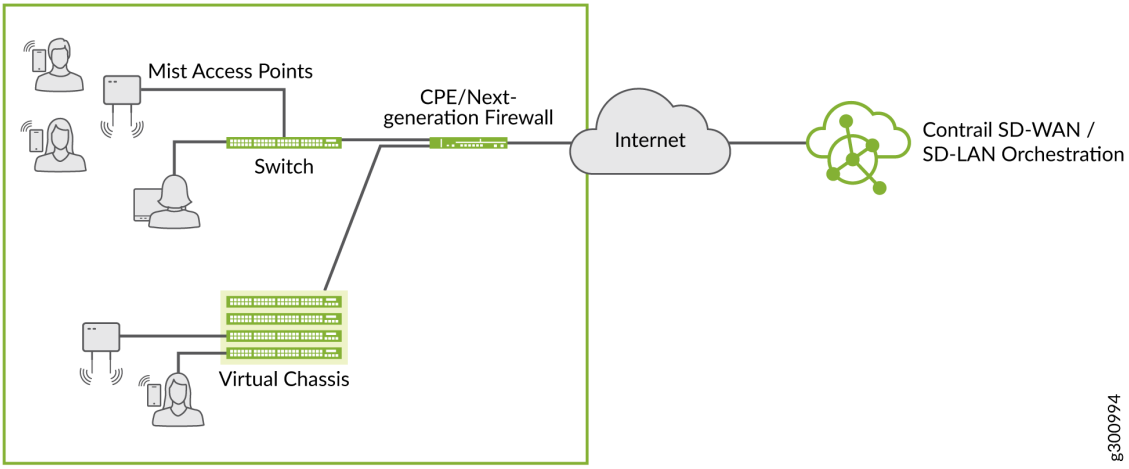
Figure 3: EX Behind a CPE or next-Generation Firewall



You can manage multiple switches by using CSO, when the switches are connected to CSO through a CPE or a next-generation firewall as shown in Figure 4 on page 15.

However, in this implementation, you must manage the connectivity and configuration between the switches and the CPE or next-generation firewall either by using configuration templates provided by CSO or manually; see the *Configure an EX Series Switch* chapter in this guide for details.

Figure 4: Multiple Switches Behind a CPE or Next-Generation Firewall



For details about the implementation of the use cases, see “Add and Provision a Switch Overview” on page 43.

SD-LAN Workflow

Before you start the SD-LAN workflow by using CSO, ensure that:

- The tenant (logical entity representing a customer) to which you want to onboard the switch is configured in CSO.
- The switch, the CPE or the next-generation firewall are running the correct versions of Junos OS supported by CSO. For information related to Junos OS supported on a switch for a particular CSO release, see the Release Notes for that CSO release at https://www.juniper.net/documentation/product/en_US/contrail-service-orchestration.
- The following ports and protocols are permitted through your network firewall:

  Table 3 on page 16 lists the ports and protocols that you must enable in your network firewalls for communication of the devices with CSO.

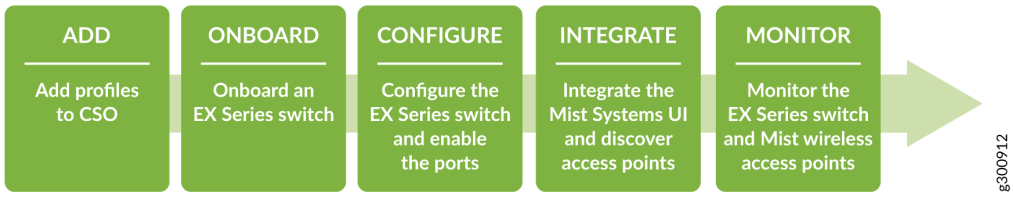
  Table 3: Ports Used for Communication with CSO

Port	Protocol	Purpose
443	TCP	Phone-home client for zero-touch provisioning (ZTP)
7804	TCP	For provisioning the stage-2 configuration on the switch after committing the stage-1 configuration.

- The devices should be in the factory default state and should be powered on.
- The devices get DHCP IP address and have Internet connectivity along with DNS resolution when connected to the network.

Figure 5 on page 16 illustrates the steps to implement Contrail SD-LAN by using CSO.

Figure 5: Contrail SD-LAN Workflow



To implement Contrail SD-LAN solution by using CSO:

1. Add the following profiles for authentication and access control to CSO.

   1. Authentication profile; see “Add Authentication Profiles” on page 23
   2. Firewall Filters; see “Add Firewall Filters and Terms” on page 28
   3. Port Profile; see “Add Port Profiles” on page 31
   4. RADIUS Server Profile; see “Add RADIUS Server Profiles” on page 36
   5. Access Profile; see “Add Access Profiles” on page 38

2. Onboard an EX Series switch:

   - As a standalone switch behind an Internet Gateway; see “Add a Switch Behind an Internet Gateway” on page 47
   - Along with the CPE; see “Add a Switch Behind a CPE” on page 57
   - Along with a next-generation firewall; see “Add a Switch Behind a Next-Generation Firewall” on page 73

   You can onboard a switch and manage it after you have only a CPE, or a next-generation firewall onboarded to and provisioned by CSO. You can also onboard more than one switch behind an internet gateway; see:

   - “Add Switches to an Existing SD-WAN Site” on page 91 to add the switch to an already provisioned CPE or next-generation firewall;
   - “Add Switches to an Existing SD-LAN Site” on page 80 to add more switches behind an Internet gateway.

3. Configure the EX Series switch.

   You can configure the EX Series switch in one of the following ways:

   - By using configuration templates; see “Configure an EX Series Switch by Using Configuration Templates” on page 97
   - By using profiles; see “Configure an EX Series Switch by Using Profiles” on page 101
   - Manually; see “Configure an EX Series Switch Manually” on page 104

4. Enable the ports of a switch to allow traffic to flow through the switch; see “Enable Ports” on page 105
5. Integrate CSO with Mist Portal to monitor access points connected to the switch; see “Integrate CSO with Mist Portal” on page 108.
6. Discover access points connected to the switch; see “Discover Mist Access Points” on page 109 .
7. Monitor the switch and the connected access points. You can monitor the following components of the switch in CSO:

   - The EX device (number of ports that are up or down, alarms, system users and so on)
   - The device chassis (view details of individual ports, view CPU and memory utilized, view fan details, and so on)

- The ports on the device (view port details such as port number, admin status, link mode and so on; % of CPU utilized by the port, packet loss, and so on)

You can launch the Mist Portal from CSO by clicking an access point and monitor the access points in the Mist portal; see the *Monitor an EX Series Switch and Connected Access Points* chapter in this guide.

2

CHAPTER

Add Profiles for SD-LAN

SD-LAN Profiles Overview | **20**

Add Authentication Profiles | **23**

Add Firewall Filters and Terms | **28**

Add Port Profiles | **31**

Add RADIUS Server Profiles | **36**

Add Access Profiles | **38**

SD-LAN Profiles Overview

SD-LAN profiles are templates for configuring port parameters such as flow control, MTU, link mode, and port speed, access control, user authentication, RADIUS server settings, and firewall filters. A user with tenant administrator privileges can add the following profiles to CSO and deploy them on the switch to configure the switch and the switch ports:

- **Authentication profiles**: Authentication profiles are used to implement network access control (NAC).

  An authentication profile defines:

  - the authentication method
  - fallback options
  - other settings such as number of retries, maximum number of authentication requests that can be allowed for a supplicant, authentication server timeout, and so on, related to the communication between the switch and the supplicant (a user or device such as printer).

  You can reference an authentication profile directly in a port profile or assign the authentication profile to a port when you configure the port manually.

  See “Add Authentication Profiles” on page 23 for details.

- **Firewall filter**: Firewall filters are used to deny or permit network access to supplicants based on the filter terms.

  You can reference an egress firewall filter and an ingress firewall filter in a port profile. You can also assign the firewall filters to a port when you configure the port manually.

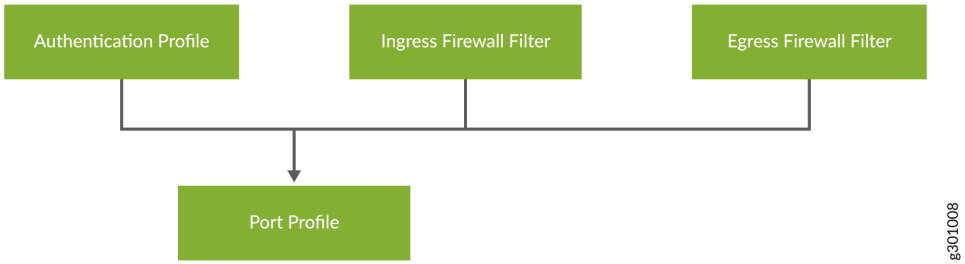
  See “Add Firewall Filters and Terms” on page 28for details.

- **Port profiles**: Port profiles are used to define the behavior of a port. You can use port profiles to simultaneously provision multiple ports with the same set of attributes. A port profile includes the following:

  - Authentication profile (Optional)
  - Firewall filters (Optional)
  - Link settings
  - Storm control settings
  - Power over Ethernet (PoE) settings
  - Port security settings

  A port profile has an authentication profile and one ingress firewall filter and one egress firewall filter assigned to it. Figure 6 on page 21 shows the relationship between an authentication profile, firewall filters, and a port profile.

Figure 6: Relationship Between a Port Profile, an Authentication Profile, and Firewall Filters



See "Add Port Profiles" on page 31 for details about adding a port profile to CSO.

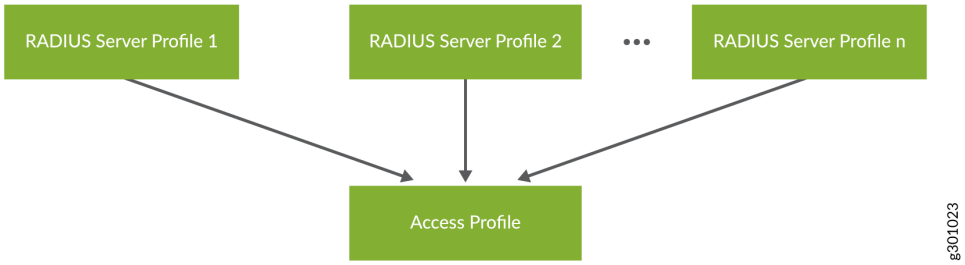
- **RADIUS server profiles**: RADIUS server profiles are used to define the RADIUS server for authentication and accounting. You define the RADIUS server IP address, password, authorization ports, accounting ports, retry counts, and server timeout in this profile.

  A RADIUS server profile is referenced by an access profile and deployed on the switch when the access profile is deployed. See "Add RADIUS Server Profiles" on page 36 for information about adding RADIUS server profiles.

- **Access profiles**: Access profiles are used to define the list of RADIUS servers to be used for authentication and accounting. An access profile has one or more RADIUS server profiles assigned to it.

  Figure 7 on page 21 shows the relationship between the a RADIUS profile and an access profile.

Figure 7: Relationship Between RADIUS Profiles and an Access Profile



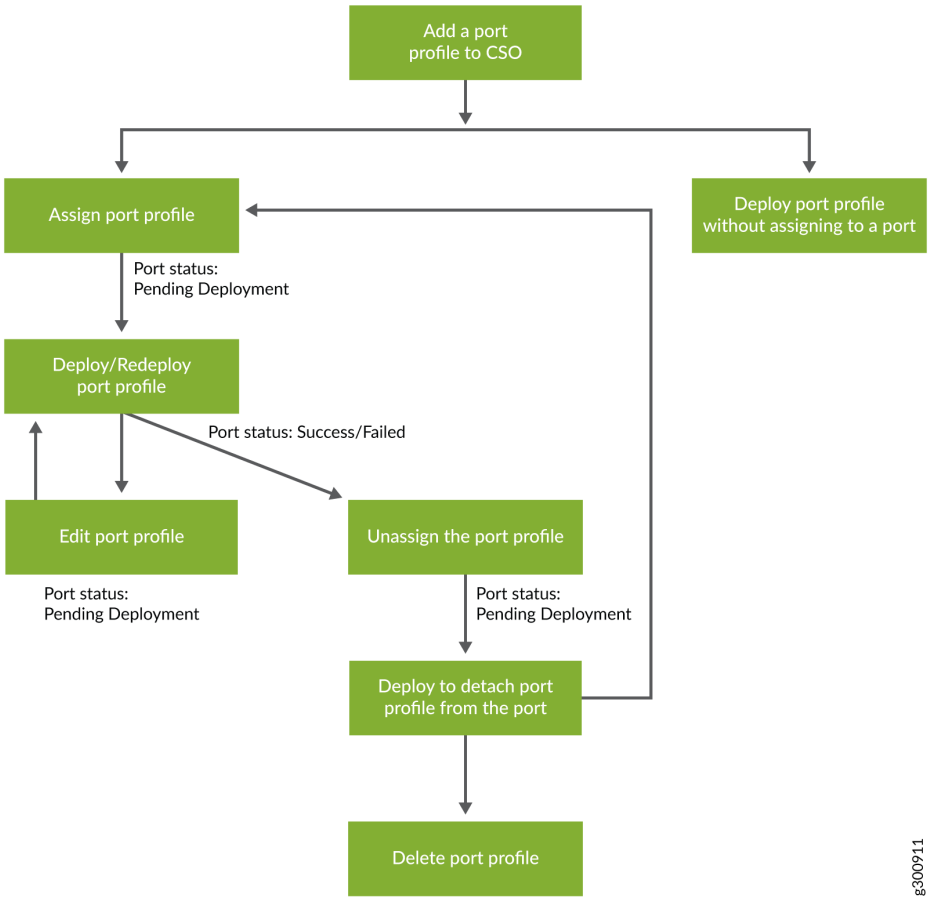
An access profile, deployed on a switch, is referenced by an authentication profile when 802.1x authentication is configured on the switch port.

See "Add Access Profiles" on page 38 for details.

Life Cycle of a Port Profile

Figure 8 on page 22 shows the life cycle of a port profile.

Figure 8: Life Cycle of a Port Profile



The life cycle of a port profile is as follows:

1. Add a port profile to CSO.
2. Assign the port profile to one or more ports on a switch.

   When you assign the port profile, the deployment status of the port is set to *Pending Deployment* indicating that the profile is only assigned to the port.
3. Deploy the port profile on one or more ports.

   During the deployment, that is, when the configuration is being committed on the port, the deployment status is changed to *In Progress*. If the deployment job completes successfully, the deployment status of the port is set to *Success*; otherwise, the deployment status is set to *Failed*.

4. Edit the port profile.

   When you edit the port profile, an authentication profile or a firewall filter associated with the port profile, the deployment status of the port profile is set to *Pending Deployment*.

5. Redeploy the port profile to ensure the changes are reflected in the port configuration.

   During the redeployment, the deployment status of the port is changed to *In Progress*. If the deployment job completes successfully, the deployment status of the port is set to *Success*; otherwise, the deployment status is set to *Failed*.

Add Authentication Profiles

Use the Add Authentication Profiles page in Customer Portal to add authentication profiles.

Adding an authentication profile involves the following steps:

1. Define the primary and secondary methods for authenticating a supplicant—802.1x (dot1x), MAC RADIUS.
2. Define the action that the port must take when the RADIUS server is not reachable or a user is not authenticated (fallback options).
3. Define the authentication process parameters, such as the number of times that the switch can request for user authentication, whether a user must be reauthenticated at regular intervals, the number of times a switch can attempt to contact the RADIUS server for authenticating a user, and so on.

To add an authentication profile:

1. Select **Configuration > SD-LAN > Authentication Profiles** in Customer Portal.

   The Authentication Profiles page appears, displaying the existing authentication profiles.

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

   The Add Authentication Profiles wizard appears.

3. Complete the configuration according to the guidelines provided in Table 4 on page 24.

   NOTE: Fields marked with * are mandatory.

4. Click **OK**.

An authentication profile is added. You are returned to the Authentication Profiles page where a confirmation message is displayed.

After you add an authentication profile, you can assign it to a port profile. See "Add Port Profiles" on page 31.

Table 4: Fields on the Add Authentication Profile Page

Setting	Guideline
General	
Profile Name	Enter a unique name for the authentication profile, which can only contain alphanumeric characters and hyphen (-); 15-character maximum.
Profile Description	Enter a description for the authentication profile.
Supplicant Mode	Select a mode for authenticating the supplicant: • Single—Authenticates only the first supplicant in a LAN. All other supplicants in the LAN that connect to the port later are allowed or denied access without any authentication, based on the first supplicant's authentication. • Single Secure—Allows only one supplicant in a LAN to connect to the port. No other supplicant in the LAN is allowed to connect until the first supplicant logs out. • Multiple—Allows multiple supplicants in a LAN to connect to the port. Each supplicant is authenticated individually.
Authentication Method	
Primary Method	Select the primary method of authenticating a supplicant: • dot1x—IEEE 802.1X standard for port-based network access control (PBNAC); protects Ethernet LANs from unauthorized user access. The 802.1x method blocks all traffic to and from a supplicant at the port until the supplicant's credentials are presented and matched on the authentication server (a RADIUS server). When the supplicant is authenticated, the switch allows traffic from and to the supplicant to transmit through it. • MAC RADIUS—Used for supplicants, connected in a LAN that need to access network resources, such as printer or camera, but do not support the 802.1X standard. When a switch detects a supplicant that is not 802.1X-enabled, the switch transmits the MAC address of the supplicant to the authentication server. The server then tries to match the MAC address with a list of MAC addresses in its database. If the MAC address matches an address in the list, the supplicant is authenticated.

Table 4: Fields on the Add Authentication Profile Page *(continued)*

Setting	Guideline
Secondary Method	The secondary method for authenticating a supplicant when the switch is unable to validate a supplicant by using the primary method: • None • dot1x, when MAC RADIUS is selected as the primary authentication method. • MAC RADIUS, when dot1x is selected as the primary authentication method.
Fallback Options You can configure authentication fallback options to specify how supplicants connected to a switch are supported if the RADIUS authentication server becomes unavailable or sends a RADIUS access-reject message.	
Server Fail	Select an action that the switch applies to supplicants when the authentication servers are not reachable. The switch can accept or deny access to supplicants or maintain the access already granted to supplicants before the RADIUS timeout occurred. You can also configure the switch to move the supplicants to a specific VLAN. • None—No action is taken. If network access is already granted to a supplicant, the access is maintained. • Deny—Network access is denied to the supplicant. • Permit—Network access is permitted to the supplicant. If a RADIUS server timeout occurs during reauthentication, traffic is allowed from and to the supplicant because the supplicant is already authenticated. • Use Cache—Recognizes already connected supplicants and reauthenticates the supplicants when there is a RADIUS timeout; new supplicants are denied access. • VLAN ID—Moves a supplicant to a specified VLAN (server-fail VLAN) if a RADIUS server timeout occurs: If you select this option, enter the VLAN ID in the text box that appears below the Server Fail field. **NOTE:** The server-fail VLAN should be already configured on the site containing the switch.
VLAN ID	If you select VLAN ID for the Server Fail option, enter the VLAN ID of the VLAN to which the supplicant must be assigned.

Table 4: Fields on the Add Authentication Profile Page *(continued)*

Setting	Guideline
Server Reject	The action the switch takes when the switch is unable to validate a supplicant because of incorrect credentials provided by the supplicant: • None—No action is taken and the supplicant is denied network access. • VLAN ID—Moves the supplicant to a specified VLAN (server-reject VLAN) with limited network access (Internet only). The server-reject VLAN is already configured on the switch. If you select this option, enter the VLAN ID in the text box that appears below the Server Reject field. **NOTE:** The server-reject VLAN should be already configured on the site containing the switch.
VLAN ID	If you select VLAN ID for the Server Reject option, enter the VLAN ID to which the supplicant must be assigned.
Guest	Select an action to be taken for a guest (corporate guest or supplicants that are not 802.1x enabled):. • None—No action is taken and the supplicant is denied network access. • VLAN ID—Move the supplicants to a specified VLAN (guest VLAN) with limited network access (Internet only). If you select this option, enter the VLAN ID of the guest VLAN in the text box that appears below this field. **NOTE:** The guest VLAN should be already configured on the site containing the switch.
VLAN ID	Enter the VLAN ID of the guest VLAN.
Advanced Settings	
Transmit Period	Enter the number of seconds that the switch waits before retransmitting the initial authentication request to the supplicant. Range: 1 through 65,535 seconds. Default: 30 seconds.

Table 4: Fields on the Add Authentication Profile Page *(continued)*

Setting	Guideline
Maximum Requests	Enter the maximum number of times that authentication request packets are retransmitted to a supplicant before the authentication session times out. Range: 1 through 10. Default: 2.
Retries	Enter the number of times that the switch attempts to contact an authentication server for authenticating a supplicant after an initial failure. Range: 1 through 10. Default: 3.
Quiet Period	Enter the number of seconds that the port remains in the wait state following a failed authentication exchange with the supplicant, before reattempting authentication. Range: 0 through 65,535 seconds. Default: 3 seconds.
Reauthentication	Click to enable or disable (default) reauthentication of the supplicant after a specified interval. If you enable this option, you must provide the reauthentication interval.
Reauthentication Interval	If you enable reauthentication, enter the number of seconds after which a supplicant must be reauthenticated. Range: 1 through 65,535 seconds. Default: 3600 seconds.
Supplicant Timeout	Enter the number of seconds that the port must wait for a response from the supplicant, before considering a timing out and resending the request. Range: 1 through 60 seconds. Default: 30 seconds.
RADIUS Server Timeout	Enter the number of seconds that the port waits for a reply from the RADIUS server when authenticating a supplicant before timing out and invoking the server-fail action (action that the switch applies to supplicants when the authentication servers are not reachable). Range: 1 through 60 seconds. Default: 30 seconds.

RELATED DOCUMENTATION

Add Port Profiles | 31

Add Access Profiles | 38

Add Firewall Filters and Terms

Use the Add Firewall Filter page to add a new ingress or egress firewall filter.

To add a firewall filter:

1. Select **Configuration > SD-LAN > Firewall Filters**.

   The EX Firewall Filters page appears.

2. Click the add icon (+) to add a new firewall filter.

   The Add Firewall Filter page appears.

3. Complete the configuration according to the guidelines provided in Table 5 on page 29.

   NOTE: Fields marked with * are mandatory.

4. Click **OK**.

   The firewall filter is added to CSO. You are returned to the EX Firewall Filters page where a confirmation message is displayed.

5. Select the firewall filter added in 4 and click the add icon (+).

   The option to add firewall term appears inline on the *Firewall-Filter-Term-Name* page.

6. Complete the configuration according to the guidelines provided in Table 6 on page 29.

7. Click **Save** to save the changes.

   A new firewall term with the provided configuration is added and a confirmation message is displayed.

Table 5: Fields on the Add Firewall Filter Page

Field	Description
Name	Enter a unique name for the firewall filter. The name can contain only alphanumeric characters and hyphen (-); the maximum length allowed is 15 characters.
Description	Enter a description for the firewall filter.

Table 6: Fields on the <Firewall-Filter-Term-Name> Page

Field	Description
Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 255 characters. If you do not enter a name, the term is saved with a default name assigned by CSO.
Description	Enter a description for the firewall filter term; maximum length is 1024 characters.
Counter	Click the toggle button to enable) or disable (default) the counter. The counter counts the number of packets that pass this filter term. **NOTE:** If you have enabled the counter for the firewall filter, you cannot add the firewall filter as an egress filter.
Logging	Click the toggle button to enable or disable (default) logging. By enabling logging, CSO logs the packet's header information in the Routing Engine. **NOTE:** If you have enabled logging for the firewall filter, you cannot add the firewall filter as an egress filter.
Source	Click the add icon (**+**) to select the source endpoints from the displayed list of IP addresses, MAC addresses, protocols, or ports to the firewall filter term. You can also select a source end point using the methods described in *Selecting Firewall Source*.
Destination	Click the add icon (**+**) to select the destination endpoints from the displayed list of IP addresses, MAC addresses, protocols, or ports to the firewall filter term. You can also select a destination end point using the methods described in *Selecting Firewall Destination*.
Select Action	Click the add icon (+) to choose whether you want to permit or deny the traffic between the source and destination endpoints. • **Allow**—Device permits the traffic. • **Deny**—Device silently drops all packets for the session.

Table 6: Fields on the <Firewall-Filter-Term-Name> Page *(continued)*

Field	Description
Endpoints	To add an endpoint to the source or destination: 1. Click **Select Source** or **Select Destination** text box and then click the lesser-than icon (<) on the right side of the page to open the End Points panel. The End Points panel displays the endpoints from addresses, MAC, protocols, and ports relevant to the source or destination based on your selection. **NOTE:** You can also search for a specific end point using the search option. 2. Select the endpoint you want to add and click the check mark icon (**√**) to add it the source or destination. The selected endpoint is added to the source or destination. To add new source and destination end points: 1. Click the less-than icon (<) on the right side of the page to open the End Points panel. 2. Click the add icon (+) on the top right of the End Points panel. A list of endpoints that you can add is displayed. 3. Select the endpoint you want to add. You can add the following endpoints: • Address or address group. • MAC address. • Protocol. • Port. 4. Click **Save** to add the new endpoint. The endpoint that you added is listed in the **End Points** panel. 5. Select the endpoint that you want to add to the source or destination, and click on the check mark icon (**√**). The endpoint is added to the source or destination as specified.

WHAT'S NEXT

> After you configure the firewall filter, assign the firewall filter as an ingress filter or egress filter in a port profile. See Add Port Profiles | 31.

Add Port Profiles

Use the Add Port Profiles page in Customer Portal to add port profiles. You add a port profile by assigning an authentication profile, a firewall filter for the ingress traffic, a firewall filter for the egress traffic, and configuring port parameters.

To add a port profile:

1. Select **Configuration > SD-LAN > Port Profiles** in Customer Portal.

   The Port Profiles page appears.

2. Click the add icon (**+**) to add a new port profile.

   The Add Port Profile wizard appears. The wizard provides step-by-step procedures to add the port profile.

3. Complete the configuration according to the guidelines provided in Table 7 on page 31.

   NOTE: Fields marked with * are mandatory.

4. Click **OK**.

   The port profile is added to CSO. You are returned to the Port Profiles page where a confirmation message is displayed.

After you add a port profile, you can deploy the port profile on one or more ports of the switch. See *Deploy or Redeploy a Port Profile*.

Table 7: Port Profile Settings

Setting	Guideline
General	

Table 7: Port Profile Settings *(continued)*

Setting	Guideline
Profile Name	Enter a unique name for the port profile which can contain only alphanumeric characters and hyphen (-); 32-characters maximum.
Profile Description	Enter a description for the port profile.
Basic Settings	
Port Mode	Select whether the port should be configured as a trunk port or an access port: • Trunk—The port can be used to connect with other switches or routers. • Access—The port can be used to connect to access points and end-user devices such as laptops or printer.
Port Authentication Settings	
Authentication Profile	Select an authentication profile to be used in the port profile. **NOTE:** An authentication profile defines the authentication method and other parameters related to communication between the switch and the supplicant. You must configure the authentication profile before referencing it in the port profile. To add an authentication profile, see “Add Authentication Profiles” on page 23. If you select None (default), no authentication profile is associated with the port profile. You can use this option when you do not want 802.1x authentication to be configured on a port.
Firewall Filter	
Firewall Filter Profile (Ingress)	Select a firewall filter profile to be used for the ingress traffic. You must configure the firewall filter before referencing it in the port profile. .
Firewall Filter Profile (Egress)	Select a firewall filter profile to be used for the egress traffic. You must configure the firewall filter before referencing it in the port profile. .
Advanced Settings	

Table 7: Port Profile Settings *(continued)*

Setting	Guideline
Link Settings	Click the toggle button to enable or disable (default) link settings on a port. If you disable this setting, the port uses the default configurations for auto negotiation, flow control, MTU, speed, and link mode. Enable this option to modify the default configuration for auto negotiation, flow control, MTU, and so on.
Auto Negotiation	Click the toggle button to enable (default) or disable autonegotiation on the port. Auto negotiation enables a port to determine the data transmission speed and the duplex mode based on the speed and duplex mode of the peer port. If you have enabled autonegotiation and also configured link mode and speed, the ports use the configured values for link mode and speed. If you disable autonegotiation, you must configure values for link mode and speed.
Flow Control	Click the toggle button to enable (default) or disable flow control on a port. Flow control enables a port to regulate network traffic so that there is no data loss during congestion. If you disable flow control, you lose data during congestion.
MTU	Enter the size (in bytes) of the maximum transmission unit (MTU) that can be transmitted through a port. Range: 256 to 9,216 bytes Default: 1,514 bytes
Speed	Select the maximum transmission speed of a port (in GB or MB). If you enable auto-negotiation and select a transmission speed, the port uses the value configured here for transmission speed. Default: 1G

Table 7: Port Profile Settings *(continued)*

Setting	Guideline
Link Mode	Select the mode of the links configured on a port: • Automatic (default) —The port automatically selects the duplex mode based on the duplex mode of the peer port. • Full Duplex—The port allows data to be sent and received at the same time over a link. • Half Duplex—The port allows data to be either only received or sent at a given time over a link. If you enable autonegotiation and also select a value for link mode, the port considers the value configured here for the operating mode of the links established on the port.
Storm Control Settings	Click the toggle button to enable or disable (default) storm control settings on a port. If you disable this setting, the port uses the defalt value for storm control. Enable this option to modify the default storm control value.
Storm Control	Enter the bandwidth (in kbps) or the percentage of the bandwidth, beyond which a port can drop packets. Also, select whether the value you enter indicates the percentage or the bandwidth, from the drop-down list. The default unit is percentage. Range: For bandwidth, 100 through 100,000,000 kbps. For percentage, 1 through 100. Default: 80 percent.
Power over Ethernet (PoE) Settings	Click the toggle button to enable or disable (default) PoE on a port. If you disable this setting, the default PoE setting is configured on a port when you deploy the profile on the port. Enable this option to modify the default PoE settings.
Maximum Power	Enter the maximum power (in Watts) that a port can provide. Range: 1 through 90 Watts. Default: 30 Watts.

Table 7: Port Profile Settings *(continued)*

Setting	Guideline
Priority	Select a priority (Low or High) for a port to be used as a source for powering a device connected to the port. If power is insufficient for all PoE ports, the PoE power to low-priority ports is shut down before power to high-priority ports is shut down. Among ports that have the same assigned priority, the power priority is determined by port number, with lower-numbered ports having higher priority. Default: Low
Port Security Settings	Click the toggle button to enable or disable (default) security on a port. If you disable this setting, the default port security is configured on a port when you deploy the profile on the port. Enable this option to modify the default settings.
Trust DHCP	Click the toggle button to enable (default) or disable trusting traffic from a DHCP server. If you disable this option, the port drops packets sent to and received from a DHCP server.
MAC Limit	Click the toggle button to enable or disable (default) setting the maximum number of MAC addresses that can be stored in the MAC table for a port. If you enable MAC Limit, you must configure a value for MAC limit and MAC limit action. If you disable this option, you cannot limit the MAC addresses that are learnt within a VLAN and, therefore, enforce security against the flooding of the Ethernet switching table.
MAC Limit	Enter the maximum number of MAC addresses that a switch can store in the MAC table for a port. Range: 1 through 10,000. Default: 1.

Table 7: Port Profile Settings *(continued)*

Setting	Guideline
MAC Limit Action	Select the action that a port must take when the number of entries in the port MAC table exceeds the MAC limit value: • Drop (Default)—Drop the packet, but do not generate an alarm • Shutdown—Disable the port and generate an alarm, an SNMP trap, or a system log entry. • Drop and Log—Drop the packet and generate an alarm, an SNMP trap, or system log entry.

RELATED DOCUMENTATION

Add Access Profiles | 38

Add RADIUS Server Profiles

Use the Add RADIUS Server Profile page in Customer Portal to configure RADIUS server profiles. In a RADIUS server profile, you can define the RADIUS server IP address, password, authorization and accounting ports, retry counts, and server timeout.

To add a RADIUS server profile:

1. Select **Configuration > SD-LAN > RADIUS Server Profiles** in Customer Portal.

   The RADIUS Server Profiles page appears.

2. Click the **Add** icon (**+**) to add a RADIUS server profile.

   The Add RADIUS Server Profile page appears.

3. Complete the configuration according to the guidelines provided in Table 8 on page 37.

   NOTE: Fields marked with * are mandatory.

4. Click **Finish**.

A RADIUS server profile is added to CSO. You are returned to the RADIUS Server Profiles page where a confirmation message is displayed.

After you add a RADIUS server profile, you can add an access profile by using the RADIUS server profile. See "Add Access Profiles" on page 38 for details.

Table 8: RADIUS Server Profile Settings

Setting	Guideline
General	
Server Name	Enter a unique name for the RADIUS server, which can contain only alphanumeric characters and hyphen (-). 64-character maximum.
Server Address	Enter the IPv4 address of the RADIUS server.
Secret	Configure the password to use with the RADIUS server. The secret password used by the local switch must match the one configured on the server. The length must be between 6 and 21 characters. You can include spaces if the character string is enclosed in quotation marks.
Advanced Settings	
Authentication Port	Enter the software port number that you want to use for authentication. Range: 1 through 65,535. Default: 1812.
Authentication Retry Count	Enter the number of times that the switch can contact a RADIUS server for authenticating a supplicant when no response is received from the authentication server. Range:1 through 100. Default: 3.
Authentication Timeout	Enter the number of seconds that the switch can wait for a response from the RADIUS server for an authentication request before retrying authentication of a supplicant. Range: 1 through 1000 seconds. Default: 3 seconds.

Table 8: RADIUS Server Profile Settings *(continued)*

Setting	Guideline
Accounting Port	Enter the software port number that you want to use for accounting. Range: 1 through 65,535. Default: 1813.
Accounting Retry Count	Enter the number of times that the switch can contact an accounting server when no response is received from the accounting server. Range: 1 through 100. Default: 3.
Accounting Timeout	Enter the number of seconds that the switch can wait for a response from the accounting server before timing out. Range: 1 through 1000 seconds. Default: 3 seconds.

RELATED DOCUMENTATION

Add Authentication Profiles | 23

Dissociating an Access Profile

Deploying an Access Profile on a Switch

Add Access Profiles

An access profile defines a list of RADIUS authentication servers and RADIUS accounting servers, and their priorities. Use the Add Access Profile page in Customer Portal to add access profiles to CSO.

To add an access profile:

1. Select **Configuration > SD-LAN > Access Profiles** in Customer Portal.

   The Access Profiles page appears.

2. Click the **Add** icon (+) to add an access profile.

The Add Access Profiles page appears.

3. Complete the configuration according to the guidelines provided in Table 9 on page 39.

> **NOTE:** Fields marked with * are mandatory.

4. Click **OK**.

   An access profile is added. You are returned to the Access Profiles page where a confirmation message is displayed.

After you add an access profile, you can deploy it on a switch; see *Deploying an Access Profile on a Switch*.

Table 9: Access Profile Settings

Setting	Guideline
General	
Profile Name	Enter a unique name for the access profile, which can contain only alphanumeric characters and hyphen (-); 64-character maximum.
Profile Description	Enter a description for the access profile.

Table 9: Access Profile Settings *(continued)*

Setting	Guideline
Authentication Servers	Add authentication servers to the access profile. To add authentication servers: 1. Click the **Add** icon (+). The Add Authentication Server(s) page appears. 2. Select a server from the Available list and click the **Right Arrow** icon to move it to the Selected list. Alternatively, if you want to add a new authentication server, click the **Add New RADIUS Server Profile** button and move it to the list of selected servers; see "Add RADIUS Server Profiles" on page 36 for details. 3. Click **OK** to save the list of authentication servers. The authentication servers are used according to their priority. The priority is assigned in the order in which the servers are listed, with the highest priority being assigned to the server on the top of the list. To change the priority, reorder the servers in the list by dragging and dropping them.
Accounting Servers	Add accounting servers to the access profile. To add accounting servers: 1. Click the **Add** icon (+). The Add Accounting Server(s) page appears. 2. Select a server from the Available list and click the **Right Arrow** icon to move it to the Selected list. Alternatively, if you want to add a new accounting server, click the **Add New RADIUS Server Profile** button and move it to the list of selected servers; see "Add RADIUS Server Profiles" on page 36 for details. 3. Click **OK** to save the list of accounting servers. The accounting servers are used according to their priority. The priority is assigned in the order in which the servers are listed, with the highest priority being assigned to the server on the top of the list. To change the priority, reorder the servers in the list by dragging and dropping them.

Table 9: Access Profile Settings *(continued)*

Setting	Guideline
Revert Interval	Enter a revert interval, which is the amount of time the switch waits after a RADIUS server has become unreachable before rechecking the connection. If the server is still not reachable, the server next in the priority list is used for authentication and accounting. Range: 0 through 604,800 seconds Default: 60 seconds

RELATED DOCUMENTATION

Add RADIUS Server Profiles | **36**

Dissociating an Access Profile

Add Port Profiles | **31**

3

CHAPTER

Onboard Devices to CSO

Add and Provision a Switch Overview | **43**

Add a Switch Behind an Internet Gateway | **47**

Add a Switch Behind a CPE | **57**

Add a Switch Behind a Next-Generation Firewall | **73**

Add Switches to an Existing SD-LAN Site | **80**

Add Switches to an Existing SD-WAN Site | **91**

Add and Provision a Switch Overview

IN THIS SECTION

- Switch Behind an Internet Gateway Overview | 44
- Switch Behind a CPE or Next-Generation Firewall Overview | 45

A user with tenant administrator privileges can onboard EX Series switches to and use Contrail Service Orchestration (CSO) to provision, deploy, and monitor EX Series switches in branch and campus deployments of enterprise networks.

You can use CSO to manage and configure the following EX Series Switches:

- EX2300, EX2300 Virtual Chassis
- EX3400, EX3400 Virtual Chassis
- EX4300, EX4300 Virtual Chassis
- EX4600, EX4600 Virtual Chassis
- EX4650, EX4650 Virtual Chassis

You can onboard a switch to CSO in one of the following ways:

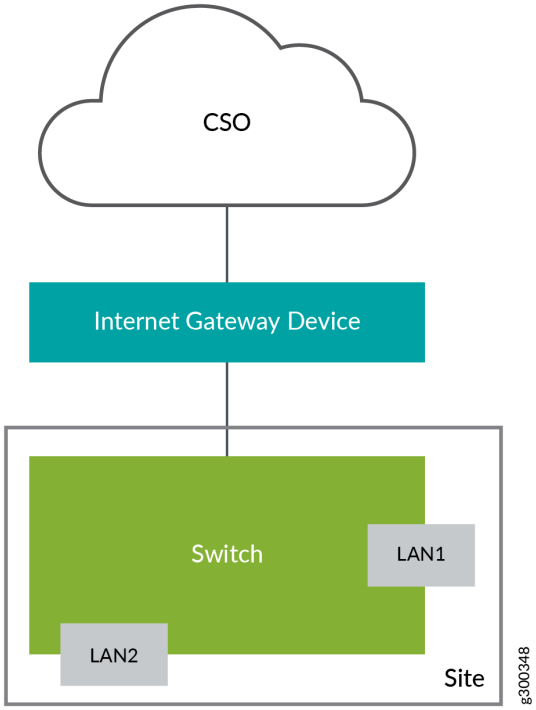
- By adding a site with the switch and connecting it to an Internet gateway device (standalone switch).
- By adding a site with a CPE and the switch connected to the CPE.
- By adding a site with a next-generation firewall and the switch connected to the next-generation firewall.
- By adding the switch to a site that already has one or more switches connected to an Internet gateway and connecting the switch to the Internet gateway.
- By adding the switch to a CPE or next-generation firewall that is already provisioned and managed by CSO.

NOTE: You can add multiple switches to a site that has a CPE or a next-generation firewall; However, in this implementation, you must manage the connectivity and configuration between the switches and the CPE or next-generation firewall either by using configuration templates in CSO or manually.

Switch Behind an Internet Gateway Overview

Figure 2 on page 14 shows a site with a switch, managed by CSO, connected to an Internet gateway. The gateway can be a device from a manufacturer other than Juniper Networks. You can also add multiple switches behind the Internet gateway to be managed by CSO.

Figure 9: Standalone Switch



You can provision the switches by either using ZTP (if the EX Series switch supports Phone-Home client) or manually configure the stage-1 configuration on the switch. See"Add a Switch Behind an Internet Gateway" on page 47 for details.

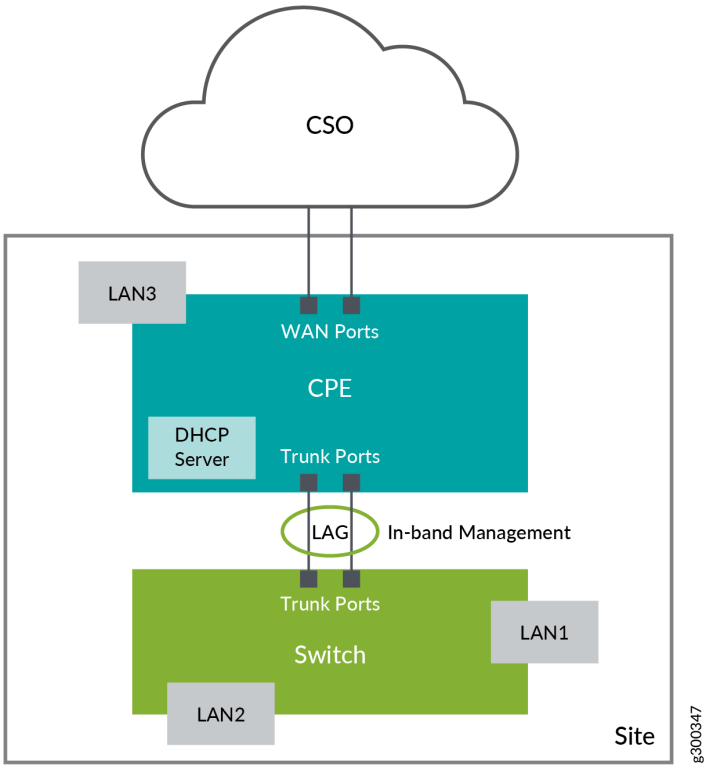
NOTE:

- Only EX Series switches running 18.4R2.7 or 18.4R3.3 Junos OS support ZTP.
- EX4300 MP, EX4600, and EX4650 switches do not support Phone-Home client. You must disable ZTP and manually configure the stage-1 configuration on the switches.

Switch Behind a CPE or Next-Generation Firewall Overview

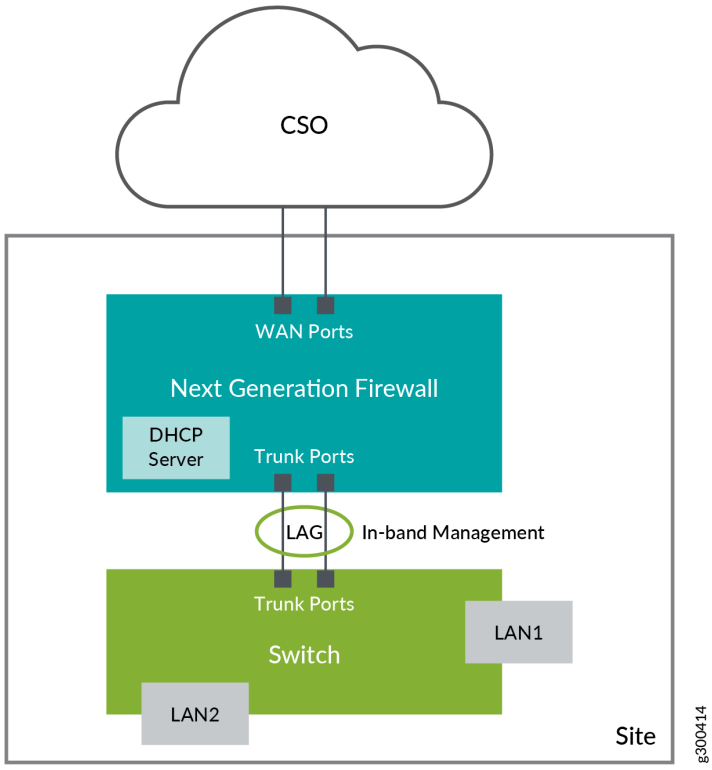
Figure 10 on page 45 shows an example of a site with a CPE and a switch connected to the CPE.

Figure 10: Switch Behind a CPE



In Figure 10 on page 45, the switch is connected to two LAN segments (LAN1 and LAN2) and the CPE. The CPE is connected to a LAN segment (LAN3) and to the EX Series switch. The switch can also be connected to a next-generation firewall as shown in Figure 11 on page 46.

Figure 11: Switch Behind a Next-Generation Firewall



NOTE: CSO does not provide an option to configure LAN segments while configuring a site with a next-generation firewall. You can add a LAN segment to the next-generation firewall by using configuration templates.

The switch and the CPE or firewall can be connected through a trunk port. However, you can use two trunk ports to connect the CPE and the switch and combine them to form a Link Aggregation Group (LAG) for higher throughput and redundancy. Traffic from LAN segments connected to the switch are routed to the CPE or firewall through the trunk ports for further routing into WAN.

You can also use the trunk ports to carry the management traffic for the switch, in addition to data (in-band management).

NOTE: The ae0 port of the SRX Series device is configured as the trunk port for communication with the switch.

The DHCP server, configured on the CPE or firewall:

- Allocates unique IP addresses to the access devices connected to the switch.
- Provides management connectivity to the switch.

During ZTP of a site with both WAN and LAN capabilities, the switch is provisioned after the CPE or firewall is provisioned.

When you add a switch to an already provisioned site, CSO redeploys the stage-2 configuration on the CPE or firewall to configure DHCP and LAG. The DHCP configuration enables management connectivity to the switch and allows CSO to discover and provision the switch.

For details about adding a switch behind a CPE, see "Add a Switch Behind a CPE" on page 57 and for details about adding a switch behind a next-generation firewall, see "Add a Switch Behind a Next-Generation Firewall" on page 73.

Add a Switch Behind an Internet Gateway

If you are adding a Virtual Chassis, ensure that you prepare the Virtual Chassis for onboarding to CSO. See "Prepare a Virtual Chassis for Onboarding to CSO" on page 137 for details.

To add a switch behind an Internet gateway for managing by CSO:

1. Select **Resources > Site Management**.

   The Sites page appears.

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

   The Add Site for *Tenant-Name* page appears.

3. Complete the configuration according to the guidelines provided in Table 10 on page 48.

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

4. 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.

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

After you click OK, site activation is initiated and the **Site Activation: *Site-Name*** page appears. If you add multiple switches, the progress of the steps executed for activating each switch is displayed.

6. - 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 10: Fields on the Add Site for Tenant-Name Page (LAN Capability)

Field	Description
Site Information	
Site Name	Enter a unique name for the site. You can use alphanumeric characters and hyphen (-). The maximum length allowed is 32 characters.

Table 10: Fields on the Add Site for Tenant-Name Page (LAN Capability) *(continued)*

Field	Description
Site Group	Select a site group to which you want to assign the site.
Site Capabilities	
LAN Capabilities	Select **LAN** to include LAN capabilities in the site.
Address and Contact Information	
Street Address	Enter the street address of the site.
City	Enter the city where the site is located.
State/Province	Enter the state or province where the site is located.
ZIP/Postal Code	Enter the postal code for the site.
Country	From the list, select the country where the site is located. Click the **Validate** button to verify the address. • The **site address verification successful** message is displayed if the address is verified. You can click the **View location on a map** link to see the address location. • If the address cannot be verified, the **Site address could not be validated** message is displayed. If you enter the wrong address and click the **Validate** button to verify the address, the **Site address could not be validated message** is displayed.
Contact Name	Enter the name of the contact person for the site.
Email	Enter the e-mail address of the contact person for the site.
Phone	Enter the phone number of the contact person for the site.
Advanced Configuration	
Domain Name Server (DNS)	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.

Table 10: Fields on the Add Site for Tenant-Name Page (LAN Capability) *(continued)*

Field	Description
NTP Server	Specify the IP addresses of one or more NTP servers.
Select Timezone	Select the time zone of the site from the list.
LAN	
Switch Devices	Displays the switches that you have added to the site. • To add a switch, click the **+** icon on the top right corner of the Switch Devices table. You can add multiple switches only to an SD-LAN site. The Add New Switch page appears. See Table 12 on page 51 for details. • To edit details of a switch, select the switch and click the **Edit** icon on the top right corner of the Switch Devices table. The Edit Switch Details page appears, displaying the same parameters that you configured while adding a switch. Modify the parameters as needed and Click **OK**. The changes that you made for the switch are saved and the updated parameters appear on the Switch Devices table. • To delete one or more switches, select the switches and click the **Delete** icon on the top right corner of the Switch Devices table. • To manage the configuration of one or more switches added to the site, select the switches from the list and click **Configuration**. The Switch Configuration page appears. See Table 13 on page 56 for details.
LAN Segments	Displays the VLANs and their IDs that you configured on the switch. • Optional: To add a VLAN, click the **+** icon on the top, right corner of the LAN Segments table. The Create LAN Segment page appears. See Table 11 on page 51 for details. • To edit details of a VLAN, select the LAN segment and click the **Edit** icon (pencil) on the top right corner of the LAN Segments table. The Edit LAN Segment page appears, displaying the same fields that are presented when you add a VLAN. Modify the parameters as needed and click **OK**. The changes that you made for the LAN segment are saved and the updated parameters appear on the LAN Segments table. • To delete one or more VLANs, select the VLANs and click the **Delete** icon (trash can) on the top right corner of the LAN Segments table.

Table 11: Fields on the Add LAN Segment Page when Adding a Site With LAN Capability

Field	Description
Add LAN Segment	
Name	Enter a name for the VLAN. The name for a VLAN should be a unique string of alphanumeric characters and some special characters (. -). No spaces are allowed and the maximum length allowed is 15 characters.
VLAN ID	Enter the VLAN ID for the VLAN. Range: 2 through 4093.

Table 12 on page 51 describes the fields on the Add New Switch page.

Table 12: Fields on the Add New Switch page

Field	Description
Device Profile	
Device Name	Enter a unique 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, 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.
Switch Details	

Table 12: Fields on the Add New Switch page *(continued)*

Field	Description
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. • Before you add a Virtual Chassis in CSO, ensure that the Virtual Chassis is setup. See "Prepare a Virtual Chassis for Onboarding to CSO" on page 88for details about setting up a Virtual Chassis. In addition, click the **View Prerequisite Configurations** link to view the requirements for adding a Virtual Chassis in CSO. • Currently, 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 12: Fields on the Add New Switch page *(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 Master 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 type, device model, 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 and EX4300 devices to act as a Virtual Chassis, all the corresponding member devices are interconnected through Virtual Chassis ports (VCPs). For EX2300, EX4600, and EX4650 devices to act as a Virtual Chassis, the uplink Ethernet ports are configured as VCPs manually and the member devices are interconnected.

Table 12: Fields on the Add New Switch page *(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 member 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 Serial Number 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 the last added member. For information on the number of devices that can be added, see "Supported Device Types, Modes, and Number of Members Allowed in a Virtual Chassis" on page 88 **NOTE:** The Routing Engine toggle button corresponding to Member 0 is always enabled, indicating that Member 0 always acts as the primary. To select a member as backup, click to enable the Routing Engine toggle button 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 12: Fields on the Add New Switch page *(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 5 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.
Boot Image	Select the boot image from the list if you want to upgrade the image for the switch. The boot image is the latest device image that is 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 automatic upgrade procedure. The boot image is populated based on the device template that you have selected while creating a site. **NOTE:** This option is not available for a Virtual Chassis. To provision a Virtual Chassis in CSO, you must manually upgrade the image to either JUNOS 18.4R2.7 or 18.4R3.3.
Auto activate	Click the toggle button to enable (default) or disable automatic activation of the switch when the switch is detected by CSO (that is, management status of the device is Device_Detected). When you enable this field, zero-touch provisioning (ZTP) of the switch is automatically triggered when the device communicates with CSO. **NOTE:** The switch must be powered on for automatic activation when you enable this option.
Activation code	If you disabled the **Auto activate** field, enter the activation code to be used for manually activating the switch For information on manually activating a switch, see *Manually Activating a Switch*.

Table 13 on page 56 describes the tabs on the Switch Configuration page.

The Access Profiles tab and Port Profiles tab are available only if you have added a physical switch or a preprovisioned Virtual Chassis, and the selected switches are of the same device type and model. If you

have added an autoprovisioned Virtual Chassis, only the Configuration Templates tab is available. The Port Profiles tab is unavailable because, in the case of autoprovisioning, port profiles can be configured only after provisioning the Virtual Chassis. The Access Profiles tab is unavailable because the access profile requires a RADIUS authentication server to be added to it. The parameters related to communication between the RADIUS server and the supplicant are defined in the authentication profile , which is, in turn, referenced by the port profile.

Table 13: Tabs on the Switch Configuration page

Tab	Description
Access Profiles	Displays the list of access profiles available in CSO. The list is populated from the Access Profiles page (**Configuration > SD-LAN > Access Profiles**). You can also click the **Search** icon to search for a specific access profile in the list. For details of the fields displayed on the Access Profiles table, see *About the Access Profiles Page*. Optional: You can select an access profile from the list to assign it to the switch.
Port Profiles	Displays the list of interfaces (ports) available in CSO. You can also click the **Search** icon to search for a specific port in the list. Optional: To assign port profiles and VLAN IDs to the ports: 1. Select one or more ports and click **Edit Configuration** on the top right corner, above the Interface List table. The Edit Port Configuration page appears. 2. From the **Port Profile** list, select a port profile to be assigned to the port. **NOTE:** The port profile must already be created from the Port Profiles page (**Configuration > SD-LAN > Port Profiles**) for it to be listed here. 3. In the **VLAN** field, if the port is configured as a trunk port in the port profile, assign multiple VLANs by selecting the VLANs in the **Available** column and clicking the right-arrow to move them to the **Selected** column. If the port is configured as an access port in the port profile, you can assign only one VLAN. 4. From the **Native VLAN** list, select a VLAN that you want to configure as native. This option appears only if you select a Trunk port profile from the Port Profile list. 5. Click **OK** to complete the configuration. You are returned to the Add On-Premise Spoke Site page.

Table 13: Tabs on the Switch Configuration page *(continued)*

Tab	Description
Configuration Templates	Displays the list of configuration templates. This list is filtered based on the device that you select. Configuration templates are predefined stage-2 templates that are added by your OpCo administrators or SP administrators. To add configuration templates and set the parameters for the selected configuration templates: 1. After you select one or more configuration templates, click **Set Parameters**. The **Device Configurations** page appears. This page consists of two tabs—Configure and Summary 2. In the Configure tab fill in the attributes for each of the configuration templates. 3. (Optional) View the CLI commands in the Summary tab. 4. Click **OK**. You have added and set the parameters for the configuration templates.

WHAT'S NEXT

After you onboard a switch, you can either add one or more switches to the site containing the switch (see Add Switches to an Existing SD-LAN Site | 80) or configure the switch in your network (see the *Configure an EX Series Switch* chapter in this guide).

Add a Switch Behind a CPE

Before you add a site with a switch behind a CPE, ensure that the switch and the CPE are powered on and connected to each other.

NOTE: When you connect a switch to a CPE before the CPE is provisioned, the IP address assigned to the EX switch by DHCP running on the CPE is not recognized by CSO. Therefore, the switch fails to connect with CSO and cannot be provisioned by CSO. To avoid this, do not connect the management interface vm0 of the switch and do one of the following:

- Add the switch to the site after provisioning the CPE.
- If you are adding the switch and the CPE in the same workflow:
  - Zeroize the switch before onboarding it with the CPE
  - If you do not zeroize the switch, log in to the switch during device activation and remove the DHCP binding by executing the following commands: **clear dhcp client binding all** and **request dhcp client renew all**.

    DHCP assigns an IP address from the switch management subnet to the EX switch and the ZTP of switch proceeds as CSO can now reach the EX switch.

To add a site with a switch behind a CPE:

1. Select **Resources > Site Management**.

   The Sites page appears.

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

   The Add Site for *Tenant-Name* page appears.

3. Complete the configuration according to the guidelines provided in Table 14 on page 59.

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

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

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

6. 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 CPE and the switch. The CPE is activated first and then the process to activate the switch is initiated.

7. - 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 14: Fields on the Add Site for Tenant-Name Page (SD-WAN and LAN Capabilities)

Field	Description
General	
Site Information	

Table 14: Fields on the Add Site for Tenant-Name Page (SD-WAN and LAN Capabilities) *(continued)*

Field	Description
Site Name	Enter a unique name for the site. You can use alphanumeric characters and hyphen (-); the maximum length is 32 characters.
Site Group	Select a site group to which you want to assign the site.
Site Capabilities	
WAN Capabilities	Select **SD-WAN** to include SD-WAN capabilities in the spoke site.
LAN Capabilities	Select **LAN** to include SD-LAN capability in the spoke site.
Configuration	
Primary Provider Hub	Select the hub site (or primary hub site in case of multihoming) to which the spoke site must connect.
Secondary Provider Hub	Select the secondary hub site to which this site must connect. This site connects to the secondary data hub site when the primary data hub is down.
Primary Enterprise Hub	Select the primary enterprise hub with which you want to connect the spoke site. If you specify a enterprise hub, then the initial site-to-site traffic as well as the central breakout (backhaul) traffic (if applicable) is sent through the enterprise hub instead of the hub site.
Secondary Enterprise Hub	Select the secondary enterprise hub for this spoke site. The spoke site connects with secondary enterprise hub when the primary enterprise hub is down.
On-Demand Mesh Threshold	
Threshold for Tunnel Creation	Specify the threshold for the number of sessions (flows) closed (in a two-minute duration) between the on-premise spoke site and a destination site. When the number of sessions closed exceeds the specified threshold, a tunnel is created between the on-premise spoke site and the destination site. The default value is 5. For example, if you specify the number of sessions as 5, dynamic mesh tunnels are created if the number of sessions closed between two spoke sites in 2 minutes exceeds 5.

Table 14: Fields on the Add Site for Tenant-Name Page (SD-WAN and LAN Capabilities) *(continued)*

Field	Description
Threshold for Tunnel Deletion	Specify the threshold for the number of sessions closed (in a 15-minute duration) between the on-premise spoke site and a destination site. When the number of sessions closed is lower than the specified threshold, the tunnel between the on-premise spoke site and destination site is deleted. The default value is 2. For example, if you specify the number of sessions closed as 2, dynamic mesh tunnels are deleted if the number of sessions closed is lesser than or equal to 2.
Address and Contact Information	
Street Address	Enter the street address of the site.
City	Enter the city where the site is located.
State/Province	Select the state or province where the site is located.
ZIP/Postal Code	Enter the postal code for the site.
Country	Select the country where the site is located. Click the **Validate** button to verify the address. • The **site address verification successful** message is displayed if the address is verified. You can click the **View location on a map** link to see the address location. • If the address cannot be verified, the **Site address could not be validated** message is displayed .
Contact Name	Enter the name of the contact person for the site.
Email	Enter the e-mail address of the contact person for the site.
Phone	Enter the phone number of the contact person for the site.
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.

Table 14: Fields on the Add Site for Tenant-Name Page (SD-WAN and LAN Capabilities) *(continued)*

Field	Description
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.
WAN	
Device Template	
Device Series	Select the device series to which the CPE belongs—SRX. NFX250. Based on the device series that you select, the supported device templates (containing information for configuring devices) are listed. Select a device template for the selected device series.
Device Information	
Serial Number	Enter the serial number of the CPE device.
Auto Activate	Click the toggle button to enable or disable automatic activation of the CPE device. When you enable this field, zero-touch provisioning (ZTP) of the CPE 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.
Activation Code	If you disable the Auto Activate field, enter the activation code for the CPE or firewall device. For information about activating a CPE or firewall device, see *Activating a CPE Device*.

Table 14: Fields on the Add Site for Tenant-Name Page (SD-WAN and LAN Capabilities) *(continued)*

Field	Description
Boot Image	Select the boot image from the drop-down list if you want to upgrade the image for the CPE 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 is populated based on the device template that you have selected while creating a site. See *Uploading a Device Image*.
WAN Links	
WAN_0 *WAN-Interface-Name*	This field is enabled by default. Enter parameters related to WAN_0. Fields marked with an asterisk (*) must be configured to proceed.
Link Type	Select whether the link would be an MPLS link or Internet link.
Access Type	If you select Internet as the link type, select the access type for the underlay link—Ethernet, LTE, ADSL, or VDSL. You can select the LTE, ADSL, or VDSL access type only for one WAN link. **NOTE:** You cannot configure an access type (LTE, ADSL, and VDSL) if you are using the Dual SRX and Dual NFX device templates. By default, Ethernet is configured as the access type for the underlay link.
Egress Bandwidth	Enter the maximum bandwidth (in Mbps) that the CPE or firewall allows over 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 DHCP, the IP address is provided by using the DHCP server of the service provider of the WAN link. • 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.

Table 14: Fields on the Add Site for Tenant-Name Page (SD-WAN and LAN Capabilities) *(continued)*

Field	Description
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	
Provider	Enter the name of the service provider who is responsible for providing the WAN link.
Cost/Month	Enter the cost per month (in a specified currency) for the WAN link. Specify the currency from the adjacent drop-down list. Range: 1 through 10,000. CSO uses this information to identify the least-expensive link to route traffic when multiple WAN links meet SLA profile parameters.
Enable Local Breakout	Click the toggle button to enable local breakout on the WAN link. By default, local breakout is disabled. **NOTE:** • If you enable this option, the WAN link can be used for local breakout. The decision of whether traffic breaks out locally from the site depends on the breakout profile that is referenced in the SD-WAN policy intent. • If you do not enable local breakout on at least one WAN link for a single CPE connection plan and at least two WAN links for a dual CPE connection plan, then local breakout is disabled for the site.
Breakout Options	Select whether you want to use the WAN link for both breakout and WAN traffic (default) or only for breakout traffic.

Table 14: Fields on the Add Site for Tenant-Name Page (SD-WAN and LAN Capabilities) *(continued)*

Field	Description

Autocreate Source NAT Rule	Click the toggle button to enable or disable the automatic creation of source NAT rules. By default, this field is enabled when local breakout is enabled on the WAN link.
	
	The automatically-created source NAT rules are implicitly defined and applied to the site and is not visible on the NAT Policies page.
	
	NOTE: You can manually override automatically created NAT rules, by creating a NAT rule within a particular rule-set. For example, to use a source NAT pool instead of an interface for translation, create a NAT rule within this particular rule-set, that includes the relevant department zone and WAN interface as the source and destination. For example:
	
	`Dept-Zone1 --> W1 : Translation=Pool-2`
	
	The manually created NAT rule is placed at a higher priority than the corresponding automatically created NAT rule.
	
	You can also add other fields (such as addresses, ports, protocols, and so on) as part of the source or destination endpoints. For example:
	
	`Dept-Zone1, Port 56578 --> W1: Translation=Pool-2`

Translation	Select the type of NAT to use for the traffic on the WAN link: • **Interface**—Use interface-based NAT, which is the default. • **Pool**—Use pool-based NAT. If you select this option, you must specify the IP addresses that are to be used for the NAT pool. **NOTE:** No NAT is performed for tenant-owned public IP addresses that were added during the tenant addition workflow.
IP Addresses	For pool-based NAT, enter one or more IP addresses, subnets, or an IP address range. Separate multiple IP addresses by using commas and use a hyphen to denote a range; for example, 192.0.2.1-192.0.2.50.
Preferred Breakout Link	Click the toggle button to enable the WAN link as the preferred breakout link. If you disable this option, then the breakout link is chosen using ECMP from the available breakout links.

Table 14: Fields on the Add Site for Tenant-Name Page (SD-WAN and LAN Capabilities) *(continued)*

Field	Description
BGP Underlay Options	**NOTE:** This setting can be configured only if the address assignment is static and local breakout is enabled. Click the toggle button to enable BGP underlay routing. When you enable BGP underlay routing, route advertisements to the primary PE node and, if configured, the secondary PE node occur as follows: • CSO advertises the WAN interface subnet. • If you configured pool-based translation, CSO advertises the NAT address pool. **NOTE:** If underlay BGP is enabled for a WAN link, then the routes learnt from BGP are installed for local breakout; CSO does not generate the static default route.
Primary Neighbor	Displays the IP address that you entered for the gateway for the WAN link.
Secondary Neighbor	If you want to provide PE resiliency, you can configure a secondary PE node. Enter the IP address of the secondary PE node. **NOTE:** If the primary PE node goes down, then the secondary PE is used as the next hop. When the primary PE comes back up, the route next hops are changed to the primary PE.
eBGP Peer-AS-Number	Enter the autonomous system (AS) number for the external (EBGP) peer. **NOTE:** If the peer AS number is not configured or the peer AS number that is configured is the same as that of the CPE site, then the BGP type is assumed to be internal BGP (IBGP).
Authentication	Select the BGP route authentication method to be used: • **None**—Indicates that no authentication should be used. This is the default. • **Use MD5**—Indicates that MD5 is to be used for authentication. If you choose this option, you must specify an authentication key.
Auth Key	If you specified that MD5 should be used for authentication, specify an MD5 authentication key (password), which is used to verify the authenticity of BGP packets.

Table 14: Fields on the Add Site for Tenant-Name Page (SD-WAN and LAN Capabilities) *(continued)*

Field	Description
Advertise Public LAN Prefixes	Click the toggle button to enable the advertisement of public LAN prefixes. This field is disabled by default. If the tenant has a public IP address pool configured and you enable the advertisement of public LAN prefixes, then for LAN segments that are created with a subnet that falls under the tenant public IP address pool, CSO advertises the LAN subnet to the BGP underlay. **NOTE:** When public LAN advertisement is enabled for the WAN link, public LAN prefixes are advertised through the BGP underlay towards MPLS or the Internet. If a site has two versions of the route installed for the same LAN prefix in the overlay and underlay, the overlay routes are always preferred over underlay.
Use For Fullmesh	Click the toggle button to specify whether the WAN link can be a part of a full mesh topology.

Mesh Overlay Link Type	When **Use for Fullmesh** field is enabled, select the type of mesh overlay link—GRE and GRE_IPSEC:
	
	• If the link type is Internet and is behind a NAT, the value for mesh overlay link type is GRE_IPSE; otherwise, the link type can be GRE..
	• If the link type is MPLS, select one of the following options:
	  ◦ GRE-IPSEC
	  ◦ GRE

Mesh Tag	When the **Use for Fullmesh** field is enabled, enter the tag to be associated with the WAN link for creating tunnels. You can assign only one tag to the link for a spoke site. An enterprise hub can have more than one tag on the WAN link. Matching mesh tags is one of the criteria used to form tunnels between sites that support meshing. For more information about mesh tags, see *Mesh Tags Overview*.
Connects to Hubs	Click the toggle button to specify that the WAN link of the site connects to a hub. **NOTE:** • For sites with a single CPE, you must enable at least one WAN link to connect to the hub so that OAM traffic can be transmitted. • For sites with a dual CPE, you must enable at least one WAN link per device to connect to the hub so that OAM traffic can be transmitted.

Table 14: Fields on the Add Site for Tenant-Name Page (SD-WAN and LAN Capabilities) *(continued)*

Field	Description
Use for OAM Traffic	If you have specified that the WAN link is connected to a hub, click the toggle button to enable sending the OAM traffic over the WAN link. This WAN link is then used to establish the OAM tunnel.
Overlay Tunnel Type	Select the mesh overlay tunnel type—GRE and GRE_IPSEC. MPLS links can have both GRE and GRE_IPSEC as the overlay link type where as Internet links can have only GRE_IPSEC as the overlay link type.
Overlay Peer Device	Displays the peer hub device to which the site is connected.
Overlay Peer Interface	Select the interface name of the hub device to which the WAN link of the site is connected.
Backup Link	Select a backup link through which traffic can be routed when the primary (other) links are unavailable. You can select any link other than the default links or links that are configured exclusively for local breakout traffic. When a primary link comes back online, CSO monitors the performance on the primary link and when the primary link meets the SLA requirements, the traffic is switched back to the primary link. Note that SLA data is not monitored for the backup link.
Default Link	Select one or more links that will be used for routing traffic in the absence of matching SD-WAN policy intents. A site can have multiple default links to the hub site. Default links are used primarily for overlay traffic but can also be used for local breakout traffic. However, a default link cannot be used exclusively for local breakout traffic. If you do not specify a default link, then equal-cost multipath (ECMP) is used to choose the link on which to route traffic.
Data VLAN ID	Enter a VLAN ID for the WAN link. Range: 2 through 4093. **NOTE:** • If you are configuring more than one WAN link on the same physical interface, only one WAN link can be untagged; for the remaining WAN links, you must configure a VLAN ID. • A combination of tagged and untagged on the same physical interface is supported only for single CPE devices.

Table 14: Fields on the Add Site for Tenant-Name Page (SD-WAN and LAN Capabilities) *(continued)*

Field	Description
WAN_1 WAN-Interface-Name	Click the toggle button to enable or disable the WAN link. When you enable the WAN link, fields related to the WAN link appear. Fields marked with an asterisk (*) must be configured to proceed. Refer to the fields described for *WAN_0 WAN-Interface-Name* for an explanation of the fields
WAN_2 WAN-Interface-Name	Click the toggle button to enable or disable the WAN link. When you enable the WAN link, fields related to the WAN link appear. Fields marked with an asterisk (*) must be configured to proceed. Refer to the fields described for *WAN_0 WAN-Interface-Name* for an explanation of the fields
WAN_3 WAN-Interface-Name	Click the toggle button to enable or disable the WAN link. When you enable the WAN link, fields related to the WAN link appear. Fields marked with an asterisk (*) must be configured to proceed. Refer to the fields described for *WAN_0 WAN-Interface-Name* for an explanation of the fields
Management Connectivity	
IP Prefix	Enter an IPv4 address prefix for the loopback interface on the CPE device. The IP address prefix must be a /32 IP address prefix and must be unique across the entire management network. If you do not specify an IPv4 address prefix, CSO automatically assigns the IP prefix from the reserved pool 100.124.0.0/14.
LAN	
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, EX4300, EX4600, and EX4650.
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	

Table 14: Fields on the Add Site for Tenant-Name Page (SD-WAN and LAN Capabilities) *(continued)*

Field	Description
Trunk Ports	Select at least two trunk ports on the CPE device to connect with the switch, which are used for the following: • LAN traffic between the switch and the CPE • Management traffic for in-band management of the switch. **NOTE:** The ae0 LAG interface of the SRX Series devices is used as the trunk port for communication with the switch.
Switch Management Subnet	Specify the subnet that the DHCP server can use to assign IP addresses. The DHCP server runs on the following ports: • Trunk ports to provide DHCP information to all devices connected to the switch and to the in-band management port, switch management port, and LAN ports on the CPE. • Out-of-band management port on the CPE to provide DHCP information to the management port on the switch. • LAN ports on the CPE to provide information to the devices connected to the CPE LAN ports.
Switch Details	
Serial Number	Specify the serial number of the switch.
Auto Activate	Click the toggle button to enable or disable automatic activation of the switch when the switch is detected by CSO (that is, management status of the device is Device_Detected). When you enable this field, zero-touch provisioning (ZTP) of the switch is automatically triggered when the device communicates with CSO. By default, auto activation for the switch is enabled, if it is enabled for the CPE and vice-versa.
Activation code	When the **Auto activate** field is disabled, enter the activation code to be used for manually activating the switch. For information, see *Manually Activating a Switch*.

Table 14: Fields on the Add Site for Tenant-Name Page (SD-WAN and LAN Capabilities) *(continued)*

Field	Description
Zero Touch Provisioning	Click the toggle button to enable or disable zero-touch provisioning (ZTP) of the switch. If you disable ZTP, you must manually copy and paste the Stage-1 configuration on the switch during site activation. See Step "Step-by-Step Procedure" on page 58 for details. **NOTE:** • Only EX Series devices running 18.4R2.7 and 18.4R3.3 firmware support ZTP. • EX4300 MP, EX4600 and EX4650 switches do not support Phone-Home client. You must disable ZTP and manually configure the stage-1 configuration on the switches.
LAN Segment	Displays the LAN segment that you configure on the switch. To add a LAN segment, click the **+** icon on the top, right corner of the LAN table. The Add LAN Segment page appears. See Table 15 on page 71.

Table 15: Fields on the Add LAN Segment Page when Adding a Switch along with CPE

Field	Description
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.
VLAN ID	Enter the VLAN ID for the LAN segment. Range: 2 through 4093.
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.
Gateway Address/Mask	Enter a valid gateway IP address and mask for the LAN segment; for example, 192.0.2.8/24.

Table 15: Fields on the Add LAN Segment Page when Adding a Switch along with CPE *(continued)*

Field	Description
DHCP	For directly connected LAN segments, click the toggle button to enable DHCP. DHCP is disabled by default. You enable DHCP if you want to assign IP addresses by using a DHCP sever. You disable DHCP if you want to assign a static IP address to the LAN segment. **NOTE:** If you enable DHCP, fields related to DHCP-related parameters appear and must be configured.
[DHCP-Related Fields]	
Address Range Low	Enter the starting IP address in the range of IP addresses that can be allocated by the DHCP server to the LAN segment.
Address Range High	Enter the ending IP address in the range of IP addresses that can be allocated by the DHCP server to the LAN segment.
Maximum Lease Time	Specify the maximum duration (in seconds) for which a client can request for and hold a lease on a DHCP server. Range: 0 through 4,294,967,295.
Name Server	Specify or select 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.
CPE Ports	Click the toggle button to include or exclude the CPE in the LAN segment. When you include the CPE in the LAN segment: • CPE ports that you can include in the LAN segment are listed. Select the ports from the **Available** column and click the right-arrow to move the ports to the **Selected** column. • The **Switch Ports** field is disabled. CSO automatically assigns LAN ports on the switch device and creates the same LAN segment on the switch. If you exclude the CPE from the LAN segment, you must specify the switch ports that connect with the LAN in the **Switch Ports** field. CSO automatically assigns LAN ports on the CPE device and creates the same LAN segment on the CPE device. **NOTE:** You can select only one port if the CPE is an SRX Series device.

Table 15: Fields on the Add LAN Segment Page when Adding a Switch along with CPE *(continued)*

Field	Description
Switch Ports	If you disable the CPE ports field, select ports on the switch that will be part of the LAN segment. Select the ports from the **Available** column and click the right-arrow to move the ports to the **Selected** column.

WHAT'S NEXT

After you onboard a switch, configure the switch in your network; see the *Configure an EX Series Switch* chapter in this guide.

Add a Switch Behind a Next-Generation Firewall

Before you add a site with a switch behind a next-generation firewall, ensure that the switch and the firewall are powered on and connected to each other.

To add a site with switch behind a next-generation firewall:

1. Select **Resources > Site Management**.

   The Sites page appears.

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

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

3. Complete the configuration settings according to the guidelines provided in Table 16 on page 75.

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

4. Click **Next**.

   A summary page is displayed.

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

6. 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 firewall device and the switch (when LAN capability is selected). The firewall device is activated first and then the process to activate the switch is initiated.

7. - 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.

> **NOTE:** You can also add a site with LAN and next generation firewall capabilities using the site templates. For more information, see *Add On-Premise Spoke Sites by Using a Site Template*.

Table 16: Fields on the Add On-Premise Spoke Site for Tenant-Name Page (Firewall and LAN)

Field	Description
General	
Site Information	
Site Name	Enter a unique name for the firewall site. You can use alphanumeric characters and hyphen (-); the maximum length is 32 characters.
Site Group	Select a site group to which you want to assign the site.
Site Capabilities	
WAN Capabilities	Select the WAN capabilities as **Next Gen Firewall** for the site.
LAN Capabilities	Select the LAN capability as **LAN** for the site.
Address and Contact Information	
Street Address	Enter the street address of the site.
City	Enter the name of the city where the site is located.
State/Province	Select the state or province where the site is located.
ZIP/Postal Code	Enter the postal code for the site.
Country	Select the country where the site is located. You can click the **Validate** button to verify the address that you specified: • The **site address verification successful** message is displayed if the address can be verified. You can click the **View location on a map** link to see the address location. • If the address cannot be verified, the **Site address could not be validated** message is displayed .
Contact Name	Enter the name of the contact person for the site.
Email	Enter the e-mail address of the contact person for the site.
Phone	Enter the phone number of the contact person for the site. Click **Next** to continue.

Table 16: Fields on the Add On-Premise Spoke Site for Tenant-Name Page (Firewall and LAN) *(continued)*

Field	Description
Advanced Configuration	
Name Server IP List	Enter one or more IPv4 addresses of the DNS server. To enter more than one DNS server address, type address, press Enter, and then type the next address, and so on. DNS servers are used to resolve hostnames into IP addresses.
NTP Server	Enter 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 for the site.
WAN	
Device Information	
Serial Number	Enter the serial number of the firewall device. Note that the serial numbers are case-sensitive.
Auto Activate	Click the toggle button to enable or disable automatic activation of the device. This option is enabled by default.
Activation Code	If the **Auto Activate** feature is disabled, enter the activation code to manually activate the device. The activation code is provided by the administrator who adds the site.
Zero Touch Provisioning	Click the toggle button to enable or disable Zero Touch Provisioning (ZTP). This option is enabled by default. If ZTP is enabled, the Boot Image field is displayed and you must select an image that supports the Phone-Home client. During ZTP, the image on the firewall device is upgraded to the image that you select for the Boot Image. If ZTP is disabled, you must manually copy (by using CLI), the Stage-1 configuration on to the firewall device.

Table 16: Fields on the Add On-Premise Spoke Site for Tenant-Name Page (Firewall and LAN) *(continued)*

Field	Description
Boot Image	When the Zero Touch Provisioning field is enabled, select the boot image from the drop-down list to upgrade the image on the firewall device to a version that supports Phone-Home client. The boot image is the device image that was previously uploaded to the image management system. The boot image is used to upgrade the device when CSO starts the ZTP process. If the boot image is not provided, then the device skips the automatic upgrade procedure. The boot image is populated based on the device template that you have selected while creating a site. By default, the **Use Image on Device** option is selected.
In-band Management Port	Select the port that you want to configure as management interface and connect it to the management device. You can configure any of the ge-0/0/x ports, where x ranges from 0 to 14, as in-band management interfaces. This field is applicable only when a switch is behind a CPE (SD-WAN or a next generation firewall device).
Firewall Policies	Select the firewall policy that you want to deploy to the standalone firewall site. The firewall policy list is populated from the **Configuration > Firewall > Firewall Policy** page. Default: Factory_Default_Fw_Policy
NAT Policies	Select the NAT policy that you want to deploy to the standalone firewall site. The NAT policy list is populated from the **Configuration > NAT > NAT Policies** page. Default: Factory_Default_NAT_Policy
Import Configuration	Click the toggle button to automatically import firewall policies and NAT policies from a next generation firewall device to CSO. By default, this field is disabled. **NOTE:** This field is available only when Zero Touch Provisioning is disabled.
LAN	
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, EX4300, EX4600, and EX4650.

Table 16: Fields on the Add On-Premise Spoke Site for Tenant-Name Page (Firewall and LAN) *(continued)*

Field	Description
Device Model	Select the device model for the switch that 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.
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 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. The DHCP server runs on the following ports: • Trunk ports to provide DHCP information to all devices connected to the switch and to the in-band management port, switch management port, and LAN ports on the CPE. • Out-of-band management port on the CPE to provide DHCP information to the management port on the switch. • LAN ports on the CPE to provide information to the devices connected to the CPE LAN ports. Example: 192.0.2.0/24
Switch Details	
Serial Number	Specify the serial number of the switch The serial number is a 12-digit number present on the rear panel of the switch.
Auto Activate	Click the toggle button to enable or disable automatic activation of the switch. When you enable this field, zero-touch provisioning of the switch is automatically triggered when the device communicates with CSO. **NOTE:** You must physically connect the switch to the CPE device (firewall) and power it on for the switch to be automatically activated when you enable this option.
Activation code	When the **Auto activate** field is disabled, enter the activation code to be used for manually activating the switch. For information, see *Manually Activating a Switch*.

Table 16: Fields on the Add On-Premise Spoke Site for Tenant-Name Page (Firewall and LAN) *(continued)*

Field	Description
Zero Touch Provisioning	Click the toggle button to enable or disable zero-touch provisioning (ZTP) of the switch. If you disable ZTP, you must manually copy and paste the Stage-1 configuration on the switch during site activation. See "Step-by-Step Procedure" on page 73 for details.
LAN Segment	Displays the LAN segment configured on the switch. To add a LAN segment, click the + icon on the top, right corner of the LAN table. The Add LAN Segment page appears. Specify values for the LAN segment based on guidelines provided in Table 17 on page 79. Fields marked * are mandatory. **NOTE:** The same LAN segment is created on the CPE device (firewall)if the switch is connected to the CPE device (firewall) that is managed by CSO.

Table 17: Fields on the Add LAN Segment Page when Adding a Switch along with Firewall

Field	Description
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.
VLAN ID	Enter the VLAN ID for the LAN segment. Range: 2 through 4093
Gateway Address/Mask	Enter a valid gateway IP address and mask for the LAN segment; for example, 192.0.2.8/24.
DHCP	For directly connected LAN segments, click the toggle button to enable DHCP. DHCP is disabled by default. You enable DHCP if you want to assign IP addresses by using a DHCP sever. You disable DHCP if you want to assign a static IP address to the LAN segment. **NOTE:** If you enable DHCP, fields related to DHCP-related parameters appear and must be configured.
[DHCP-Related Fields]	

Table 17: Fields on the Add LAN Segment Page when Adding a Switch along with Firewall *(continued)*

Field	Description
Address Range Low	Enter the starting IP address in the range of IP addresses that can be allocated by the DHCP server to the LAN segment.
Address Range High	Enter the ending IP address in the range of IP addresses that can be allocated by the DHCP server to the LAN segment.
Maximum Lease Time	Specify the maximum duration (in seconds) for which a client can request for and hold a lease on a DHCP server. Range: 0 through 4,294,967,295.
Name Server	Specify or select 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.

WHAT'S NEXT

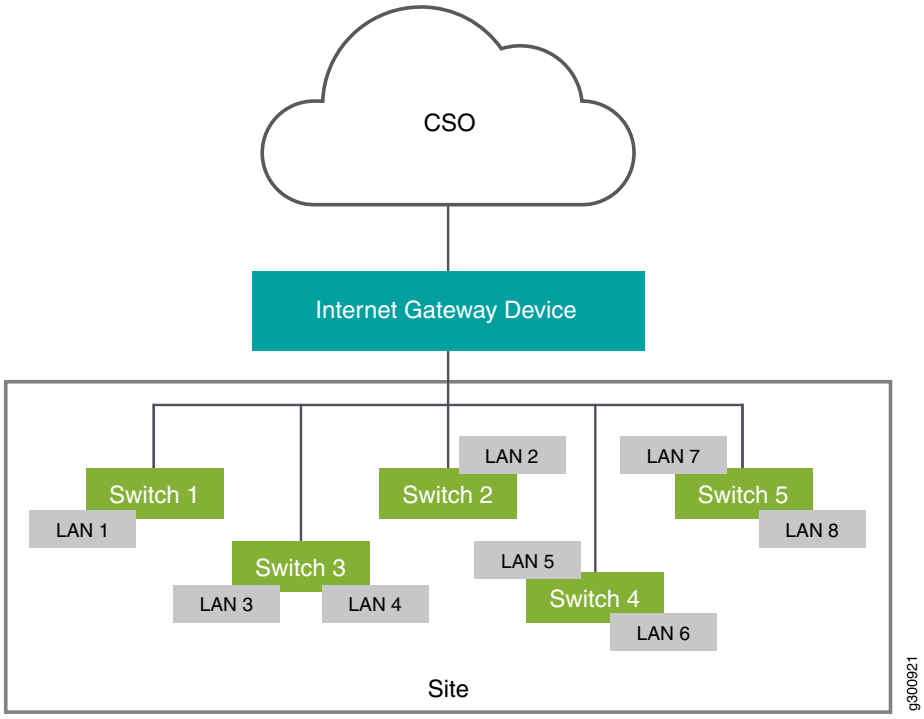
After you onboard a switch, configure the switch in your network; see the *Configure an EX Series Switch* chapter in this guide.

Add Switches to an Existing SD-LAN Site

From CSO Release 5.1.1 onward, you can add one or more EX Series switches to an existing SD-LAN site. Physical, standalone EX Series switches and EX Series Virtual Chassis are supported.

Figure 12 on page 81 shows an SD-LAN site, with multiple EX Series switches, managed by CSO.

Figure 12: SD-LAN Site with Multiple Switches



To add a switch to an existing site:

1. Select **Resources > Site Management**.

   The Sites page appears.

2. Do one of the following:

   - a. Select the site to which you want to add the switch.

     b. Click **Add > Add Switch**.

     The Add Switch page appears.

   - a. Click the *Site-Name* link of the site (to which you want to add the switch) in the Sites column.

     The *Site-Name* page appears.

     b. On the Devices tab, click **Add Switch**.

     The Add Switch page appears.

1. Complete the configuration according to the guidelines provided in Table 18 on page 83.

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

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

3. (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 switch to the site.

   The site activation process is initiated and the Site Activation: *Site-Name* page appears displaying the progress of the steps executed for activating the switch. If you add one or more EX Series switches, the progress of the steps executed for activating each switch is displayed.

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.

Table 18 on page 83 provides guidelines on using the fields on the Add Switch page.

Table 18: Fields on the Add Switch Page

Field	Description
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, 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.
Switch Details	
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. • Before you add a Virtual Chassis in CSO, ensure that the Virtual Chassis is setup. See “Step-by-Step Procedure” on page 88 for details about setting up a Virtual Chassis. In addition, click the **View Prerequisite Configurations** link to view the requirements for adding a Virtual Chassis in CSO. • Currently, 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 18: Fields on the Add Switch Page *(continued)*

Field	Description
Serial Number	If you disabled the Virtual Chassis toggle button, specify the serial number of the physical switch. You can either view the serial number on the label that is present on the rear panel of the switch or log in to the CLI of the switch in operational mode and enter **show chassis hardware**. The serial number is a case-sensitive, alphanumeric string.
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 Master 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 member devices 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 member devices in the Virtual Chassis are running the same firmware (either JUNOS 18.4R2.7 or 18.4R3.3). • For EX3400 and EX4300devices to act as a Virtual Chassis, all the corresponding member devices are interconnected through Virtual Chassis ports (VCPs). For EX2300, EX4600, EX4650 devices to act as a Virtual Chassis, the uplink Ethernet ports are configured as VCPs manually and the member devices are interconnected.

Table 18: Fields on the Add Switch Page *(continued)*

Field	Description
Master Serial Number	If you selected Auto Provisioning, enter the serial number of the primary device (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:** • 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 device 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 device or the Remove (-) icon to remove a member device. For information on the number of member devices that can be added, see Table 20 on page 88. **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 device as backup, click the Routing Engine check box corresponding to that member device; the remaining member devices act as line cards.
Zero Touch Provisioning	Click to enable or disable ZTP on the switch. If you disable ZTP, you must manually copy and paste the Stage-1 configuration on the switch during site activation. See “Step-by-Step Procedure” on page 82 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.

Table 18: Fields on the Add Switch Page *(continued)*

Field	Description
Boot Image	Select the boot image from the list if you want to upgrade the image for the switch. The boot image is the latest device image that is 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 automatic upgrade procedure. The boot image is populated based on the device template that you have selected while creating a site. **NOTE:** This option is not available for a Virtual Chassis. To provision a Virtual Chassis in CSO, you must manually upgrade the image to either JUNOS 18.4R2.7 or 18.4R3.3.
Auto activate	Click the toggle button to enable or disable automatic activation of the switch. When you enable this field, zero-touch provisioning of the switch is automatically triggered when the device communicates with CSO.
Activation code	When the **Auto activate** field is disabled, enter the activation code to be used for manually activating the switch. For information, see *Manually Activating a Switch*.
Profiles You are directed to this page only if you have added a physical switch or a preprovisioned Virtual Chassis. If you have added an autoprovisioned Virtual Chassis; you are automatically directed to the Summary page. This is because, in the case of autoprovisioning, port profiles can be configured only after provisioning the Virtual Chassis.	
Access Profiles	Displays the access profile configured on the device from the Access Profiles page (Configuration > SD-LAN > Access Profiles). For details of the fields displayed on the Access Profiles List table, see *About the Access Profiles Page*. Optional: You can select an access profile from the list to assign it to the switch.

Table 18: Fields on the Add Switch Page *(continued)*

Field	Description
Interface List	Displays the list of interfaces (ports) available in CSO. Optional: Click the **Search** icon to search for a specific port in the list. For more information on the fields displayed in the Interface List table, see Table 19 on page 87. Optional: To assign port profiles and VLAN IDs to the ports: 1. Click **Edit Configuration** on the top-right corner of the Interface List table. The Configuration page appears. 2. From the **Port Profile** list, select a port profile to be assigned to the port. **NOTE:** The port profile must already be created from the Port Profiles page (**Configuration > SD-LAN > Port Profiles**) for it to be listed here. 3. In the **VLAN** field, if the port is configured as a trunk port in the port profile, assign multiple VLANs by selecting the VLANs in the **Available** column and clicking the right-arrow to move them to the **Selected** column. If the port is configured as an access port in the port profile, you can assign only one VLAN. 4. From the **Native VLAN** list, select a VLAN that you want to configure as native. This option appears only if you select Trunk port profile from the Port Profile list. 5. Click **OK** to complete the configuration. You are returned to the Add On-Premise Spoke Site page.

Table 19 on page 87 describes the fields on the Interface List table.

Table 19: Fields on the Interface List Table on the Port Profile Page

Field	Description
Port	Name of the port.
VLAN	ID of the VLAN configured on the port. If the port is a trunk port, all the VLAN IDs configured on the port are displayed.
Native VLAN	ID of the VLAN configured to accept untagged frames.

Table 19: Fields on the Interface List Table on the Port Profile Page *(continued)*

Field	Description
Port Profile	Port profile used for configuring the port. If the port is configured manually, the column displays **Manually Configured**.

Table 20 on page 88 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 20: 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 or EX4300 devices as Virtual Chassis, interconnect all the corresponding member devices through Virtual Chassis ports (VCPs).

     If you've added EX2300, EX4600, or EX4650 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 primary 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 or EX4300 devices as Virtual Chassis, interconnect all the corresponding member devices through Virtual Chassis ports (VCPs).

     If you've added EX2300, EX4600, or EX4650 devices as Virtual Chassis, configure the uplink 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 **Switch Details** section in Table 18 on page 83 for details.

Release History Table

Release	Description
5.1.1	From CSO Release 5.1.1 onward, you can add one or more EX Series switches to an existing SD-LAN site. Physical, standalone EX Series switches and EX Series Virtual Chassis are supported.

RELATED DOCUMENTATION

Add a Switch to an Existing SD-WAN Site Or Next-Generation Firewall Site

Add Switches to an Existing SD-WAN Site

You can add one switch (physical switch) to an existing on-premise spoke site that already has a CPE or a next-generation firewall device provisioned, to provide LAN capability to the site.

NOTE: To manage more than one switch through a CPE or a next-generation firewall, you must manage the connectivity and configuration between the switches and the CPE or next-generation firewall either by using configuration templates or manually. CSO can manage the connectivity between the switch and the next-generation firewall for only one switch.

To add a switch to an already provisioned CPE or next-generation firewall:

1. Select **Resources > Site Management**.

   The Sites page appears.

2. Do one of the following:

   - To add a switch from the Sites page:

     a. Select the site to which you want to add the switch.

     b. Click **Add > Add Switch**.

        The Add Switch page appears.

   - To add a switch from the *Site-Name* page:

     a. Click the *Site-Name* link of the site (to which you want to add the switch) in the Sites column.

        The *Site-Name* page appears.

     b. On the Devices tab, click **Add Switch**.

        The Add Switch page appears.

3. Complete the configuration according to the guidelines provided in Table 18 on page 83.

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

4. Click **Next** and review the configuration from the **Summary** tab.

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

6. Click **OK** to add the switch to the site.

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

7. - 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 21: Fields on the Add Switch Page

Field	Description
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, 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.
CPE Settings This setting is applicable only when you are adding a switch to an SD-WAN, next-generation firewall, or an enterprise hub site.	
Trunk Ports	Select at least two trunk ports on the CPE device to connect with the switch, which are used for the following:. • LAN traffic between the switch and the CPE or firewall. • Management traffic for in-band management of the switch. **NOTE:** The ae0 port of the SRX Series devices is used as the trunk port for communication with the switch.
Switch Management Subnet	Specify the subnet that the DHCP can use to assign IP addresses. The DHCP server runs on the following ports: • Trunk ports to provide DHCP information to all devices connected to the switch and to the in-band management port, switch management port, and LAN ports on the CPE or firewall. • Out-of-band management port on the CPE or firewall to provide DHCP information to the management port on the switch. • LAN ports on the CPE or firewall to provide information to the devices connected to the CPE or firewall LAN ports.

Table 21: Fields on the Add Switch Page *(continued)*

Field	Description
Switch Details	
Serial Number	Specify the serial number of the physical switch. You can either view the serial number on the label that is present on the rear panel of the switch or log in to the CLI of the switch in operational mode and enter **show chassis hardware**. The serial number is a case-sensitive, alphanumeric string.
Auto activate	Click the toggle button to enable or disable automatic activation of the switch. When you enable this field, zero-touch provisioning of the switch is automatically triggered when the device communicates with CSO. **NOTE:** You must physically connect the switch to the CPE and power it on for the switch to be automatically activated when you enable this option.
Activation code	When the **Auto activate** field is disabled, enter the activation code to be used for manually activating the switch.
Zero Touch Provisioning	Click to enable or disable ZTP on the switch. If you disable ZTP, you must manually copy and paste the Stage-1 configuration on the switch during site activation. See "Step-by-Step Procedure" on page 82 for details **NOTE:** • Only EX Series switches running 18.4R2.7 and 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.
Boot Image	Select the boot image from the list if you want to upgrade the image for the switch. The boot image is the latest device image that is 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 automatic upgrade procedure. The boot image is populated based on the device template that you have selected while creating a site.
Port Profile	

Table 21: Fields on the Add Switch Page *(continued)*

Field	Description
Access Profiles List	Displays the access profile configured on the device. If no access profile is configured on the device, you can create an access profile and assign it to the device by clicking the **+** icon on the top-right corner above the Access Profiles List table.
Interface List	Displays the list of interfaces present on the device. You can assign the ports to VLAN from here. To assign the ports to a VLAN: 1. Click **Edit Configuration** on top-right corner above the Interface List table. The Configuration page appears. 2. From the **Port Profile** drop-down list, select a port profile to be assigned to the port. 3. In the **VLAN** field, select one or more VLANs to be assigned to the port if the port is a trunk port. If the port is configured as an access port, you can assign only one VLAN. 4. From the **Native VLAN** list, select a VLAN that you want to configure as native. This option appears only if you select Trunk port profile from the Port Profile list. Default: VLAN1

WHAT'S NEXT

After you onboard the switch, configure the switch in your network; see the *Configure an EX Series Switch* chapter in this guide.

4

CHAPTER

Configure an EX Series Switch

Configure an EX Series switch Overview | **97**

Configure an EX Series Switch by Using Configuration Templates | **97**

Configure an EX Series Switch by Using Profiles | **101**

Configure an EX Series Switch Manually | **104**

Enable Ports | **105**

Configure an EX Series switch Overview

When you onboard an EX Series switch to CSO, you configure the stage-1 parameters. You can deploy stage-2 configuration on the switch by:

- Using configuration templates; see "Configure an EX Series Switch by Using Configuration Templates" on page 97 for details.
- Using profiles; see "Configure an EX Series Switch by Using Profiles" on page 101 for details.

  NOTE: You can configure both a physical device and members of a virtual chassis by using profiles. However, you cannot configure and monitor EX4600 and EX4650 Series switches by using profiles, if the switches are configured as a virtual chassis.

- Configuring manually; see "Configure an EX Series Switch Manually" on page 104 for details.

Configure an EX Series Switch by Using Configuration Templates

CSO provides default configuration templates to configure EX Series switches. See "Default Configuration Templates For EX Series Switches" on page 141 for information about default configuration templates provided by CSO for EX Series devices.

To deploy a configuration template to one or more EX Series devices:

1. Select **Resources > Devices**.

   The Devices page appears.

2. Select the EX Series device on which you want to deploy configuration templates and click **More > Deploy Configuration**.

   The Deploy Configuration to Devices page appears displaying the selected device in the Devices table.

3. From the **Configuration Template** field, choose the configuration template that you want to deploy.

4. Complete the configuration according to the guidelines provided in Table 22 on page 98.

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

5. Click **OK**.

   The settings that you entered are saved and you are returned to the Devices page. A confirmation message appears indicating that a job was created.

   You can view the status of the jobs from the Jobs page (**Monitor > Jobs**).

Table 22: Deploy Template <Template-Name> To Devices Settings

Setting	Guideline
Select Devices	
Configuration Template	Displays the name of the configuration template that you are deploying.

Table 22: Deploy Template <Template-Name> To Devices Settings *(continued)*

Setting	Guideline
Devices	You can specify the devices on which you want to deploy the configuration template in the following ways: • By adding the devices manually: 1. From the list of devices displayed, select one or more devices by clicking the check box next to each device name. **NOTE:** You can search for devices or filter the list of devices displayed. 2. Click **Next**. You are taken to the Configure Global Parameters or the Configure Device Parameters tab. • By uploading a comma-separated values (CSV) file containing the device information: **NOTE:** You must ensure that the CSV file is in the format that CSO can read and that the number of device records is 200 or lower. You can download a sample file by clicking the **Download Sample CSV File** button. 1. Click **Upload CSV File**. The Upload CSV File page appears. 2. Click **Browse** to open the file selection dialog, select a file, and click **Open**. The name of the file that you selected is displayed in the CSV File field. 3. Click **OK**. You are returned to the previous page where the devices that you imported are selected and displayed in the table. 4. Click **Next**. You are taken to the Configure Global Parameters or the Configure Device Parameters tab.
Configure Global Parameters	**NOTE:** This tab is displayed only if the configuration template contains parameters that are global in scope. Specify the global parameters that are common to all the devices that you selected in the preceding step. After you are done, click **Next**. You are taken to the Configure Device Parameters tab.

Table 22: Deploy Template <Template-Name> To Devices Settings *(continued)*

Setting	Guideline
Configure Device Parameters	
Devices	The devices that you selected in the preceding step are displayed in the Devices table, and the first device is selected by default. For each device, the device name, device family, operational status, and the configuration status are displayed. When you first arrive on this tab, the configuration status for each device is *Not configured*. The *Device-Name* Parameters pane on the right displays the input parameters (from the configuration template) that you can specify for each device. After you specify the values for one device, you can select a different device and enter the configuration values. • If the configuration template contains validations for the parameters, CSO validates the values you entered for the device and changes the configuration status to Valid and displays a green check mark (√). • If the configuration template does not contain any validations, CSO changes the configuration status to Valid and displays a green check mark (√). • If the values that you entered do not match the validation, the configuration status displays Invalid. **NOTE:** You can optionally delete a device by selecting the device and clicking the delete (trash can) icon. After you specify the input parameter values for all the devices and ensure that the configuration status of all devices is Valid, click **Next**. You are taken to the Summary tab.
Summary	
Devices	The devices that you selected in the preceding step are displayed in the Devices table, and the first device is selected by default. For each device, the device name, device family, and operational status are displayed. For each device, the *Device-Name* Configuration pane on the right displays the actual configuration that will be deployed on the device. After you review the configuration for all the devices, click **Next**. You are taken to the Deploy tab.

Table 22: Deploy Template <Template-Name> To Devices Settings *(continued)*

Setting	Guideline
Deploy	
Deployment Schedule	Specify whether the configuration should be deployed on devices immediately (**Deploy now**) or deployed later (**Deploy later**). If you choose to deploy the configuration later, you must enter the date (in MM/DD/YYYY format) and time (in HH:MM:SS 24-hour or AM/PM format) that you want the deployment to occur.

WHAT'S NEXT

After you deploy the configuration template on the switch, enable the ports of the switch; see Enable Ports | 105.

Configure an EX Series Switch by Using Profiles

IN THIS SECTION

- Deploy an Access Profile on a Switch | 102
- Configure Switch Ports by Using a Port Profile | 102

You configure an EX Series switch by using profiles by:

- Deploying the access profile on the switch to configure RADIUS servers.
- Assigning port profiles to the ports and deploying the port profile to configure 802.1x authentication and port parameters.

Deploy an Access Profile on a Switch

An access profile defines the list of RADIUS servers to be used for authentication and accounting. You can deploy only one access profile on a switch.

To deploy an access profile on a switch:

1. Select **Resources > Devices** in Customer Portal.

   The Devices page appears.

2. Click the switch on which you want to deploy the access profile.

   The *Devices-Name* page appears.

3. Click the **Device Settings** tab.

   The access profiles configured are listed in a tabular format.

4. Select the access profile that you want to deploy on the switch.

5. In the **Type** field:
   - Click **Run now** to deploy the access profile immediately.
   - Click **Schedule at a later time** to deploy the access profile later.

     If you select this option, enter the date and time when you want to deploy in the Date and Time fields that appear.

6. Click **Deploy**.

   If you select the Run now option, a job is created to deploy the profile immediately; otherwise, the job to deploy is created on the date and at the time that you schedule.

Configure Switch Ports by Using a Port Profile

You can configure one or more switch ports at the same time by assigning and deploying a port profile. A port profile defines the authentication settings for the port and other port parameters such as flow control, link mode, storm control, MAC limit, and so on. The behavior of the port is defined by the values for parameters defined in the port profile.

To assign and deploy a port profile on one or more switch ports:

1. Select one or more ports and click **More > Edit Configuration**. Alternatively, right-click the ports and click **Edit Configuration**.

   The Edit Port(s) page appears.

2. For **Options**, select **Use Port Profile**.

   The Port Profile drop down list and an option to select the VLAN appears.

3. Select a port profile that you want to assign to the port or ports from the **Port Profile** drop down list.

4. In the VLAN field:

   - If the port is configured as a trunk port in the port profile, assign multiple VLANs by selecting the VLANs in the Available column and clicking the right-arrow to move them to the Selected column.
   - If the port is configured as an access port in the port profile, assign a single VLAN by selecting the VLAN in the Available column and clicking the right-arrow to move it to the Selected column.

5. Click **Next**.

   Deployment options appear.

6. (Optional) Select the **Do not deploy** option if you want to only assign the profile to the selected ports, but not push and commit the configuration (in the profile) on the switch.

7. For the **Type** field, do one of the following:

   - Click **Run now** to save the edited configuration in CSO and commit the edited configuration on the switch.
   - Click **Schedule at a later time** to commit the edited configuration on the switch later.

     If you select this option, enter the date and time when you want to deploy in the fields that appear when you select the option.

8. Click **Next**.

   A summary of all the port profile parameter appears.

9. (Optional) Click **Edit** to revisit the settings and make further changes.

10. Click **OK**.

    If you select the Run now option, a job is created to deploy the profile at once; otherwise, the job to deploy is created on the date and at the time that you scheduled.

    When you deploy a port profile, the deployment status of the ports is set to Pending Deployment indicating that the profile is assigned to the ports. When the profile is in the process of being committed on the ports, the deployment status changes to In Progress. If the deployment job completes successfully,

the deployment status of the ports is set to Success and if the job fails, the deployment status is set to Failed.

After the deployment job completes successfully:

- A message appears on the top of the Ports page indicating that the deployment is successful.
- The deployment Status of the port is set to Deployed.
- The Port Profile column in the Ports tab on the *Switch-Name* page displays the port profile currently assigned and deployed on the port.

WHAT'S NEXT

> After you deploy the configuration template on the switch, enable the ports of the switch; see Enable Ports | 105.

Configure an EX Series Switch Manually

To manually configure an EX Series switch:

1. In Customer Portal, select **Resources > Devices**.

   The Devices page appears.

2. Click the switch for which you want to configure or edit port parameter.

   The *Switch-Name* page appears.

3. On the Ports tab, select the port that you want to configure and click **More > Edit Configuration**.

   The Edit Port Configuration page appears.

4. Edit the port parameters. Refer to the instructions in the "Add Port Profiles" on page 31 topic for configuring the port parameters. topic for completing the port configuration.

5. Click **Next**.

   Deployment options appear.

6. (Optional) Select the **Do not deploy** option if you want to only save the edited configuration in CSO, but not push and commit the configuration to the switch.

7. For the **Type** field, do one of the following:
   - Click **Run now** to save the edited configuration in CSO and commit the edited configuration on the switch.
   - Click **Schedule at a later time** to schedule a time to commit the edited configuration on the switch.

     If you select the Schedule at later time option, enter the date and time when you want to deploy, in the fields that appear when you select the option.
8. Click **Next**.

   A summary of all the port profile parameter appears.
9. (Optional) Click **Edit** to revisit the settings and make further changes.
10. Click **OK**.

    If you select the Run now option, a job is created to deploy the profile at once; otherwise, the job to deploy is created on the date and at the time that you scheduled.

    During the deployment, the deployment status of the port is set to Pending Deployment..

WHAT'S NEXT

> After you deploy the configuration template on the switch, enable the ports of the switch; see Enable Ports | 105.

Enable Ports

You enable a port to allow traffic through the port. When you enable a port, the Admin status of the port is changed to Up.

NOTE: You can enable one or more ports at the same time.

To enable one or more ports:

1. Select the ports and click **More > Enable Port(s)**. Alternatively, right-click the ports and click **Disable Port(s)**.

   A job to enable the ports is initiated.

After a port is enabled, the Admin Status is changed to Up.

> **NOTE:** The device is monitored once every five minutes. Therefore, it takes upto five minutes for the change in the Admin Status to reflect on the CSO GUI.

5

CHAPTER

Integrate CSO with Mist UI and Discover Access Points

Integrate CSO with Mist Portal | **108**

Discover Mist Access Points | **109**

Integrate CSO with Mist Portal

You can integrate CSO with Mist Portal to view Mist access points (APs) present in your branch and campus networks.

By using Mist Portal with CSO, you can:

- View operational and analytics data of LAN and get an insight about the functioning of the LAN.
- Set and enforce performance metrics such as throughput, capacity, roaming, and uptime in your wireless networks.

> **NOTE:** You can skip integration with Mist Portal if you do not want to have Mist access points in your network.

If the EX switch is behind a CPE or a firewall, create a LAN segment on the CPE or firewall and assign the switch port connected to the access point to the LAN Segment. Ensure that DHCP is enabled on the LAN segment. Refer "Creating a LAN Segment for Discovering Mist Access Points" on page 142 to create the LAN Segment.

To integrate CSO with Mist Portal:

1. Select **Administration** > **WiFi Settings** in Customer Portal.

   The WiFi Settings page appears.

2. Click the Enable/Disable toggle button to integrate CSO with Mist Portal.

   The Username and Password fields appear.

3. In the Username field, enter the e-mail address for your Mist account.

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

WHAT'S NEXT

After you enable integration of CSO with Mist Portal, you can discover access points connected to the switches managed by CSO. See Discover Mist Access Points | 109 for details.

Discover Mist Access Points

After Contrail Service Orchestration (CSO) is integrated with the Mist portal, you can discover the access points connected to a switch in Customer Portal. This integration enables you to launch the Mist portal from CSO and monitor the access points connected to the switch.

> **NOTE:** Before you discover a Mist access point, ensure that the access point is claimed in the Mist portal.

To discover the access points connected to a switch:

1. Click **Resources > Devices**.

   The Devices page appears.

2. Select the switch for which you want to discover the connected access points.

3. Click the **Discover Connected APs**.

   A job is triggered to discover the access points connected to the switch.

   After the job is completed successfully, the access points connected to the switch are listed in the Devices page.

WHAT'S NEXT

After you discover the access points, you can start monitoring them in Mist Portal; see *Monitor Mist Access Points* in *Contrail SD-LAN: Manage Branch and Campus Switching*.

CHAPTER 6

Monitor an EX Series Switch and Connected Access Points

Monitor an EX Series Switch Overview | **111**

Monitor Port Level Information | **112**

Monitor Chassis-Level Information | **113**

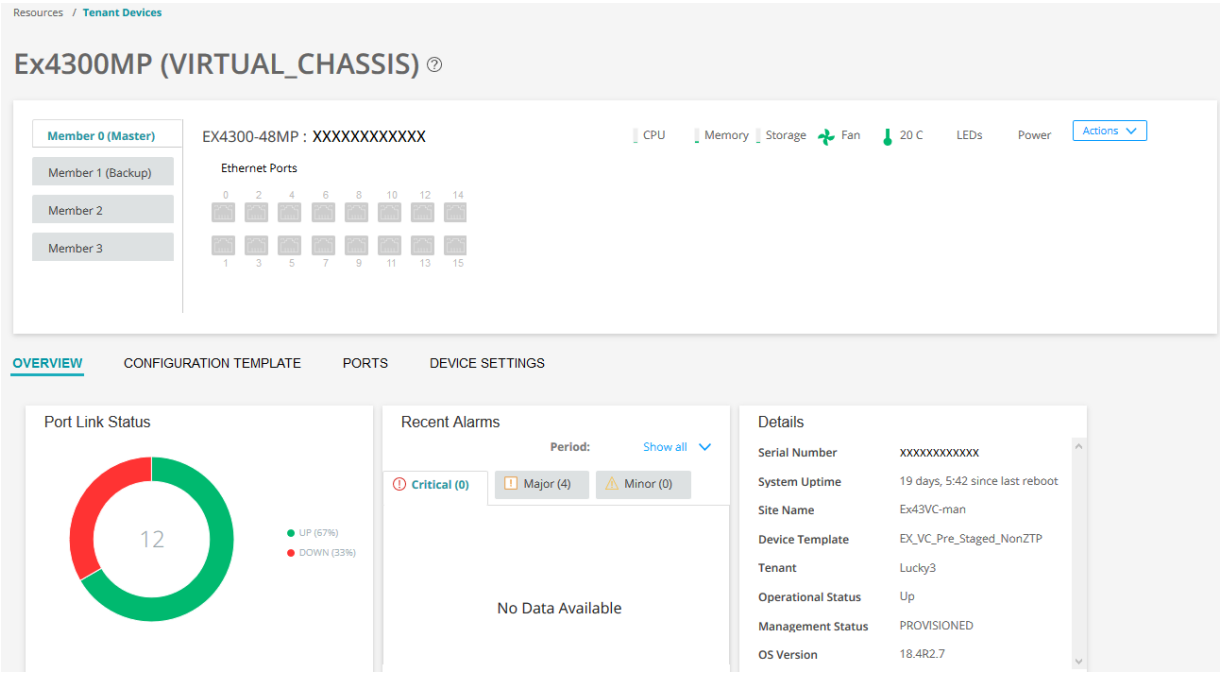
Monitor Device Level Information | **119**

Monitor Mist Access Points | **123**

Monitor an EX Series Switch Overview

You can monitor an EX Series switch, both physical and Virtual Chassis (VC) at the port level, chassis level, and device level from the *Device-Name* page. You can launch the Mist Portal from the Devices page to monitor access points connected to the switch.

Figure 13: EX Virtual Chassis



You can access the *Device-Name* page from the Sites page or the Devices page:

- To access the *Device-Name* page from the Devices page:
  1. Click **Resources > Devices**.

     The Devices page appears.

  2. Select an EX Series switch in the Device Name column of the Devices List.

     The *Device-Name* page appears.

- To access the *Device-Name* page from the Sites page:
  1. Click **Resources > Site Management**.

     The Sites page appears.

  2. Click the *Site-Name* of the site for which you want to view the device information.

The *Site-Name* page appears.

3. Click the **Devices** tab.

   The list of devices added to the site appears.

4. Click an *EX Series switch* from the list.

   The *Device-Name* page appears.

You can view the following on the *Device-Name* page:

- Chassis view—Displays the ports of the switch as icons. For a Virtual Chassis, the member devices in the Virtual Chassis are listed on the left side of the chassis view. To view the ports of a member device, click the member device.
- Overview tab—Displays widgets with information related to device details and statistics, such as number of links that are up and down, resource utilization, top ports consuming maximum bandwidth.
- Configuration template tab—Displays the configuration templates applied on the device.
- Ports tab—Lists all the ports on the device. You can manage the switch ports from here.
- Device Settings tab—Lists the access profiles configured in CSO. A check mark appears before the access profile that is deployed on the switch. You can change the access profile deployed on the switch from this tab.

On the *Device-Name* page, you can monitor the device at:

- Port level; see “Monitor Port Level Information” on page 112.
- Chassis level; see “Monitor Chassis-Level Information” on page 113.
- Device level; see “Monitor Device Level Information” on page 119.

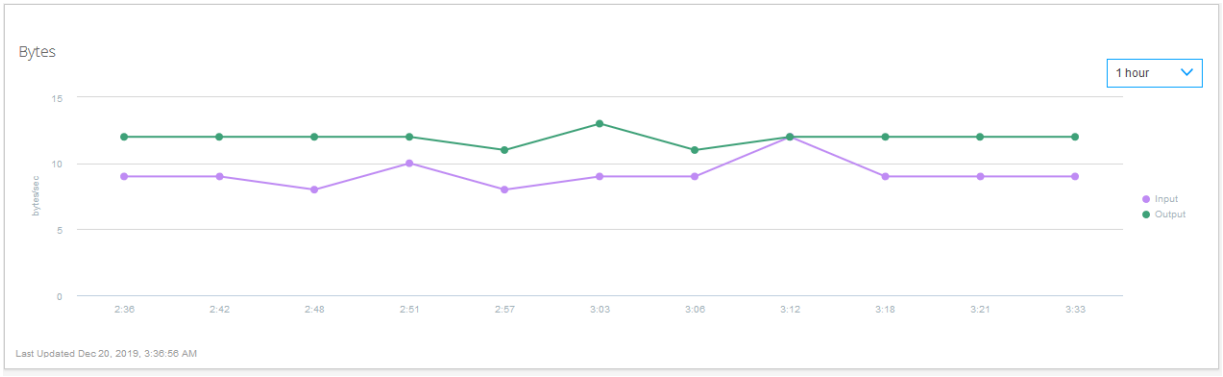
Monitor Port Level Information

To view port level information of a switch, click the **Ports** tab and then click on a port to view the information and statistics for the port.

You can view the following information about a port for the past 1 hour, 8 hours, 1 day, 1 week, and 1 month time duration:

- Details—Provides port details such as port number, admin status, link mode, and so on.
- Utilization—Displays the CPU utilized (in %) by the port for processing the incoming and outgoing packets during the selected time span.
- Errors—Displays the number of errors in the incoming (input) and outgoing (output) packets for the selected time span.
- Packet Loss—Displays number of incoming (input) and outgoing (output) packets lost for the selected time span.
- Bytes—Displays the incoming (input) and outgoing (output) packets in bytes for the selected time span as shown in Figure 14 on page 113.

Figure 14: Incoming and Outgoing Bytes in a Port



- Packets—Represents the number of incoming (input) and outgoing (output) packets for the selected time span.

> **NOTE:** The statistics on the Port Overview tab are refreshed after every 30 seconds. The date and time of the last refresh appear at the bottom-left corner on each widget.

Monitor Chassis-Level Information

The chassis view, present at the top of the *Device-Name* page, displays the device model and the switch ports in a graphical format.

For a Virtual Chassis (VC), the members are displayed on the left side of the chassis view. You can click on a member device to view its ports.

NOTE: The chassis view is refreshed after every 60 seconds.

The ports on the chassis view are color coded depending on the admin and link statuses:

- Green—If the admin status and link status are up.
- Red—If the admin status is up and the link status is down.
- Dark Gray—If the admin status and link status are down.
- Light Gray—If the port is not configured as part of any LAN segment.

You can hover over a port on the chassis view to view general information (such as administrative status, link status, and link mode) about the port.

Figure 15: Port Details Displayed on a Virtual Chassis.

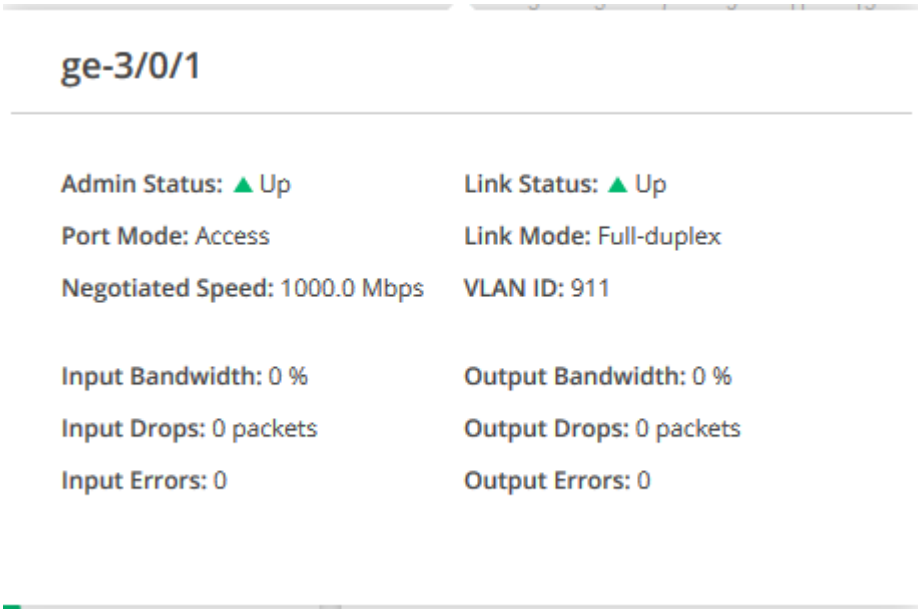


Table 23 on page 114 describes the port details that you can see on the chassis view.

Table 23: Port Details Displayed on Chassis View

Field	Description
Admin Status	Indicates whether the administrative status of the port is up (Up) or down (Down): The ports are color-coded to indicate the administrative status: • Green—Indicates that the admin status is up (enabled). • Gray—Indicates that the admin status is down (disabled).

Table 23: Port Details Displayed on Chassis View *(continued)*

Field	Description
Link Status	Indicates whether the operational status of the connection with a peer port is up (Up) or down (Down). The ports are color-coded to indicate the administrative status: • Green—Indicates that the connection to the port is up. • Red—Indicates that the connection to the port is down.
Port Mode	Indicates the mode in which the port operates: • Access (default)—Only one VLAN is configured on the port. • Trunk—One or more VLANs are configured on the port. (Optional) A native VLAN may also be configured.
Link Mode	Mode in which the link to the port operates—Half-duplex or Full-duplex.
Power Consumption	Power consumed by the port, in watts (W).
PoE Status	Indicates whether the port is configured to transmit electrical power through an Ethernet cable (ON) or not (OFF).
Negotiated Speed	Current negotiated speed (in Kbps, Mbps, and Gbps) of the port.
VLAN	ID of the VLAN configured on the port.
Input Bandwidth Utilization	Bandwidth (in %) consumed by the incoming packets on the port.
Output Bandwidth Utilization	Bandwidth (in %) consumed by the outgoing packets on the port.
Input Drops	Number of incoming packets dropped by the port due to congestion.
Output Drops	Number of outgoing packets dropped by the port due to congestion.
Input Errors	Number of errors in the incoming packets.
Output Errors	Number of errors in the outgoing packets.

Monitor System Health

Table 24 on page 116 describes the system meters available on the chassis view.

> **NOTE:** The UI is refreshed once every 30 seconds while the CSO database polls the devices every five minutes. So, it may take up to five minutes for the statistics to be updated.

Table 24: System Meters on the Chassis View Dashlet

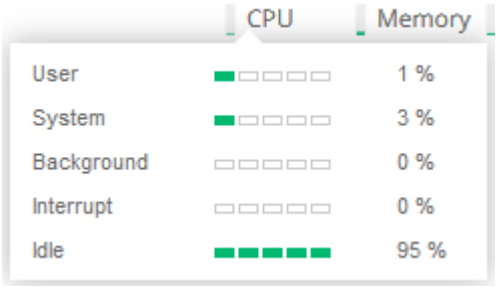
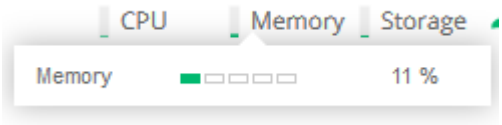
System Meter	Description
CPU	Displays the percentage of CPU utilized by users, system, background processes, interrupts, and the percentage of time the CPU was idle; see Figure 16 on page 116. **Figure 16: CPU Meter**  For a VC, the CPU meter is displayed only for the primary member.
Memory	Memory (in %) utilized in the switch; see Figure 17 on page 116 **Figure 17: Memory Meter**  For a VC, memory is displayed only for the primary member.

Table 24: System Meters on the Chassis View Dashlet *(continued)*

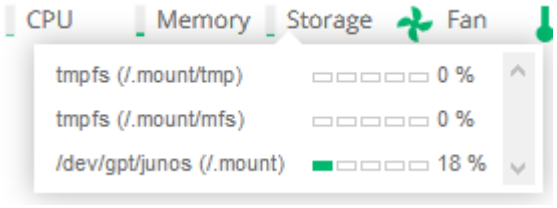
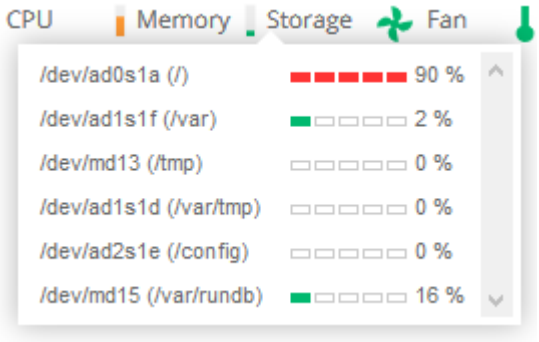
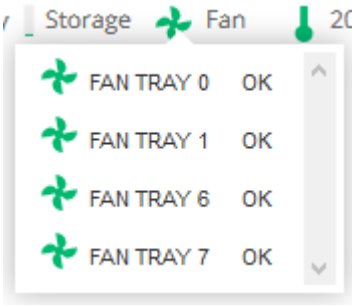
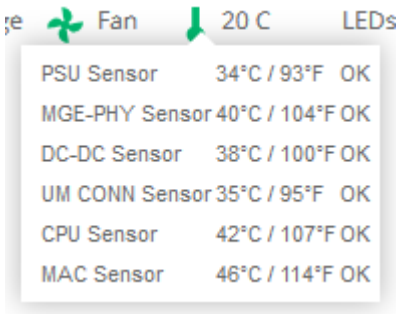
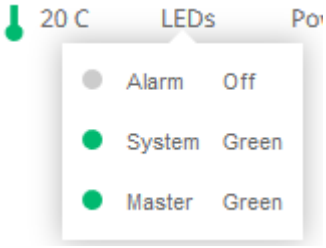
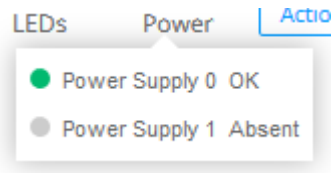
System Meter	Description
Storage	Storage space (in %) allocated to the logical partitions of the switch. Figure 18 on page 117 shows the storage meter for a VC, while Figure 19 on page 117 shows the storage meter for a physical device. **Figure 18: Virtual Chassis Storage Meter**  **Figure 19: Physical Device Storage Meter** 
Fan	Details of the fan present on the switch; see Figure 20 on page 117. **Figure 20: Fan Tray Indicator**  For a VC, FAN is displayed only for the primary member.

Table 24: System Meters on the Chassis View Dashlet *(continued)*

System Meter	Description
Temperature	Temperature of the components in the available FPC; see Figure 21 on page 118. **Figure 21: Temperature Indicator** 
LEDs	Severity level of the Alarms, System, and Primary LEDs; see Figure 22 on page 118. **Figure 22: LED Indicator** 
Power	Details of the switch power supplies; see Figure 23 on page 118. **Figure 23: Power Supply Indicator** 

Monitor Device Level Information

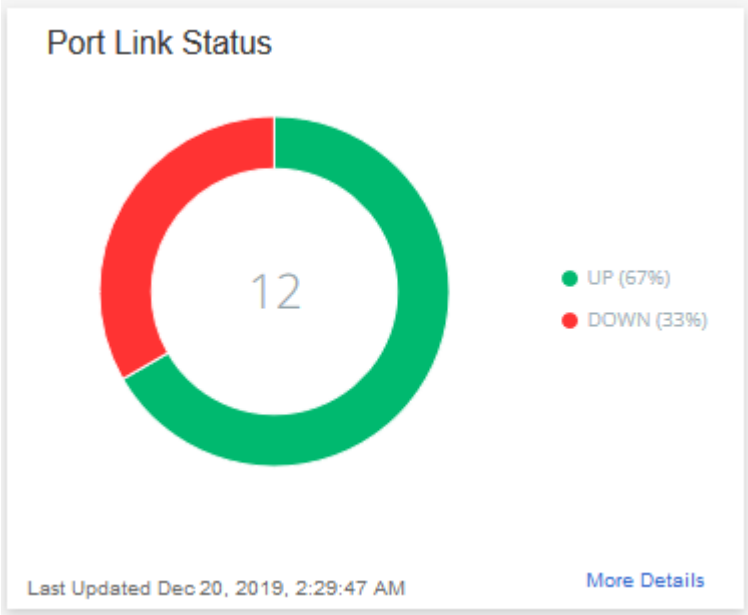
You can view the following device information and device level statistics for the past 1 hour, 8 hours, 1 day, 1 week, and 1 month in the Overview tab of the *Device-Name* page:

- Port Link Status—Represents the number of links that are up and down in the switch as a Donut chart.

  Mouse hover over the chart to view the number and percentage of links that are up and down; see Figure 24 on page 119.

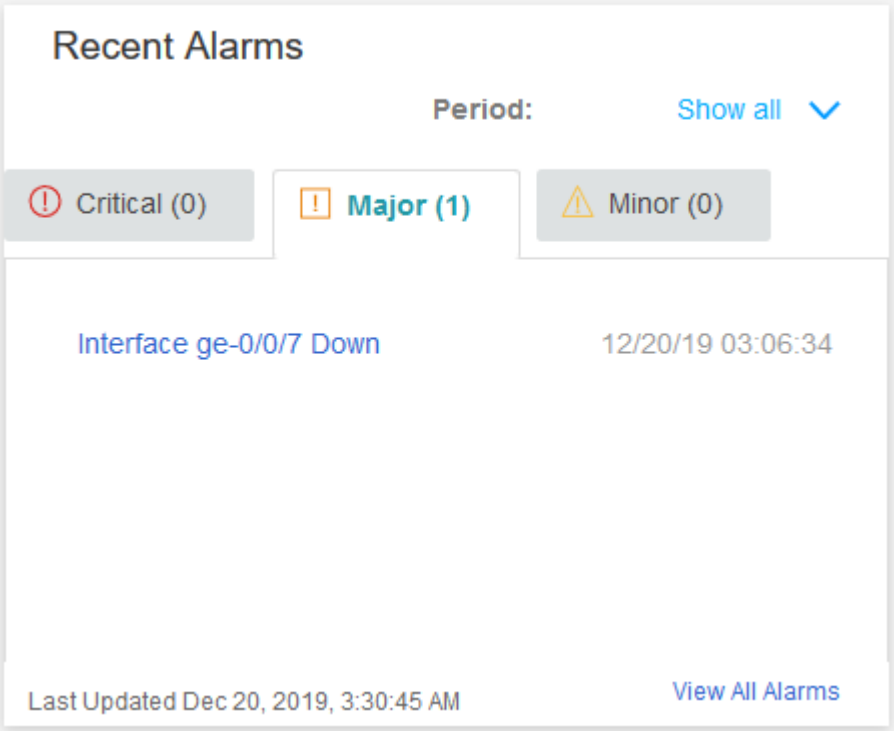
  Click the **More Details** link to view the Ports tab.

Figure 24: Port Link Status for a Switch



- Recent Alarms—Lists the recent critical, major, and minor alarms generated on the switch; see Figure 25 on page 120.

Figure 25: Recent Alarms on a Device



Click the *View All Alarms* link to view information about all the alarms, on the Alarms page.

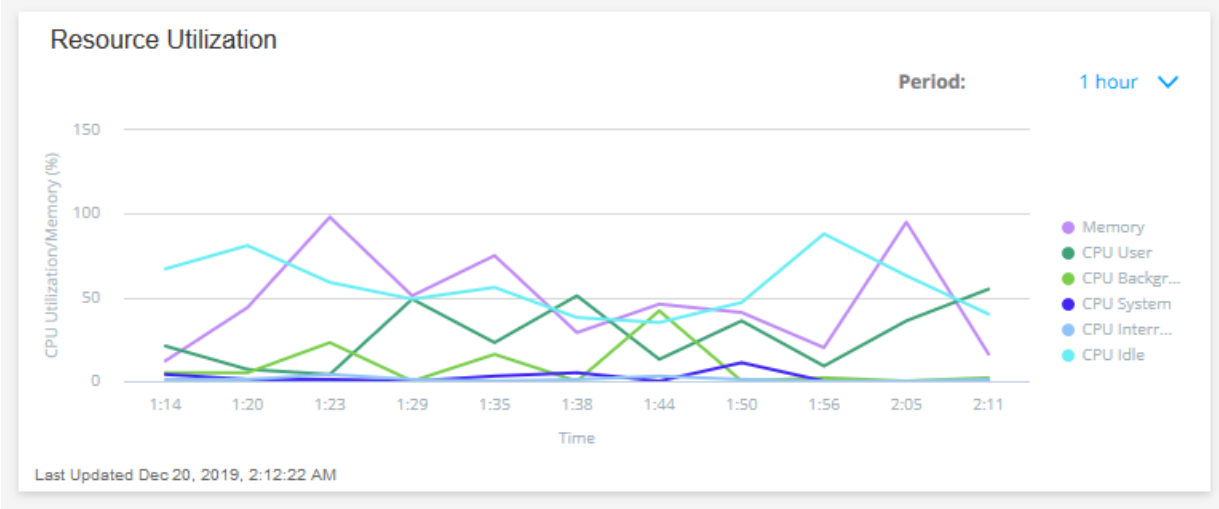
See About the Alarms Page for more information.

- Details—Displays generic details, such as serial number, management IP address, OS version, and device template used to configure the switch.
- Resource Utilization—Displays the percentage of memory and CPU utilized in the switch for the selected time span; see Figure 26 on page 121.

  CPU utilization is displayed for the following processes—user, background, system, interrupt, and idle.

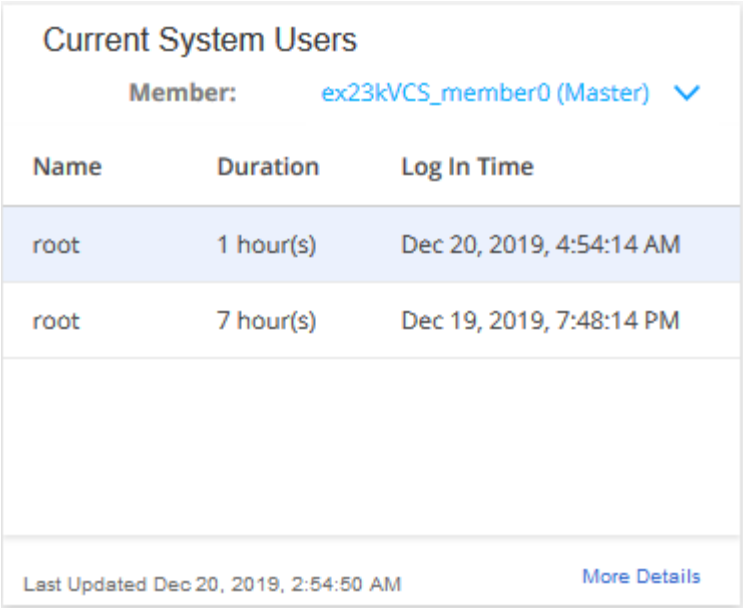
  NOTE: The CPU user process indicates the percentage of time that the CPU is handling user operations.

Figure 26: Memory and CPU Utilized by the Switch



- Current System Users—Displays details (such as name, duration, and login time) of the users who are currently logged in to the switch; Figure 27 on page 121 shows users logged in to a Virtual Chassis.

Figure 27: Current System Users

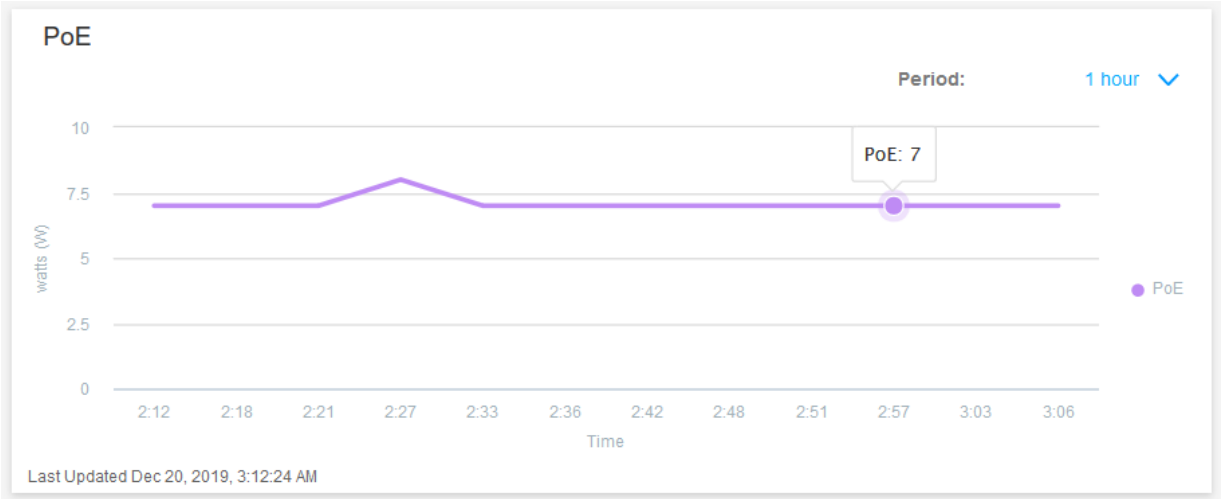


Click the *More Details* link on this pane to view additional information (such as username and session type) about the current users, on the View Details page.

- PoE—Displays the total power [in Watts (W)] provided by the PoE interfaces; see Figure 28 on page 122.

NOTE: This graph is displayed only for P models of EX Series switches.

Figure 28: Power over Ethernet Statistics

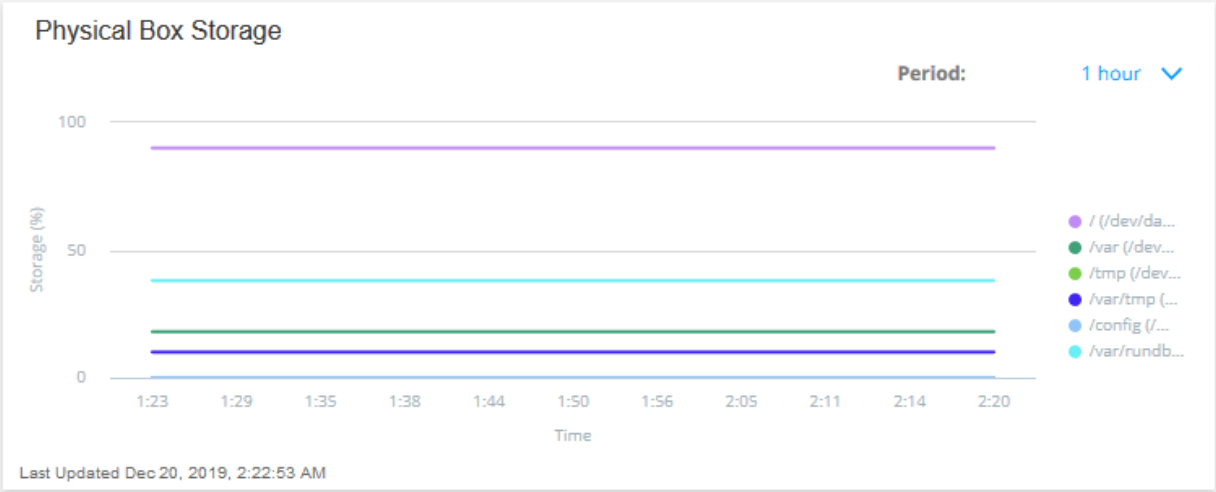


- Top Ports by Input Bandwidth—Displays the top 10 ports on which the incoming packets consume the maximum bandwidth.
- Top Ports by Output Bandwidth—Displays the top 10 ports on which the outgoing packets consume the maximum bandwidth.
- Top Ports with Input Errors—Displays the top 10 ports with the highest number of errors in incoming packets.
- Top Ports with Output Errors—Displays the top 10 ports with the highest number of errors in outgoing packets.
- Top Ports with Input Packet Loss—Displays the top 10 ports that drop the highest number of incoming packets.
- Top Ports with Output Packet Loss—Displays the top 10 ports that drop the highest number of outgoing packets.
- Licenses—Displays details of licenses (such as license name and description) installed on the switch.

  Click the **More Details** link on this pane to view additional information about the licenses, on the Device License Files page.

  See About the Device License Files Page for more information.
- Physical Box Storage—Displays the storage space (in %) allocated to the logical partitions of the switch; see Figure 29 on page 123.

Figure 29: Space Consumed by Different Partitions on the Switch

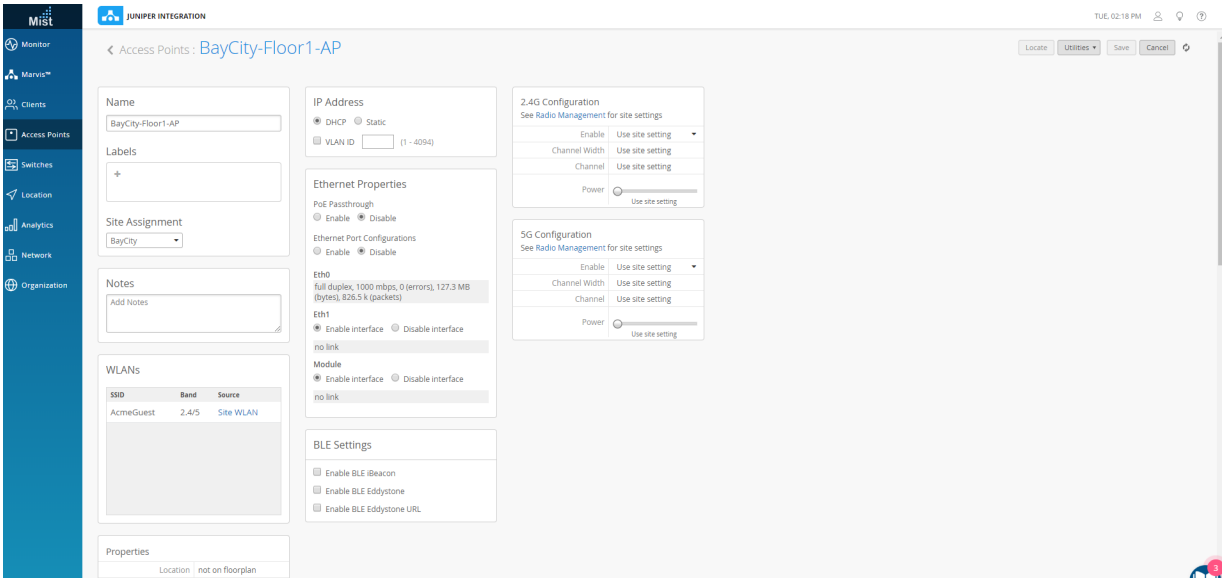


Monitor Mist Access Points

You can view and monitor the Mist access points on Mist Portal. Mist Portal displays WLANs, Ethernet properties, Bluetooth Low Energy (BLE) settings, and other configurations such as 2.4GHz and 5GHz configurations. Figure 30 on page 124 shows an access point displayed on Mist Portal.

For information about monitoring the access points, see Mist documentation at https://www.mist.com/documentation/category/insights/.

Figure 30: Details of an Access Point Displayed on Mist Portal



CHAPTER 7

Troubleshoot Issues

Gather Troubleshooting Data | **126**

Troubleshoot Connectivity Issues Between the Switch and CSO | **127**

Virtual Chassis is not Connecting to CSO | **129**

Device Activation is Failing When Using ZTP | **131**

ZTP of an EX Series Switch is Failing | **132**

Device Statistics are not Displayed | **133**

Unable to Monitor Ports | **134**

Chassis View is not Refreshing | **134**

Ports are not Reflecting the Configured Behavior | **135**

Gather Troubleshooting Data

Gather the following information for troubleshooting:

- All the configuration information of the site associated with the device that you want to troubleshoot.

  To download the configuration information of a site:

  1. In Customer Portal, access the tenant in which the site is present.
  2. Navigate to **Monitor > Jobs**.

     The Job page appears.
  3. Click the job that was triggered to create the site.

     The Job Status page appears.
  4. Click **View Detailed Logs**.

     The View Job Log page appears.
  5. Select **All** in the drop-down menu and click **Download Logs**.
  6. Open or save the file on your local system.

     The logs are downloaded as a ***.csv** file.

- Stage-1 configuration on the devices in the site

  To download the stage-1 configuration:

  1. In Customer Portal, navigate to **Resources > Devices**.

     The Devices page appears
  2. Select the switch for which you want to download the stage-1 configuration and click **Stage1 Config**.

     The Copy the following config and deploy it to the device page appears displaying the stage-1 configuration pushed to the device by CSO.
  3. Click **Save as** to save the file on your local system.

- Job IDs and details of failed jobs

  To obtain details of failed jobs:

1. In Customer Portal, access the tenant in which the site is present.
2. Navigate to **Monitor > Jobs**.

   The Job page appears.
3. Search for the jobs with failed status.

   The Jobs page lists all the jobs for the tenant that failed.
4. Click a failed job pertaining to the site or the device of your interest.

   The Job Status page appears.
5. Click **View Detailed Logs**.

   The View Job Log page appears.
6. Select **All** in the drop-down menu and click **Download Logs**.
7. Open or save the file on your local system.

   The logs are downloaded as a ***.csv** file.

- Device system logs and core dumps

  Execute the **show log** and the **show system core-dumps** command to obtain the log and core dump files from the switch.
- Outstanding alarms on the device

  Execute the **show system alarms** command to obtain the active alarms on the switch.
- Operational status of the device
- Outputs for standard troubleshooting commands; for example: **show system license**, **show system app-id version**, **show security flow-session destination-prefix 8.8.8.8**, and **netstat -an|grep 7804**.

Troubleshoot Connectivity Issues Between the Switch and CSO

Problem
Description: Switch is not connecting to CSO.

Solution

To troubleshoot connectivity issues:

- Ensure that a proper time is set on the device. To verify the time, execute the following command in the operational mode on the switch:

  For a VC, execute the command on the primary VC.

```
Cli> show system uptime
```

```
Current time: 2020-01-06 20:17:36 UTC
Time Source:  LOCAL CLOCK
System booted: 2019-12-22 00:00:23 UTC (2w1d 20:17 ago)
Protocols started: 2019-12-22 00:03:13 UTC (2w1d 20:14 ago)
Last configured: 2020-01-06 19:02:32 UTC (01:15:04 ago) by root
8:17PM  up 15 days, 20:17, 1 user, load averages: 0.00, 0.01, 0.00
```

  If the time displayed is not the current time, either configure an NTP server or set time manually using the **set date** command in the YYYYMMDDhhmm.ss) format.

```
> set date 202001061218.00
```

- Ensure that an IP address is assigned to the switch and a default route is assigned.

  Check the IP address by using the **cli> show interfaces terse** command.

  Also, check for the default route (0.0.0.0) by using the **cli> show route** command.

- Ensure that the device is able to connect to TCP ports 443 and 7804 of CSO.

  Use the following commands to check whether the switch can reach ports 7804 and 443 of CSO:

```
root> telnet <cso-hostname> port 443
root> telnet <outbound-ssh-ip> port 7804

      where, <cso-hostname> is the hostname of the CSO server and <outbound-ssh-ip>
      is the outbound ssh IPv4 address of the switch. You can view the outbound-ssh
      IPv4 address in the set system services outbound-ssh client line present in
      the stage-1 configuration of the switch. For example:

      set system services outbound-ssh client CSO-xxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx 192.168.0.1.. port
      7804
```

  If the switch is unable to connect to TCP ports 443 and 7804, ensure that these ports are not blocked by the network firewall.

If the switch is unable to connect, check the DNS server configuration on the switch. The DNS server should be obtained either by using a DHCP server or should be configured statically.

Execute the **cat /etc/resolv.conf** command on the switch to view the DNS server that is configured.

If there is no DNS server configured to resolve the hostnames, do one of the following:

- Map IP hostname manually in the **/etc/hosts** file on the switch.
- Configure a static DHCP server by using the **set system name-server 8.8.8.8** command.

- Ensure that the device is able connect to redirect.juniper.net.

```
root> telnet redirect.juniper.net port 443
```

```
Trying 192.168.50.50 ..
Connected to <Redirect server host-name>.
 Escape character is '^]'.
```

Virtual Chassis is not Connecting to CSO

Problem
Description: Virtual Chassis (VC) is not connecting to CSO

Solution

To resolve this issue:

- Ensure that all the members of the VC are up and the status of the members is PRSNT in the **show virtual-chassis** command.
- Verify that the serial number that you entered while configuring the site is that of the primary member in the VC.

  Execute the **show virtual-chassis** command on any member of the VC to find the serial number of the primary.

  If the serial number you provided is not the same as the serial number of the primary, edit the serial number.
- Log in to the primary member of the VC and try to access the ports 443 and 7804 on CSO by using Telnet to check reachability of CSO from the switch. Ping may or may not work.

```
root> telnet <cso-hostname> port 443
root> telnet <outbound-ssh-ip> port 7804
```

where, **<cso-hostname>** is the hostname of the CSO server and **<outbound-ssh-ip>** is the outbound ssh IPv4 address of the switch. You can view the outbound-ssh IPv4 address in the **set system services outbound-ssh client** line present in the stage-1 configuration of the switch. For example:

set system services outbound-ssh client CSO-xxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx 192.168.0.1.. port 7804

- Log in to the primary member and execute the **tail -f /var/log/messages** command to look for any error messages related to the VC not being able to connect to CSO.

  Table 25 on page 130 lists the error messages to look for that indicate connectivity issues with CSO.

  Table 25: Error Messages Indicating Connectivity Issues with CSO

Error	Cause and Action
404/400 from redirect server	• Device serial number might not be registered in redirect server To resolve this issue, look into the site creation log in the CSO. If there is an error indicating that device serial number is not available, contact Juniper support to add the serial number to the redirect server. • Verify the serial number entered while creating a site to ensure there are no typos. You should provide the serial number of the primary device while configuring the site. • Verify the audit logs for the Site Creation job to ensure that the site is configured properly.
401 Unauthorized	It is normal for this error message to appear once. This error message indicates that the device can reach CSO and CSO is able to recognize the device. But, if this message appears multiple times, verify whether the Auto Activate option was disabled while configuring the site. If the option is disabled, activate the device manually from the Devices page.. To verify, select the site and click the **Edit** icon (Pen) on the Sites page (**Resources > Site Management**). The Auto Activate field indicates whether auto activation was enabled or disabled while configuring the site. Enable the Auto Activate option, if needed. In some rare cases, if the same serial number is used in another tenant, the 401 unauthorized message may be thrown continuously.

Table 25: Error Messages Indicating Connectivity Issues with CSO *(continued)*

Error	Cause and Action
Unable to resolve hostname	Device is not able to resolve redirect.juniper.net or the CSO hostname into IP address. Check the DNS server configuration on the device. The DNS server should be obtained either by using a DHCP server or should be configured statically. The DHCP server provides the DNS server to the switch for resolving the redirect server and CSO server hostnames. Execute the **cat /etc/resolv.conf** command on the switch to view the DNS server that is configured. If there is no DNS server configured to resolve the hostnames, do one of the following: • Map IP hostname manually in the **/etc/hosts** file on the switch. • Configure a static DHCP server by using the **set system name-server 8.8.8.8** command.
Certificate Verification Failed	Ensure that the NTP server assigned to the switch is working fine and that the time displayed on the switch is close to the current time.

Device Activation is Failing When Using ZTP

Problem
Description: Zero-touch provisioning (ZTP) is failing on the switch.

Solution

For an EX Series switch, ZTP is only supported on Junos OS Releases 18.4R2.7 and 18.4R3.3. Check the version of Junos OS installed on the device by using the **show version** command for a physical switch and **show version all-members** command for a virtual chassis.

If the Junos OS version is earlier than Junos OS Release 18.4R2.7 and 18.4R3.3, upgrade the image on the device and attempt device activation again.

ZTP is not supported on EX4300MP, EX4600, and EX4650 switches.

To troubleshoot device activation failure during ZTP, check the ZTP logs for error messages on the **Monitor > Jobs** page on the CSO GUI. ZTP might fail because of any of the following reasons:

- Device unable to reach TCP port 7804 on CSO.

  Verify reachability to port 7804 on CSO from the outbound-ssh IP address present in the Stage-1 configuration. You can obtain the Stage-1 configuration of the switch from the Devices tab of the Sites page (**Resources > Site Management**) of the CSO GUI.

You can view the outbound-ssh IP address from the statement similar to the following sample in the stage-1 configuration:

```
set system services outbound-ssh client CSO-xxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx
192.168.0.1.. port 7804
```

- The device might have failed to initiate connection to CSO.

  Execute the following command by logging in to the CLI to verify whether the device can initiate connection to CSO and whether the connection to CSO is established.

```
{master:0}
root@host> show system connections | match 7804
tcp4       0      0  192.2.2.2.60225                            203.0.113.10.7804
                           ESTABLISHED
tcp4       0      0  192.2.2.2.56840                            203.0.113.10.7804
                           ESTABLISHED
```

  You can also verify the connection status by logging into the shell of the device.

```
netstat -an | grep 7804
root@host> start shell
root@host:RE:0% netstat -an | grep 7804
tcp4       0      0  192.2.2.2.51973        203.0.113.10.7804       ESTABLISHED
```

- Conflicting configuration might be causing commit errors.

  View the ZTP logs in one of the following ways and rectify the conflicting error:

  - On the **Monitor > Jobs** page.
  - You can also view the ZTP logs by executing the **tail -f /var/log/phc.log** or **tail -f /var/log/messages** command from the device shell.
  - You can also use the **monitor start phc.log** or **monitor start messages** commands to view the ZTP logs.

ZTP of an EX Series Switch is Failing

Problem

Description: ZTP of an EX Series switch is failing.

Solution

ZTP of an EX Series switch may fail because of the following reasons:

For a switch connected behind a CPE or firewall:

- DHCP may not be configured on the link connecting the switch to the CPE, firewall, or Internet gateway.

  To rectify this issue, try connecting the switch to CPE or next-generation firewall after the CPE is fully provisioned.

- If the CPE or next-generation firewall connected to the switch is an SRX Series device, there may be issues with the certificates installed on the SRX series device.

  To rectify this issue, disable the AUTO_INSTALL_DEFAULT_TRUSTED_CERTS_TO_DEVICE parameter in the SRX Series device template and retry adding the site with the SRX series device and the switch. Reinstall certificates on the SRX Series device after ZTP of the CPE and the switch is successful.

- If the CPE or next-generation firewall connected to the switch is an SRX Series device running on Junos OS release 19.3R2-S1 or 19.3R2-S2, the port connecting to the CPE or next-generation firewall and the switch might be blocked by RSTP.

  To resolve this issue, disable the RSTP protocol on the SRX Series device or add the **set protocols rstp force-version stp** statement as part of the stage-2 configuration on the SRX Series device.

- The trunk ports connecting the CPE or next-generation firewall and the EX Series switch may be assigned to a LAN segment.

  To resolve this issue, check the ports connecting the switch and the CPE or firewall. If the trunk port is assigned to a LAN segment, remove the association of the LAN segment configured on the trunk port and retry ZTP,

- If the bootstrap process is failing, check the trunk ports connecting the CPE or next-generation firewall and the switch by using the **show lldp neighbors** command. The port that you assigned in the CPE may not be actually connected to the trunk ports of the switch and therefore, the switch might not be getting the DHCP information resulting in ZTP not succeeding.

  To resolve this issue, reconnect the CPE or next-generation firewall and the switch.

Device Statistics are not Displayed

Problem

Description: The switch statistics are not displayed on the dashboard on the *Device-Name* page.

Solution

The CSO GUI fetches data from the CSO database once every 30 seconds. The CSO database polls the switch once every five minutes. So, it might take upto five minutes for changes in the device statistics to be reflected.

If the statistics is not populating even after 10 minutes, contact Juniper support.

Unable to Monitor Ports

Problem
Description: Statistics are not displayed for a port.

Solution

To rectify this issue:

- Ensure that the port is assigned to a VLAN.

  To check whether the port is assigned to a VLAN:

  1. Select the port in the Ports tab.
  2. Click **More > Edit Configuration**.

     The Edit Configuration page appears.

  You can view the VLANs assigned to the port in the VLANs field.

- Ensure that the port is configured on CSO. CSO monitors only those ports that are configured through CSO and is part of a VLAN.

  You can verify whether a port is configured through CSO or not on the Ports tab of the *Devices* page. The Admin Status of a port that is not configured through CSO is set to **Unconfigured**.

- The CSO GUI fetches data from the CSO database once every 30 seconds The CSO database polls the switch once every five minutes. So, it might take upto five minutes for changes in the device statistics to be reflected.

  If the statistics is not populating even after 10 minutes, contact Juniper support.

Chassis View is not Refreshing

Problem
Description: Chassis view is not refreshing.

Solution

The CSO GUI fetches data from the CSO database once every 30 seconds The CSO database polls the switch once every five minutes. So, it might take upto five minutes for changes in the device statistics to be reflected.

If the statistics is not populating even after 10 minutes, contact Juniper support.

Ports are not Reflecting the Configured Behavior

Problem

Description: Ports are not reflecting the configured behavior.

Solution

Ports may not reflect the configured behavior for one of the following reasons:

- A wrong port profile is deployed on the port.

  To rectify this issue:

  1. Check the port profile assigned to the port on the Ports tab of the *Devices* page (**Resources > Devices**).

     The Port Profile column displays the port profile assigned to the port. If the port is configured manually, Manually Configured is displayed.

  2. Verify the port configuration by clicking **More > Edit Configuration** and modify the configuration or the port profile assigned to the port, as needed.

- The port profile is only assigned and not deployed on the port.

  If the port profile is only assigned, the Deployment Status of the port is set to Pending Deployment. Select the port and click **More > Deploy** to deploy the profile.

8

CHAPTER

Appendix

Prepare a Virtual Chassis for Onboarding to CSO | **137**

Default Configuration Templates For EX Series Switches | **141**

Creating a LAN Segment for Discovering Mist Access Points | **142**

Prepare a Virtual Chassis for Onboarding to CSO

IN THIS SECTION

- Setting up a Virtual Chassis for Provisioning | 137
- Setup a Virtual Chassis for Autoprovisioning | 138
- Setup a Virtual Chassis for Preprovisioning | 139
- Members Allowed in a Virtual Chassis | 140

This topic provides steps on how to prepare a Virtual Chassis for onboarding to CSO. CSO supports the onboarding and provisioning of the following Virtual Chassis:

- EX2300 Virtual Chassis
- EX3400 Virtual Chassis
- EX4300 Virtual Chassis
- EX4600 Virtual Chassis
- EX4650 Virtual Chassis

Setting up a Virtual Chassis for Provisioning

You can provision a Virtual Chassis in one of the following ways:

- Autoprovisioning: The Virtual Chassis determines the roles (primary, backup, and line card) of the member devices.
- Preprovisioning: You determine the roles (primary, backup, and line card) of the member devices in the Virtual Chassis.

Before you provision a Virtual Chassis, ensure that:

- All members of the Virtual Chassis are wired and working; that is, the Virtual Chassis Ports (VCP) on the member devices are connected to each other.
- Virtual Chassis mode is enabled on all the member devices.
- Virtual Chassis management entity on all member devices can communicate with CSO.

For information about the number of member devices allowed in each Virtual Chassis, see “Members Allowed in a Virtual Chassis” on page 140.

Setup a Virtual Chassis for Autoprovisioning

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 primary 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.

Setup a Virtual Chassis for Preprovisioning

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

Members Allowed in a Virtual Chassis

Table 20 on page 88 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 26: Supported Device Types, Modes, and Number of Members Allowed in a Virtual Chassis

Virtual Chassis	Virtual Chassis Member	Number of Members Allowed
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.

Default Configuration Templates For EX Series Switches

A configuration template is used to deploy configurations such as user, password, SNMP, and Class of Service on to the switch after it is activated.

Table 27 on page 141 lists the default configuration templates available in CSO for configuring an EX Series switch.

Table 27: Default Configuration Templates Provided by CSO

Configuration Template	Description
Local User	Configure users on an EX Series switch.
EX password config	Configure password for an EX Series switch.
SNMP Configuration	Configure SNMP on an EX Series switch.
PoE	Configure PoE on an EX Series switch.
Banner	Configure the banner text for an EX Series switch.
DNS	Configure DNS on an EX Series switch.
NTP	Configure NTP on an EX Series switch.
Service	Configure services on an EX Series switch.
Syslog	Configure system log parameters on an EX Series switch.
IGMP Snooping	Configure IGMP snooping on an EX Series switch.
Class of Service	Configure Class of Service (CoS) on an EX Series switch.
LACP	Configure LACP on an EX Series switch.
LAG Trunk	Configure a link aggregation group (LAG) on a switch when the switch is operating in trunk mode..
MC-LAG	Configure multichassis link aggregation group (MC-LAG) on an MC-LAG peer device.

Table 27: Default Configuration Templates Provided by CSO *(continued)*

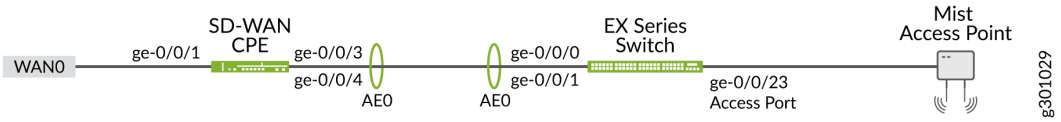
Configuration Template	Description
VRRP	Configure VRRP on an EX Series switch.

For information about using configuration templates, see "Configure an EX Series Switch by Using Configuration Templates" on page 97.

Creating a LAN Segment for Discovering Mist Access Points

Figure 31 on page 142 depicts the LAN segment connecting the SD-WAN CPE or firewall and the EX port connecting the Mist access points.

Figure 31: LAG Segment for Discovering Access Points



To create a LAN segment for discovering Mist access points:

1. On the Sites page (**Resources > Site Management**), click the CPE or next-generation firewall site.

   The *Site-Name* page appears.

2. Click the **LAN** tab and configure the following parameters for the LAN segment:
   - Name
   - VAN ID
   - Gateway/Address Mask
   - Enable the DHCP server
3. Click **Save**.

   The LAN segment is created on the CPE or next-generation firewall.

4. Click the **Devices** tab on the Site management page.

The devices present in the site are listed.

5. Click on the switch for which you want to discover the connected access points.

   The *device-name* page appears.

6. Click the **Ports** tab.

   The ports on the switch are displayed.

7. Click the port that is connected to the access point and select **More > Edit Configuration**.

   The Edit port Configuration page appears.

8. Do the following:
   - For Configuration options, select **Manual**.
   - For Port type, select Access.
   - For VLAN, Select the LAN segment created in step 3 and move it to the Selected column.
9. Click Next and click Deploy Now.

   A job is created to deploy the configuration.

After the configuration is deployed, you can enable the option to integrate CSO with Mist Portal; see “Integrate CSO with Mist Portal” on page 108.