JUNIPER NETWORKS | Engineering Simplicity

J-Web Application Package for EX Series Ethernet Switches

J-Web Application Package User Guide for EX Series Switches

Published
2024-12-20

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.

J-Web Application Package for EX Series Ethernet Switches J-Web Application Package User Guide for EX Series Switches
Copyright © 2024 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 This Guide | x

1 **Overview**

Overview | 2

J-Web User Interface for EX Series Switches Overview | **2**

J-Web Interface—Application Package | **6**

Understanding J-Web User Interface Sessions | **14**

Dashboard for EX Series Switches | **14**

Understanding J-Web Configuration Tools | **50**

Understand Alarm Types and Severity Levels on EX Series Switches | **52**

Using the Commit Options to Commit Configuration Changes (J-Web Procedure) | **54**

2 **Configuration**

Starting J-Web | 58

Starting the J-Web Interface | **58**

J-Web Configuration Tools | 59

Using the Point and Click CLI Tool in the J-Web Interface to Edit Configuration Text | **59**

Using the CLI Editor in the J-Web Interface to Edit Configuration Text | **61**

Using the J-Web CLI Terminal | **62**

- Configuring the Web Browser | **62**
- Setting Domain Name, Hostname, and Name Server | **63**
- Enabling SSH on your system | **63**
- Sample Configuration on an EX Series Switch | **63**

Using the CLI Viewer in the J-Web Interface to View Configuration Text | **64**

System Basics Configuration | 66

Connecting and Configuring an EX Series Switch (J-Web Procedure) | **66**

Configuring Date and Time for the EX Series Switch (J-Web Procedure) | **70**

Configuring System Identity for an EX Series Switch (J-Web Procedure) | 71

Configuring Management Access for the EX Series Switch (J-Web Procedure) | 73

Generating SSL Certificates to Be Used for Secure Web Access (EX Series Switch) | 76

Rebooting or Halting the EX Series Switch (J-Web Procedure) | 77

Class of Service Configuration | 79

Defining CoS Drop Profiles (J-Web Procedure) | 79

Defining CoS Classifiers (J-Web Procedure) | 80

Defining CoS Code-Point Aliases (J-Web Procedure) | 83

Assigning CoS Components to Interfaces (J-Web Procedure) | 84

Defining CoS Forwarding Classes (J-Web Procedure) | 86

Defining CoS Rewrite Rules (J-Web Procedure) | 87

Defining CoS Schedulers (J-Web Procedure) | 90

Defining CoS Scheduler Maps (J-Web Procedure) | 95

Security and Management Configuration | 97

Configuring 802.1X Authentication (J-Web Procedure) | 97

Configuring LLDP (J-Web Procedure) | 100

Configuring Port Mirroring to Analyze Traffic (J-Web Procedure) | 102

Configuring Port Security (J-Web Procedure) | 104

Routing Policies and Packet Filtering Configuration | 108

Configuring Routing Policies (J-Web Procedure) | 108

Configuring Firewall Filters (J-Web Procedure) | 116

Ethernet Switching Configuration | 123

Configuring VLANs for EX Series Switches (J-Web Procedure) | 123

Configuring Spanning Tree Protocols on EX Series Switches (J-Web Procedure) | 127

Configuring IGMP Snooping on EX Series Switches (J-Web Procedure) | 133

Configuring Redundant Trunk Groups on EX Series Switches (J-Web Procedure) | 137

Interfaces | 139

Configuring Gigabit Ethernet Interfaces (J-Web Procedure) | **139**

Configuring Aggregated Ethernet Interfaces (J-Web Procedure) | **148**

Configuring PoE (J-Web Procedure) | **153**

- Configuring PoE on EX2200, EX2200-C, EX3200, EX3300, EX4100, EX4100-F, EX4100-H, EX4200, and EX4400 Switches | **153**
- Configuring PoE on EX6200 Switches | **155**

Configuring Services | 158

Configuring DHCP Services (J-Web Procedure) | **158**

- Configuring DHCP Services (J-Web Procedure) on EX Series Switches | **158**

Configuring SNMP (J-Web Procedure) | **162**

Configuring Layer 3 Protocols | 168

Configuring BGP Sessions (J-Web Procedure) | **168**

Configuring an OSPF Network (J-Web Procedure) | **176**

Configuring a RIP Network for EX Series Switches (J-Web Procedure) | **183**

Configuring Static Routing (J-Web Procedure) | **188**

Configuring Real-Time Performance Monitoring | 191

Configuring Real-Time Performance Monitoring (J-Web Procedure) | **191**

Viewing Real-Time Performance Monitoring Information | **201**

Software Installation and Upgrades | 202

Updating J-Web Interface on EX Series Switches (J-Web Procedure) | **202**

- Installing J-Web Application Package by Using Auto Update | **202**
- Installing J-Web Application Package by Using Manual Update | **203**

Upgrading Junos OS on EX Series Switches (J-Web Procedure) | **204**

- Installing Junos OS Upgrades by Uploading File from Local Computer | **204**

Configuration, Files, Users, Licenses, and Product Registration | 206

Managing Configuration Files Through the Configuration History (J-Web Procedure) | **206**

- Displaying Configuration History | **207**
- Displaying Users Editing the Configuration | **208**

Comparing Configuration Files with the J-Web Interface | 209
Downloading a Configuration File with the J-Web Interface | 209
Loading a Previous Configuration File with the J-Web Interface | 210

Setting or Deleting the Rescue Configuration (J-Web Procedure) | 210

Uploading a Configuration File (J-Web Procedure) | 211

Managing Log, Temporary, and Crash Files on the Switch (J-Web Procedure) | 212

Cleaning Up Files | 212
Downloading Files | 213
Deleting Files | 213

Managing Users (J-Web Procedure) | 214

Managing Licenses for the EX Series Switch (J-Web Procedure) | 217

Adding New Licenses | 218
Deleting Licenses | 218
Displaying License Keys | 218
Downloading Licenses | 219

Registering the EX Series Switch with the J-Web Interface | 219

Generating Support Information Reports for EX Series Switches Using the J-Web Interface | 219

Virtual Chassis Configuration | 221

Configuring a Virtual Chassis on an EX Series Switch (J-Web Procedure) | 221

Configuring an EX2200, EX2200-C, EX3300, EX4100, EX4100-F, EX4100-H, EX4200, EX4400, EX4500, or EX4550 Virtual Chassis (J-Web Procedure) | 221

Enabling Virtual Chassis Mode on an EX8200 Switch (J-Web Procedure) | 225

Configuring an EX8200 Virtual Chassis (J-Web Procedure) | 225

Preprovision the Virtual Chassis | 225
Configure Virtual Chassis Members | 226
Configure Virtual Chassis Ports | 226

3 **Monitoring**

Monitoring Tasks | 229

Check Active Alarms with the J-Web Interface | 230

Monitor System Log Messages | 231

Monitoring Chassis Information | 238

Monitoring System Properties | **241**

Monitoring System Process Information | **245**

Monitoring Switch Control Traffic | **246**

Monitoring Interface Status and Traffic | **250**

Monitoring PoE | **252**

Monitoring Hosts Using the J-Web Ping Host Tool | **254**

Monitoring Network Traffic Using Traceroute | **257**

Monitoring DHCP Services | **259**

Monitoring OSPF Routing Information | **264**

Monitoring RIP Routing Information | **269**

Monitoring BGP Routing Information | **271**

Monitoring Routing Information | **275**

Monitoring Ethernet Switching on EX Series Switches (J-Web) | **278**

Monitoring IGMP Snooping | **281**

Monitoring Spanning Tree Protocols on Switches | **282**

Monitoring CoS Classifiers | **286**

Monitoring CoS Drop Profiles | **288**

Monitoring CoS Value Aliases | **290**

Monitoring CoS Forwarding Classes | **291**

Monitoring Interfaces That Have CoS Components | **294**

Monitoring CoS Rewrite Rules | **296**

Monitoring CoS Scheduler Maps | **298**

Monitoring the Virtual Chassis Status and Statistics on EX Series Virtual Chassis | **301**

Monitoring 802.1X Authentication | **303**

Monitoring Port Security | **304**

4 **Administration**

Software, Files, Licenses, Logs | 308

Uploading a Configuration File (J-Web Procedure) | **308**

Managing Configuration Files Through the Configuration History (J-Web Procedure) | **309**

- Displaying Configuration History | **309**
- Displaying Users Editing the Configuration | **311**
- Comparing Configuration Files with the J-Web Interface | **312**
- Downloading a Configuration File with the J-Web Interface | **312**
- Loading a Previous Configuration File with the J-Web Interface | **312**

Setting or Deleting the Rescue Configuration (J-Web Procedure) | **313**

Updating J-Web Interface on EX Series Switches (J-Web Procedure) | **314**

- Installing J-Web Application Package by Using Auto Update | **314**
- Installing J-Web Application Package by Using Manual Update | **315**

Upgrading Junos OS on EX Series Switches (J-Web Procedure) | **316**

- Installing Junos OS Upgrades by Uploading File from Local Computer | **316**

Managing Licenses for the EX Series Switch (J-Web Procedure) | **317**

- Adding New Licenses | **318**
- Deleting Licenses | **318**
- Displaying License Keys | **318**
- Downloading Licenses | **318**

Rebooting or Halting the EX Series Switch (J-Web Procedure) | **319**

Managing Log, Temporary, and Crash Files on the Switch (J-Web Procedure) | **320**

- Cleaning Up Files | **320**
- Downloading Files | **321**
- Deleting Files | **321**

Registering the EX Series Switch with the J-Web Interface | **322**

Generating Support Information Reports for EX Series Switches Using the J-Web Interface | **323**

5 **Troubleshooting**

Troubleshooting Task | 325

Troubleshooting Interface Configuration and Cable Faults | **325**

- Interface Configuration or Connectivity Is Not Working | **325**

FAQ | 327

J-Web Application Package for EX Series—Frequently Asked Questions | 327

About This Guide

Use this guide to configure, monitor, and troubleshoot your EX Series switch using the J-Web Application package. The J-Web Application package provides complete features of J-Web and is an installable package.

- Junos® OS for EX Series Ethernet Switches

1

PART

Overview

Overview | 2

CHAPTER 1

Overview

IN THIS CHAPTER

- J-Web User Interface for EX Series Switches Overview | 2
- J-Web Interface—Application Package | 6
- Understanding J-Web User Interface Sessions | 14
- Dashboard for EX Series Switches | 14
- Understanding J-Web Configuration Tools | 50
- Understand Alarm Types and Severity Levels on EX Series Switches | 52
- Using the Commit Options to Commit Configuration Changes (J-Web Procedure) | 54

J-Web User Interface for EX Series Switches Overview

IN THIS SECTION

- J-Web Packages | 3
- Release Compatibility | 4
- Software Requirements | 5

Juniper Networks EX Series Ethernet Switches are shipped with the Juniper Networks Junos operating system (Junos OS) installed.

Junos OS has the following primary user interfaces:

- Juniper Web Device Manager (J-Web) GUI
- Junos OS CLI

You can use these interfaces to access, configure, and manage your EX Series switch.

This topic provides an overview of the J-Web interface. For information about the CLI, see CLI User Interface Overview.

J-Web Packages

For Junos OS Release 14.1X53-D10 and later, the J-Web interface is available in two packages:

- Platform package—Provides basic features of J-Web and is installed as part of Junos OS.
- Application package—Provides complete features of J-Web and is an installable package.

1. **Platform Package**

   The Platform package of J-Web is installed as part of Junos OS that is shipped with your EX Series switch. The Platform package provides the basic features of the J-Web interface. The Platform package enables you to configure and maintain your switch.

2. **Application Package**

   The Application package is not installed by default on your switch. You must download it and install it over the Platform package on your switch. The Application package provides all the features of the J-Web interface that enable you to configure, monitor, maintain, and troubleshoot your switch.

The Platform package, which is installed as part of the Junos OS that is shipped with your switch, follows the Junos OS release cycle. However, the Application packages have their own release cycle which is independent of the Junos OS release cycle. This separate release cycle helps you get the latest features of J-Web by installing the latest version of the Application package, without waiting for Junos OS releases.

NOTE: The J-Web Application package is hot-pluggable. You can install it on top of the current Junos OS installation, and you need not reboot the switch after the installation.

NOTE: To determine which J-Web package you are currently using, click **Help > About**. The About window appears. If you are using a Platform package, only the Platform package details are displayed. If you are using an Application package, then the Platform package and Application package details are displayed.

If your current J-Web package is:	Then you can:
Platform package	Upgrade to the Application package.

(Continued)

If your current J-Web package is:	Then you can:
Application package	Update to a latest version of the Application package available on the Juniper Networks server that is compatible with the Junos OS on your switch.

NOTE: If you upgrade Junos OS on your switch, the current J-Web package is replaced with the J-Web Platform package that is associated with the upgraded Junos OS release. You can then install the latest Application package that is associated with the main release of the upgraded Junos OS, over the Platform package.

Release Compatibility

The Application packages of J-Web have their own release cycles (A1, A2, A3, and so on), which are independent of the Junos OS release cycle. An Application package is compatible only with the corresponding major release of Junos OS.

The Table 1 on page 4 illustrates the example of the release compatibility.

Table 1: J-Web Release Compatibility Matrix

Junos OS Release	Associated J-Web Application Package Release
14.1X53-D10	Application package 14.1X53-A1
14.1X53-D35	Application package 14.1X53-A2
15.1R1	Application package 15.1A1
15.1R3	Application package 15.1A2 **NOTE**: Application package 15.1A2 cannot be installed on Junos OS Release 15.1R1. Application package 15.1A3 (if applicable)
16.1R1	16.1A1

Table 1: J-Web Release Compatibility Matrix *(Continued)*

Junos OS Release	Associated J-Web Application Package Release
17.1R1	Application package 17.1A1
17.2R1	Application package 17.2A1
17.3R1	Application package 17.3A1
15.1X53-D57	Application package 15.1X53-A2
17.4R1	Application package 17.4A1
18.1R1	Application package 18.1A1
18.1R2	Application package 18.1A2
18.2R1	Application package 18.2A1
18.3R1	Application package 18.3A1
18.4R1	Application package 18.4A1

Any available later version of the Application package for a Junos OS release supersedes the earlier version. Thus, if Application package version 15.1A2 is available for 15.1R1, it will supersede version 15.1A1. We recommend that you install the latest available version of the Application package.

NOTE: If you are using Junos OS Release 22.4R1, you must upgrade to 22.4R3-S2 or later before you install Application Package 22.4A2.

Software Requirements

To access the J-Web interface, your management device requires the following software:

- Supported browsers—Microsoft Internet Explorer version 9 or 10, Mozilla Firefox, and Google Chrome.

TIP: For best viewing of the J-Web user interface, set the screen resolution to 1440 X 900 pixels.

NOTE:

- The browser and the network must support receiving and processing HTTP 1.1 GZIP compressed data.
- Microsoft ended Internet Explorer support in June 2022. Therefore, starting with Junos OS Release 22.4R1 or later, J-Web user interface is not supported in Internet Explorer.

- Language support—English-version browsers

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
15.1R1	Application package 15.1A2 cannot be installed on Junos OS Release 15.1R1.
14.1X53-D10	For Junos OS Release 14.1X53-D10 and later, the J-Web interface is available in two packages

RELATED DOCUMENTATION

- FAQ: J-Web Application Package on EX Series Switches
- EX Series Switch Software Features Overview
- CLI User Interface Overview

J-Web Interface—Application Package

IN THIS SECTION

- J-Web Application Package—First Look | 7

NOTE: This topic applies only to the J-Web Application package.

With the J-Web Application package, you can:

- Get a high-level, graphical view of the chassis and the status of the switch, such as the system health information, alarms, or system status.
- Configure the switch, and view the configuration history.
- Monitor the switch by viewing information about configuration and hardware on the switch such as events, alarms, security, and routing options.
- Maintain the switch by updating the J-Web interface, upgrading Junos OS, uploading configurations, managing licenses and files, or rebooting the switch.

  NOTE: Juniper Networks devices require a license to activate the feature. Refer to the Licensing Guide for general information about License Management: Licenses for Network Management. To understand more about managing licences through J-Web, see "Managing Licenses for the EX Series Switch (J-Web Procedure)" on page 217.

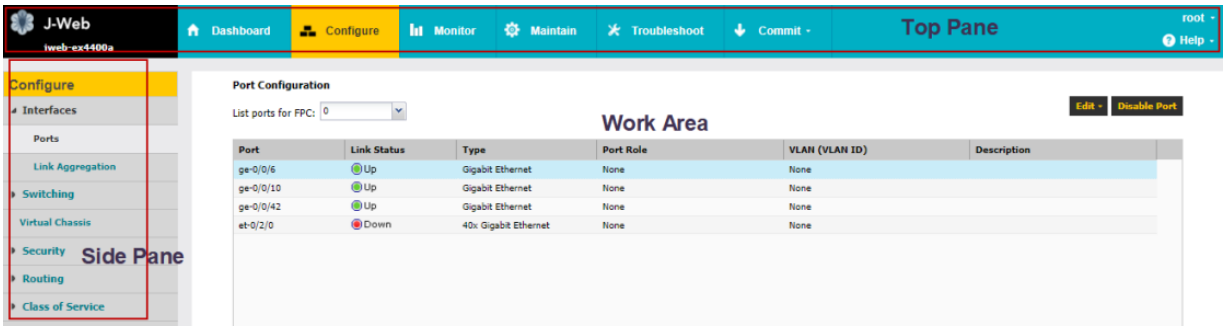
- Troubleshoot network issues by running diagnostic tools. Troubleshoot interface configuration and faults by using ping, traceroute, or packet capture, or by using the CLI terminal.

J-Web Application Package—First Look

Each page of the J-Web interface is divided into panes (see Figure 1 on page 8).

- Top pane—It is located at the top of the page and displays the J-Web logo and hostname, tasks–Dashboard, Configure, Monitor, Maintain, Troubleshoot, Commit, Update Available logo (if available), and username and Help.
- Side pane—It is located on the left side of the page. It displays suboptions of the tasks–Configure, Monitor, Maintain, or Troubleshoot – currently selected in the top pane. Click a suboption to access it in the work area.
- Work area—This is the main work area of the J-Web interface, located below the top pane and to the right of the side pane. It displays various text boxes, selection boxes, buttons and other options corresponding to the suboption that you select in the side pane. It is the location where you monitor, configure, and manage (maintain) the switch.

Figure 1: J-Web First look



The layout of the panes enables you to quickly navigate through the interface. Table 2 on page 8 summarizes the elements of the J-Web interface.

The J-Web interface provides CLI tools that enable you to perform all of the tasks that you can perform from the Junos OS CLI, including a CLI Viewer to view the current configuration, a CLI Editor for viewing and modifying the configuration, and a Point & Click CLI editor that enables you to click through all of the available CLI statements.

Table 2: J-Web Application Package Interface Elements

Element	Description
Top Pane	
J-Web *Hostname*	The J-Web logo and hostname of the switch.

Table 2: J-Web Application Package Interface Elements *(Continued)*

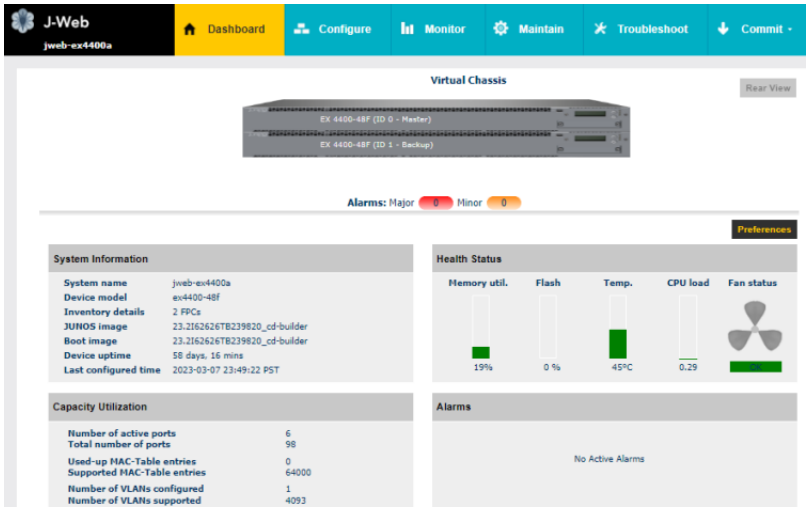
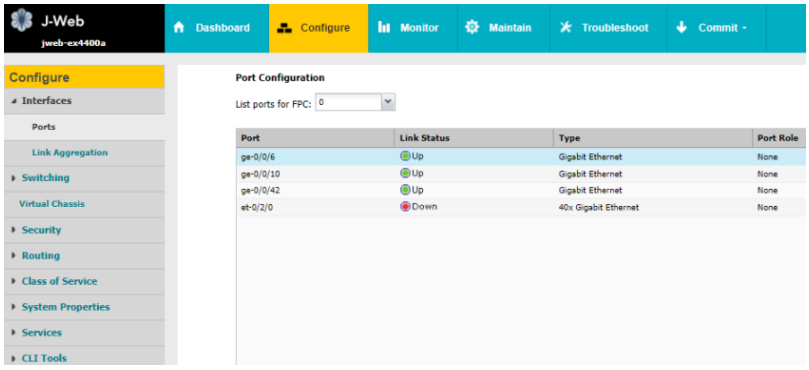
Element	Description
Taskbar—Dashboard	Dashboard—Use the dashboard to view system information. When you log in to the J-Web user interface, the dashboard for the Juniper Networks EX Series Ethernet Switches appears. **Figure 2: Example of the J-Web Dashboard Tab** 
Taskbar—Configure	Configure the switch, and view the configuration history. **Figure 3: Example of the Configure Tab** 

Table 2: J-Web Application Package Interface Elements *(Continued)*

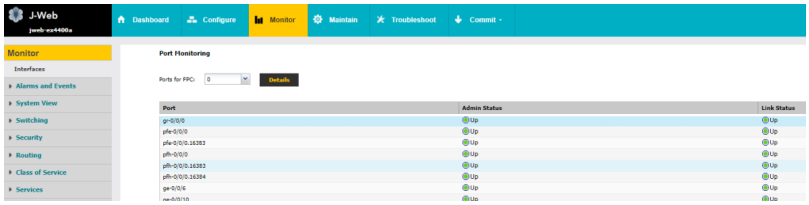
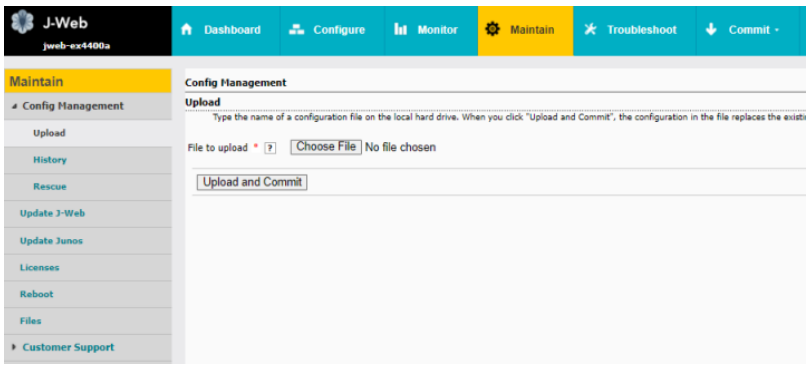
Element	Description
Taskbar—Monitor	View information about configuration and hardware on the switch such as events, alarms, security, and routing options. **Figure 4: Example of the Monitor Tab** 
Taskbar—Maintain	Update the J-Web interface, upgrade Junos OS, upload configurations, manage licenses and files, and reboot the switch. **Figure 5: Example of the Maintain Tab** 

Table 2: J-Web Application Package Interface Elements *(Continued)*

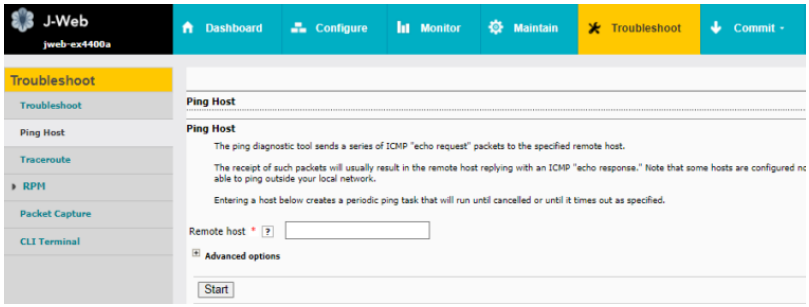
Element	Description
Taskbar—Troubleshoot	Run diagnostic tools to troubleshoot network issues. Troubleshoot interface configuration and faults by using ping, traceroute, or packet capture, or by using the CLI terminal. **Figure 6: Example of the Troubleshoot Tab** 

Table 2: J-Web Application Package Interface Elements *(Continued)*

Element	Description

Commit Options	A set of options using which you can configure committing multiple changes with a single commit.
	• Commit—Commits the candidate configuration of the current user session, along with changes from other user sessions.
	• Compare—Displays the XML log of pending configurations on the device.
	• Discard—Discards the candidate configuration of the current user session, along with changes from other user sessions.
	• Preference—Indicates your choice of committing all configurations changes together or committing each configuration change immediately. The two commit options are:
	  • **Validate configuration changes**—Loads all configuration changes for an accumulated single commit. If there are errors in loading the configuration, the errors are logged. This is the default mode.
	  • **Validate and commit configuration changes**—Sets the system to force an immediate commit on every page after every configuration change.
	  NOTE: There are some pages on which configuration changes must be committed immediately. For such pages, if you configure the commit options for a single commit, the system displays warning notifications that remind you to commit your changes immediately. An example of such a page is the Ports page (Configure > Interfaces > Ports).

Update Available	This icon message appears only if there is a J-Web Application package update available on the Juniper Networks server. Mouse over the icon to know the latest version of J-Web Application package available on the Juniper Networks server. Click on the icon to update the J-Web Application package.
username	The username you used to log in to the switch. The down arrow option displays the **Logout** option. Logout ends your current session and returns you to the login page.

Table 2: J-Web Application Package Interface Elements *(Continued)*

Element	Description
Help	Displays links to help topics and information about the J-Web interface. • Help Contents—Provides context-sensitive help topics. • About—Displays information about the J-Web interface, such as the version number.
Icon legend	(Applies to the Point & Click CLI editor only) Explains icons that appear in the user interface to provide information about configuration statements: • C—Comment. Mouse over the icon to view a comment about the *configuration statement*. • I—Inactive. The configuration statement does not apply for the switch. • M—Modified. The configuration statement has been added or modified. • *—Mandatory. The configuration statement must have a value.
Work Area	
Configuration hierarchy	(Applies to the Junos OS CLI configuration editor only) Displays the hierarchy of committed statements in the switch configuration. • Click **Expand all** to display the entire hierarchy. • Click **Hide all** to display only the statements at the top level. • Click **+** to expand individual items. • Click **-** to hide individual items.

RELATED DOCUMENTATION

- Using the Commit Options to Commit Configuration Changes (J-Web Procedure) | 54
- EX Series Switch Software Features Overview
- Connecting and Configuring an EX Series Switch (J-Web Procedure) | 66
- CLI User Interface Overview

Understanding J-Web User Interface Sessions

You establish a J-Web session with the switch through HTTPS-enabled Web browser. To use HTTPS, you must have installed a certificate on the switch and enabled HTTPS. See *Generating SSL Certificates to Be Used for Secure Web Access (EX Series Switch)*.

When you attempt to log in through the J-Web interface, the switch authenticates your username with the same methods used for Telnet and SSH.

If the switch does not detect any activity through the J-Web interface for 15 minutes, the session times out and is terminated. You must log in again to begin a new session.

To explicitly terminate a J-Web session at any time, click **Logout** in the top pane.

RELATED DOCUMENTATION

J-Web User Interface for EX Series Switches Overview | 2

Configuring Management Access for the EX Series Switch (J-Web Procedure) | 73

Dashboard for EX Series Switches

IN THIS SECTION

- Graphical Chassis Viewer | 15
- System Information Panel | 18
- Health Status Panel | 21
- Capacity Utilization Panel | 25
- Alarms Panel | 26
- File System Usage | 26
- Chassis Viewer | 26

NOTE: This topic applies only to the J-Web Application package.

When you log in to the J-Web user interface, the dashboard for the Juniper Networks EX Series Ethernet Switches appears. Use the dashboard to view system information.

The Update Available window appears if there is a latest update of the J-Web Application package available on the Juniper Networks server. This window is enabled by the auto update feature of J-Web.

NOTE:

- The Update Available window will *not* appear when you log in, if you have not selected the **Check for updates automatically on every login** in the *Update Preference* section in the **Maintain > Update J-Web** side pane. By default, the *Check for update automatically on every login* is selected.
- If you choose *Update Later*, you can update to the latest J-Web Application package by clicking the orange icon next to *Update Available* on the top pane of the J-Web interface or through **Maintain > Update J-Web**.
- Starting in Junos OS Release 22.3R1 which aligns with the J-Web Application package release 22.3A1, J-Web supports EX4400 switches.
- Starting in Junos OS Release 22.4R1 which aligns with the J-Web Application package release 22.4A1, J-Web supports EX4100 and EX4100-F switches.
- Starting in Junos OS Release 23.1R1 which aligns with the J-Web Application package release 23.1A1, J-Web supports EX4400-24X switches.
- Starting in Junos OS Release 23.2R1 which aligns with the J-Web Application package release 23.2A1, J-Web supports EX4400-EM-1C uplink module for EX4400 and EX4400-24X switches.
- Starting in Junos OS Release 24.4R1 which aligns with the J-Web Application package release 24.4A1, J-Web supports EX4100-H-12MP, EX4400-48XP, and EX4400-48MXP switches.

The dashboard comprises a graphical chassis viewer and four panels.

Graphical Chassis Viewer

The Dashboard panel displays a graphical view of the chassis of a switch. In a Virtual Chassis, it displays a graphical view of each member switch.

In a Virtual Chassis, the default values are shown on the Dashboard panel when no chassis image is clicked. The panel displays the value for a switch if you click its image.

NOTE:

- If the member switch is not present, inactive, or not provisioned, you cannot expand the member switch image.
- Starting in J-Web Application Package Release 19.2A1, J-Web supports EX4650 switches.

  NOTE: For EX4650 switches, chassis viewer supports only the standalone view and does not support the Virtual Chassis configuration.

- Starting in Junos OS Release 22.3R1 which aligns with the J-Web Application package release 22.3A1, J-Web supports EX4400 switches. For EX4400 switches, chassis viewer supports both the standalone view and Virtual Chassis configuration.
- Starting in Junos OS Release 22.4R1 which aligns with the J-Web Application package release 22.4A1, J-Web supports EX4100 and EX4100-F switches. For EX4100 and EX4100-F switches, chassis viewer supports both the standalone view and Virtual Chassis configuration.
- Starting in Junos OS Release 23.1R1 which aligns with the J-Web Application package release 23.1A1, J-Web supports EX4400-24X switches. For EX4400-24X switches, chassis viewer supports both the standalone view and Virtual Chassis configuration.
- Starting in Junos OS Release 23.2R1 which aligns with the J-Web Application package release 23.2A1, J-Web supports EX4400-EM-1C uplink module for EX4400 and EX4400-24X switches.
- Starting in Junos OS Release 24.4R1 which aligns with the J-Web Application package release 24.4A1, J-Web supports EX4100-H-12MP, EX4400-48XP, and EX4400-48MXP switches.

Table 3 on page 16 lists the details that are displayed on each member switch.

Table 3: Details of a Virtual Chassis Member Switch

Details	Example
Model number of the member switch	**EX3300**

Table 3: Details of a Virtual Chassis Member Switch *(Continued)*

Details	Example
Assigned ID that applies to the entire Virtual Chassis configuration	**ID 2** **NOTE**: If the member switch is not provisioned, the serial number of the switch is displayed instead of its ID.
Role of the member switch	**Master** Possible roles are: **Master**, **Backup**, or **Linecard**
Status of the member switch	**Prsnt** Possible statuses are: **Prsnt**, **NotPrsnt**, **Inactive**, or **Unprvsnd**

The status of the member switch is displayed on the image of the switch. If the member switch appears dimmed, it means the switch is not present, is inactive, or is not provisioned in the Virtual Chassis. If the member switch does not appear dimmed, it means the switch is present and is active.

Table 4 on page 17 describes the possible status of a member switch.

Table 4: Status of a Member Switch in a Virtual Chassis

If the member switch is	It appears as	It means the member switch
Present	**Prsnt**	Has established physical and logical connections with Virtual Chassis member switches.
Not present	dimmed and **NotPrsnt**	Has been disconnected from the existing Virtual Chassis.
Inactive	dimmed and **Inactive**	Has established physical connections, but is unable to establish logical connections.
Not provisioned	dimmed and **Unprvsnd**	Cannot synchronize with the existing preprovisioned Virtual Chassis.

Click **Rear View** for a graphical view of the rear panel of the switch.

Click **Preferences** to choose which panels must be displayed and set the refresh interval for chassis viewer information. Click **OK** to save your changes and return to the dashboard or click **Cancel** to return to the dashboard without saving changes.

NOTE: You can drag the various panels to different locations in the J-Web window.

System Information Panel

Table 5: System Information

Field	Description
System name	Indicates the local name of the EX Series switch. The local name of the EX Series switches changes when an individual image is clicked. For EX4650, EX4400, EX4100, EX4100-H, and EX4100-F switches: • Indicates the switch's host name. • Displays the switch's specific host name when you click on the individual line card.
Device model	Indicates the model of the EX Series switch. In a Virtual Chassis configuration, to indicate the model of a switch, click the image of that switch. **NOTE**: In a Virtual Chassis setup for an EX6210, EX8208, or EX8216 switch, the Device model field displays details of the primary Routing Engine. To view details of a member, select it. By default, the EX4650, EX4400, EX4100, EX4100-H, and EX4100-F switches show the model of the primary switch. When you click on the image, the model of the switch is displayed.

Table 5: System Information *(Continued)*

Field	Description
Inventory details	Indicates the following: • For EX3200, EX2200, EX2200-C, EX3300, EX4200, EX4300-48MP, EX4500, and EX4550 switches that are not configured as Virtual Chassis, the value displayed in Inventory details field is always 1 FPC. FPC is a legacy term for a slot in a large Juniper Networks chassis; which simply refers to the standalone switch. • For EX2200 and EX2200-C switches configured as a Virtual Chassis, the value displayed in the Inventory details field is 1–4 FPC, with the number corresponding to the number of member switches. • For EX3300 switches configured as a Virtual Chassis, the value displayed in the Inventory details field is 1–6 FPC, with the number corresponding to the number of member switches. **NOTE**: For Junos OS Release 14.1X53-D10 and later, EX3300 switches configured as a Virtual Chassis display the value 1–10 FPC in the Inventory details field. • For EX4200, EX4500, and EX4550 switches configured as a Virtual Chassis, the value displayed in the Inventory details field is 1–10 FPC, with the number corresponding to the number of member switches. • For EX4650, EX4400, EX4100, EX4100-H, and EX4100-F switches, the value displayed in Inventory details field is equal to the number of FPCs. • For EX6210 switches, the values displayed in the Inventory details field are 1–2 CB and 1–9 FPC. CB, or Control Board, refers to the SRE module. FPC refers to line cards and the FPC within the CB.

Table 5: System Information *(Continued)*

Field	Description
	• For an EX8208 switch, the values displayed in Inventory details field are 1–3 CB and 0–8 FPC. CB, or Control Board, refers to SRE and SF modules. FPC refers to line cards. • For EX8216 switches, the values displayed in Inventory details field are 1–2 CB and 0–16 FPC. CB, or Control Board, refers to RE modules and FPC refers to line cards. • For an XRE200 External Routing Engine in an EX8200 Virtual Chassis, the value displayed in Inventory details is 1 XRE. XRE refers to RE modules. For XRE200 External Routing Engines configured as a Virtual Chassis, the values displayed in Inventory details are 1–2 XRE and 0–4 LCC, where LCC refers to the EX8200 line card chassis.
Junos image	Indicates the version of the Junos OS image. In a Virtual Chassis configuration, the Junos OS image of the primary switch is displayed by default. To display the Junos OS image of a specific switch, click the image of that switch. **NOTE**: For EX4650, EX4400, EX4100, EX4100-H, and EX4100-F switches, the Junos OS image of the primary switch is displayed by default. To display the Junos OS image of a specific switch, click the image of that switch.
Boot image	Indicates the version of the boot image that is used. In a Virtual Chassis configuration, the boot image of the primary switch is displayed by default. To display the boot image of a specific switch, click the image of that switch. **NOTE**: For EX4650, EX4400, EX4100, EX4100-H, and EX4100-F switches, the boot image of the primary switch is displayed by default. To display the boot image of a specific switch, click the image of that switch.

Table 5: System Information *(Continued)*

Field	Description
Device uptime	Indicates the time since the last reboot. In a Virtual Chassis configuration, to display the uptime of the specific switch, click the image of that switch. **NOTE**: For EX4650, EX4400, EX4100, EX4100-H, and EX4100-F switches, click the image of the switch to display the uptime.
Last configured time	Indicates the time when the switch was last configured. For EX4400, EX4100, EX4100-H, and EX4100-F switches in Virtual Chassis configuration, indicates the last configured time of the primary by default. To display the last configured time of a specific switch, click the image of that switch.

Health Status Panel

Table 6: Health Status

Field	Description
EX2200, EX2200-C, EX3200, EX3300, EX4200, and EX4300-48MP Switches	
Memory util.	Indicates the memory used in the Routing Engine. In a Virtual Chassis configuration, the memory utilization value of the primary Routing Engine is displayed. **NOTE**: In EX4300-48MP switches, you can use only the built-in QSFP+ ports as VCPs to connect the switch in a Virtual Chassis. You cannot connect the ports on the uplink module in EX4300-48MP switches to Virtual Chassis ports (VCPs).
Flash	Indicates the usage and capacity of internal flash memory and any external USB flash drive.

Table 6: Health Status *(Continued)*

Field	Description
Temp.	Indicates the chassis temperature status. Temperatures are listed in Celsius and the corresponding Fahrenheit values. **NOTE**: The **Temp** field is unavailable for a standalone EX2200-C switch. The **Temp** field is dynamically available for an EX2200 Virtual Chassis switch based on the model of the member clicked.
CPU load	Indicates the average CPU usage over 15 minutes. In a Virtual Chassis configuration, on loading the primary or backup switch, the CPU load for that switch's Routing Engine is displayed by default. To display the CPU load for a specific switch's Routing Engine, click the image of that switch.
Fan status	Indicates the status of the fans in the fan tray. The possible values are **OK**, **Failed**, and **Absent**. In a Virtual Chassis configuration, the fan status of the primary switch is displayed by default. To display the fan status for any switch , click the image of that switch. **NOTE**: The **Fan status** field is unavailable for a standalone EX2200-C switch. The **Fan status** field is dynamically available for an EX2200 Virtual Chassis switch based on the model of the member clicked.
EX4500 and EX4550 Switches	
Memory util.	Indicates the memory used in the Routing Engine. In a Virtual Chassis configuration, the memory utilization value of the primary Routing Engine is displayed.
Flash	Indicates the usage and capacity of internal flash memory and any external USB flash drive.
Temp.	Indicates the chassis temperature status. Temperatures in the dashboard are listed in Celsius and the corresponding Fahrenheit values. **NOTE**: The **Temp** field is unavailable for an EX4500 switch.
CPU load	Indicates the average CPU usage over 15 minutes.
Fan status	Indicates the status of the fans in the fan tray. The possible values are **OK**, **Failed**, and **Absent**. This field also indicates the direction of airflow of the fan tray. The possible values are **Front to back** and **Back to front**.

Table 6: Health Status *(Continued)*

Field	Description
EX4650, EX4400, EX4100, EX4100-H, and EX4100-F Switches	
Fan status	Indicates the status of the fans in the fan tray. The possible values are **OK**, **Failed**, and **Absent**. **NOTE**: The fans are located on the side panel of the chassis. For EX4400, EX4100, and EX4100-F switches in Virtual Chassis, displays the primary member's fan status. **NOTE**: EX4100-F-12T, EX4100-F-12P, and EX4100-H-12MP, are fanless switches that have natural convection cooling.
Temp.	Indicates temperature of the sensor near to Routing Engine. In EX4400, EX4100, EX4100-H, and EX4100-F Virtual Chassis, the primary FPCs Routing Engine temperature is displayed by default. To display the temperature of the FPC Routing Engine of the specific switch, click the image of that switch.
Memory util.	Indicates the memory used in the Routing Engine. To display the Routing Engine memory utilization of the EX4400, EX4100, EX4100-H, and EX4100-F switches, click primary or line card for primary or click backup for backup.
CPU load	Indicates the average CPU usage over 15 minutes. In EX4400, EX4100, EX4100-H, and EX4100-F Virtual Chassis, the primary Routing Engine CPU load is displayed by default. To display the chassis Routing Engine CPU load of the specific switch, click the image of that switch.
EX6210 Switches	
Memory util.	Indicates the memory used in the primary Routing Engine. Click the **backup Routing Engine** to view the memory used in the backup Routing Engine.
CPU load	Indicates the average CPU usage over 15 minutes.
Flash	Indicates the usage and capacity of internal flash memory and any external USB flash drive.

Table 6: Health Status *(Continued)*

Field	Description
Fan status	Indicates the status of the fans in the fan tray. The possible values are **OK**, **Failed**, and **Absent**.
EX8208 Switches	
Memory util.	Indicates the memory used in the external Routing Engine. In an EX8200 Virtual Chassis, the memory utilization value of the XRE200 External Routing Engine in the primary role is displayed. Click the **XRE200 External Routing Engine** in the backup role to view the memory used in the backup external Routing Engine.
CPU load	Indicates the average CPU usage over 15 minutes.
Flash	Indicates the usage and capacity of internal flash memory and any external USB flash drive.
EX8216 Switches	
Memory util.	Indicates the memory used in the external Routing Engine. In an EX8200 Virtual Chassis, the memory utilization value of the XRE200 External Routing Engine in the primary role is displayed. Click the XRE200 External Routing Engine in the backup role to view the memory used in the backup external Routing Engine.
CPU load	Indicates the average CPU usage over 15 minutes.
Flash	Indicates the usage and capacity of internal flash memory and any external USB flash drive.
XRE200 External Routing Engines	
Memory util.	Indicates the memory used in the external Routing Engine. In an EX8200 Virtual Chassis, the memory utilization value of the XRE200 External Routing Engine in the primary role is displayed. Click the backup XRE200 External Routing Engine to view the memory used in backup external Routing Engine.
CPU load	Indicates the average CPU usage over 15 minutes.
Flash	Indicates the usage and capacity of internal flash memory and any external USB flash drive.

Table 6: Health Status *(Continued)*

Field	Description
Fan Status	Indicates the status of the fans in the fan tray. The possible values are **OK**, **Failed**, and **Absent**.

Capacity Utilization Panel

Table 7: Capacity Utilization

Field	Description
Number of active ports	Indicates the number of active ports in the switch. Configured Virtual Chassis ports (VCPs) are considered as active ports.
Total number of ports	Indicates the number of ports in the switch. In EX3300 Virtual Chassis, the total number of ports of all of the switches is displayed. For EX4650 switches, on loading the switch, the consolidated values for all the FPCs are displayed by default. For EX4400, EX4100, and EX4100-F switches, on loading the switch, the consolidated values for all the FPCs are displayed by default and dedicated VCP ports are not considered.
Used-up MAC-Table entries	Indicates the number of MAC table entries.
Supported MAC-Table entries	Indicates the maximum number of MAC table entries permitted. For EX4650 switches, the supported maximum number of MAC table entries are 288000. For EX4400, EX4100, and EX4100-F switches, the supported maximum number of MAC table entries are 64000.

Table 7: Capacity Utilization *(Continued)*

Field	Description
Number of VLANs configured	Indicates the number of VLANs configured. **NOTE**: Only tagged VLANs are counted.
Number of VLANs supported	Indicates the maximum number of VLANs supported. For EX switches, the supported maximum number of VLANs are 4094.

Alarms Panel

Displays information about the last five alarms raised in the system. For example, if there are 5 major alarms, then details of all 5 major alarms are displayed. If there are 4 major alarms and 3 minor alarms, then details of the 4 major alarms and 1 minor alarm are displayed. Major alarms are displayed in red and minor alarms are displayed in yellow.

In an EX8200 Virtual Chassis, the top 5 alarms for the primary external Routing Engine are displayed by default. If you select an EX8200 member switch of the Virtual Chassis, the top 5 alarms for that member switch are displayed.

File System Usage

To display the file system storage details of a switch in the backup or line card role, click the image of that switch.

For EX4650, EX4400, EX4100, and EX4100-F switches, the directory, space used, and the file type details are displayed. By default, primary switch file system storage details are displayed. When you click the image, line card switch file system storage details are displayed.

Chassis Viewer

Click the **Rear View** button to see the back of the chassis image. Click the **Front View** button to see the front of the chassis image. In a Virtual Chassis configuration, the **Rear View** button is disabled if the switch is not selected.

NOTE: For EX4650 switches, chassis viewer supports only the standalone view and does not support Virtual Chassis configuration.

Starting in Junos OS Release 22.3R1 which aligns with the J-Web Application package release 22.3A1, J-Web supports EX4400 switches.

Starting in Junos OS Release 22.4R1 which aligns with the J-Web Application package release 22.4A1, J-Web supports EX4100 and EX4100-F switches.

Starting in Junos OS Release 23.1R1 which aligns with the J-Web Application package release 23.1A1, J-Web supports EX4400-24X switches.

Starting in Junos OS Release 23.2R1 which aligns with the J-Web Application package release 23.2A1, J-Web supports EX4400-EM-1C uplink module for EX4400 and EX4400-24X switches.

Starting in Junos OS Release 24.4R1 which aligns with the J-Web Application package release 24.4A1, J-Web supports EX4100-H-12MP, EX4400-48XP, and EX4400-48MXP switches.

- Table 8 on page 28—Describes the chassis viewer for EX2200 switches.
- Table 9 on page 28—Describes the chassis viewer for EX2200-C switches.
- Table 10 on page 29—Describes the chassis viewer for EX3200, EX3300, and EX4200 switches.
- Table 11 on page 32—Describes the chassis viewer for EX4100 and EX4100-F switches.
- Table 12 on page 34—Describes the chassis viewer for EX4100-H switches.
- Table 13 on page 36—Describes the chassis viewer for EX4400 switches.
- Table 14 on page 39—Describes the chassis viewer for EX4500 switches.
- Table 15 on page 40—Describes the chassis viewer for EX4550 switches.
- Table 16 on page 42—Describes the chassis viewer for EX4650 switches.
- Table 17 on page 43—Describes the chassis viewer for EX6210 switches.
- Table 18 on page 45—Describes the chassis viewer for EX8208 switches.
- Table 19 on page 46—Describes the chassis viewer for EX8216 switches.
- Table 20 on page 48—Describes the chassis viewer for the XRE200 External Routing Engines.

Table 8: Chassis Viewer for EX2200 Switches

Field	Description
Front View	
Interface status	In the image, the following colors denote the interface status: • Green—Interface is up and operational. • Yellow—Interface is up but is nonoperational. • Gray—Interface is down and nonoperational. Mouse over the interface (port) to view more information.
Rear View	
Management (**me0**) port	The management port is used to connect the switch to a management device for out-of-band management.
Console port	The console port is used to connect the switch to a management console or to a console server. (You might do this for initial switch configuration.)
USB port	Indicates the USB port for the switch. **NOTE**: We recommend that you use USB flash drives purchased from Juniper Networks for your EX Series switch.
Fan tray	Mouse over the fan tray icon to display name, status, and description information.
Power supply	Mouse over the power outlet icon to display name, status, and description information.

Table 9: Chassis Viewer for EX2200-C Switches

Field	Description
Front View	

Table 9: Chassis Viewer for EX2200-C Switches *(Continued)*

Field	Description
Interface status	In the image, the following colors denote the interface status: • Green—Interface is up and operational. • Yellow—Interface is up but is nonoperational. • Gray—Interface is down and nonoperational. Mouse over the interface (port) to view more information.
Management (**me0**) port	The management port is used to connect the switch to a management device for out-of-band management.
Console port	The console port is used to connect the switch to a management console or to a console server. (You might do this for initial switch configuration.)
USB port	Indicates the USB port for the switch. **NOTE**: We recommend that you use USB flash drives purchased from Juniper Networks for your EX Series switch.
Rear View	
Power supply	Mouse over the power outlet icon to display name, status, and description information.

Table 10: Chassis Viewer for EX3200, EX3300, and EX4200 Switches

Field	Description
Front View	

Table 10: Chassis Viewer for EX3200, EX3300, and EX4200 Switches *(Continued)*

Field	Description
Interface status	In the image, the following colors denote the interface status: • Green—Interface is up and operational. • Yellow—Interface is up but is nonoperational. • Gray—Interface is down and nonoperational. Mouse over the interface (port) to view more information. For a Virtual Chassis configuration, select the switch to view the interface status. If an SFP+ uplink module is installed in the switch, mouse over the port icon to display whether the module is configured to operate in 1-gigabit mode or in 10-gigabit mode. If the module is configured to operate in 1-gigabit mode, the tool tip information is displayed for all 4 ports. If the module is configured to operate in 10-gigabit mode, the tool tip information is displayed only for 2 ports. On an EX3300 switch with the 4x GE/XE SFP+ module, mouse over the port icon to display whether the module is configured to operate in 1-gigabit mode or 10-gigabit mode. For SFP, SFP+, and XFP ports, the interfaces appear dimmed if no transceiver is inserted. The chassis viewer displays `Transceiver not plugged-in` when you mouse over the port icon.
LCD panel	LCD panel configured for the LEDs on the ports. Mouse over the icon to view the current character display.
Rear View of the EX3200 Switch	
Management (**me0**) port	The management port is used to connect the switch to a management device for out-of-band management.
Console port	The console port is used to connect the switch to a management console or to a console server. (You might do this for initial switch configuration.)

Table 10: Chassis Viewer for EX3200, EX3300, and EX4200 Switches *(Continued)*

Field	Description
USB port	Indicates the USB port for the switch. **NOTE**: We recommend that you use USB flash drives purchased from Juniper Networks for your EX Series switch.
Fan tray	Mouse over the fan tray icon to display name, status, and description information.
Power supply	Mouse over the power supply icon to display name, status, and description information.
Rear View of the EX3300 and EX4200 Switch	
Fan tray	Mouse over the fan tray icon to display name, status, and description information. For a Virtual Chassis, the status of the fans of the selected member switch is displayed.
Virtual Chassis port	Displayed only when EX4200 switches are configured as a Virtual Chassis. The following colors denote the Virtual Chassis port (VCP) status: • Green—VCP is up and operational. • Yellow—VCP is up but is nonoperational. • Gray—VCP is down and nonoperational.
USB port	Indicates the USB port for the switch. **NOTE**: We recommend that you use USB flash drives purchased from Juniper Networks for your EX Series switch.
Management (**me0**) port	The management port is used to connect the switch to a management device for out-of-band management.
Console port	The console port is used to connect the switch to a management console or to a console server. (You might do this for initial switch configuration.)
Power supplies	Mouse over the power supply icons to display name, status, and description information.

Table 11: Chassis Viewer for EX4100 and EX4100-F Switches

Field	Description
Front View	
RJ-45 ports	Mouse over the interface (port) to view more information. EX4100 Switches: • EX4100-24P switch supports 24 RJ-45 ports (10/100/1000BASE-T) that support PoE+. • EX4100-24T switch supports 24 RJ-45 ports (10/100/1000BASE-T). • EX4100-48P switch supports 48 RJ-45 ports (10/100/1000BASE-T) that support PoE+. • EX4100-48T switch supports 48 RJ-45 ports (10/100/1000BASE-T). EX4100-F Switches: • EX4100-F-12T switch supports 12 RJ-45 ports (10/100/1000BASE-T). • EX4100-F-12P switch supports 12 RJ-45 ports (10/100/1000BASE-T) that support support PoE+. • EX4100-F-24P switch supports 24 RJ-45 ports (10/100/1000BASE-T) that support PoE+. • EX4100-F-24T switch supports 24 RJ-45 ports (10/100/1000BASE-T). • EX4100-F-48P switch supports 48 RJ-45 ports (10/100/1000BASE-T) that support PoE+. • EX4100-F-48T switch supports 48 RJ-45 ports (10/100/1000BASE-T).
SFP ports	Mouse over the interface (10 GE SFP+ Uplink ports) to view more information.

Table 11: Chassis Viewer for EX4100 and EX4100-F Switches *(Continued)*

Field	Description
USB type C port	Displays USB Type C console port.
Chassis status LEDs	Displays status LEDs labeled **SYS**, **ALM**, **MST**, and **CLD**.
Port mode LEDs	Displays port mode LEDs labeled **SPD**, **DX**, **EN**, and **PoE**.
Factory Reset/Mode button	Displays the Factory Reset/Mode button, which is used to reset the switches to the factory-default configuration.
Virtual Chassis ports	EX4100 and EX4100-F switches have dedicated Virtual Chassis ports (VCPs) that you can use to interconnect member switches of a Virtual Chassis. You can interconnect a maximum of 10 switches to form a Virtual Chassis.
Rear View	
Management port	The management port (MGMT) is used to connect the switch to a management device for out-of-band management.
Console port	The Console port (RJ-45) labeled as **CON** is used to connect the switch to a management console or to a console server.
USB port	Indicates the USB port for the switch. **NOTE**: We recommend that you use USB flash drives purchased from Juniper Networks for your EX Series switch.

Table 11: Chassis Viewer for EX4100 and EX4100-F Switches *(Continued)*

Field	Description
Power supply	Mouse over the power supply icon to display name, status, and description information. **NOTE**: EX4100-F-12T and EX4100-F-12P switches use external power adapters.
Fan tray	Mouse over the fan tray icon to display fan's status information. **NOTE**: EX4100-F-12T and EX4100-F-12P are fanless switches that have natural convection cooling.

Table 12: Chassis Viewer for EX4100-H Switches

Field	Description
Front View	
RJ-45 ports	Mouse over the interface (port) to view more information. EX4100-H Switches: • EX4100-H-12MP switch supports 12 RJ-45 ports (8 10/100/1000BASE-T RJ-45 ports and 4 100/1000/2500-Base-T RJ-45 ports).
SFP ports	Mouse over the interface (10 GE SFP+ Uplink ports) to view more information. EX4100-H-12MP switch supports four 10GbE SFP+ ports.
USB type C port	Displays USB Type C console port.
Chassis status LEDs	Displays status LEDs labeled **SYS**, **ALM**, **MST**, and **CLD**.

Table 12: Chassis Viewer for EX4100-H Switches *(Continued)*

Field	Description
Port mode LEDs	Displays port mode LEDs labeled **SPD**, **DX**, **EN**, and **PoE**.
Factory Reset/Mode button	Displays the Factory Reset/Mode button, which is used to reset the switches to the factory-default configuration.
Virtual Chassis ports	EX4100-H switches have dedicated Virtual Chassis ports (VCPs) that you can use to interconnect member switches of a Virtual Chassis. You can interconnect a maximum of 10 switches to form a Virtual Chassis.
Management port	The management port (MGMT) is used to connect the switch to a management device for out-of-band management.
Console port	The Console port (RJ-45) labeled as **CON** is used to connect the switch to a management console or to a console server.
USB type A port	Indicates the USB type A port for the switch. **NOTE**: • We recommend that you use USB flash drives purchased from Juniper Networks for your EX Series switch.
Power supply	Mouse over the power supply icon to display name, status, and description information. **NOTE**: • EX4100-H-12MP switch uses external power adapter. • The EX4100-H-12MP switch has two hot swappable power supply units (AC or DC).

Table 13: Chassis Viewer for EX4400 Switches

Field	Description
Front View	
RJ-45 ports	Mouse over the interface (port) to view more information. • EX4400-24T switch supports 24 RJ-45 ports (10/100/1000BASE-T). • EX4400-24P switch supports 24 RJ-45 ports (10/100/1000BASE-T) that support PoE-bt. • EX4400-24MP switch supports 24 RJ-45 ports (100-Mbps/1-Gbps/2.5-Gbps/5-Gbps/10- Gbps) that support PoE-bt. • EX4400-48T switch supports 48 RJ-45 ports (10/100/1000BASE-T). • EX4400-48P and EX4400-48XP switches support 48 RJ-45 ports (10/100/1000BASE-T) that support PoE-bt. • EX4400-48MP switch supports 36 RJ-45 ports (100-Mbps/1-Gbps/2.5-Gbps) and 12 RJ-45 ports (100-Mbps/1-Gbps/2.5-Gbps/5-Gbps/10- Gbps) that support PoE-bt. • EX4400-48MXP switch supports 36 RJ-45 ports (1-Gbps/2.5-Gbps) and 12 RJ-45 ports (1-Gbps/2.5-Gbps/5-Gbps/10- Gbps) that support PoE-bt.

Table 13: Chassis Viewer for EX4400 Switches *(Continued)*

Field	Description
SFP ports	Mouse over the interface (port) to view more information. EX4400-48F switch supports 36 small form-factor pluggable (SFP) ports and 12 small form-factor pluggable plus (SFP+) ports. EX4400-24X switch supports 24 1GbE/10GbE SFP/SFP+ ports and two 100GbE QSFP28 ports. **NOTE**: SFP port is not available for EX4400-48XP and EX4400-48-MXP switches.
USB port	Displays USB Type C console port.
Chassis status LEDs	Displays status LEDs labeled **SYS**, **ALM**, **MST**, and **CLD**.
Port mode LEDs	Displays port mode LEDs labeled **SPD**, **DX**, and **EN**.
Factory Reset/Mode button	Displays the Factory Reset/Mode button, which is used to reset the switches to the factory-default configuration.
Extension module slot	Displays a slot for installing an optional extension module. Extension modules are hot-insertable and hot-removable field replaceable units (FRUs). The 1x100GbE QSFP28 extension module (EX4400-EM-1C) supports Media Access Control Security (MACsec) with AES-256 encryption. You can install one 40GbE QSFP+ transceiver or one 100GbE QSFP28 transceiver in the extension module.
Rear View	

Table 13: Chassis Viewer for EX4400 Switches *(Continued)*

Field	Description
Management port	The management port (me0) is used to connect the switch to a management device for out-of-band management. **NOTE**: For EX4400-24X, the MGMT port is available on the front panel.
Virtual Chassis ports	The QSFP28 ports are configured as Virtual Chassis ports (VCPs) by default. You can configure them as network ports and operate them as 100 GbE network ports by using QSFP28 transceivers.
Console port	The Console port (RJ-45) labeled as **CON** is used to connect the switch to a management console or to a console server. **NOTE**: For EX4400-24X, the CON port is available on the front panel.
USB port	Indicates the USB port for the switch. **NOTE**: • We recommend that you use USB flash drives purchased from Juniper Networks for your EX Series switch. • For EX4400-24X, the USB port is available only on the front panel.
Mini USB port	Indicates the mini USB port for the switch. **NOTE**: Mini USB port is not available for EX4400-24X, EX4400-48XP, and EX4400-48MXP switches.

Table 13: Chassis Viewer for EX4400 Switches *(Continued)*

Field	Description
Power supply	Mouse over the power supply icon to display name, status, and description information. **NOTE**: The EX4400 switch has two hot swappable power supply units (AC or DC).
Fan tray	Mouse over the fan tray icon to display status of the fans and airflow direction information.

Table 14: Chassis Viewer for EX4500 Switches

Field	Description
Front View	
Interface status	In the image, the colors listed below denote the interface status: • Green—Interface is up and operational. • Yellow—Interface is up but is nonoperational. • Gray—Interface is down and nonoperational. Mouse over the interface (port) to view more information. For a Virtual Chassis configuration, select the switch to view the interface status. If an SFP+ uplink module is installed in the switch, mouse over the interface (ports) on the module for more information. For SFP and SFP+ ports, the interfaces appear dimmed if no transceiver is inserted. The chassis viewer displays `Transceiver not plugged-in` when you mouse over the port icon.
LCD panel	LCD panel configured for the LEDs on the ports. Mouse over the icon to view the current character display.
Console port	The console port is used to connect the switch to a management console or to a console server.

Table 14: Chassis Viewer for EX4500 Switches *(Continued)*

Field	Description
Management (**me0**) port	The management port is used to connect the switch to a management device for out-of-band management. Use this port for initial switch configuration.
USB port	Indicates the USB port for the switch. **NOTE**: We recommend that you use USB flash drives purchased from Juniper Networks for your EX Series switch.
Rear View of the EX4500 Switch	
Fan tray	Mouse over the fan tray icon to display status of the fans and airflow direction information. For a Virtual Chassis, the status of the fans of the selected member switch is displayed.
Virtual Chassis port	Displayed only when switches are configured as a Virtual Chassis. The colors listed below denote the Virtual Chassis port (VCP) status: • Green—VCP is up and operational. • Yellow—VCP is up but is nonoperational. • Gray—VCP is down and nonoperational.
Power supplies	Mouse over the power supply icons to display name, status, and description information.
Intraconnect module	Mouse over the module to display details of the intraconnect module. The intraconnect module helps the switch achieve line rate on all its ports.
Virtual Chassis module	Mouse over to display details of the switches in the Virtual Chassis configuration.

Table 15: Chassis Viewer for EX4550 Switches

Field	Description
Front View	

Table 15: Chassis Viewer for EX4550 Switches *(Continued)*

Field	Description
Interface status	In the image, the colors listed below denote the interface status: • Green—Interface is up and operational. • Yellow—Interface is up but is nonoperational. • Gray—Interface is down and nonoperational. Mouse over the interface (port) to view more information. For a Virtual Chassis configuration, select the switch to view the interface status. If an expansion module or a Virtual Chassis module is installed in the switch, mouse over the interface (ports) on the module for more information. On an EX4550-32F switch, for SFP and SFP+ ports, the interfaces appear dimmed if no transceiver is inserted. The chassis viewer displays `Transceiver (1G/10G) not plugged in` when you mouse over the port icon.
LCD panel	LCD panel configured for the LEDs on the ports. Mouse over the icon to view the current character display.
Console port	The console port is used to connect the switch to a management console or to a console server.
Mini Console port	The mini console port is used to connect the switch to the management console.
Management (**me0**) port	The management port is used to connect the switch to a management device for out-of-band management. Use this port for initial switch configuration.
PIC1 slot	You can insert an uplink module or a Virtual Chassis module in the PIC1 slot. Mouse over to display the details of the module inserted (uplink or Virtual Chassis).
USB port	Indicates the USB port for the switch. **NOTE**: We recommend that you use USB flash drives purchased from Juniper Networks for your EX Series switch.
Rear View of the EX4550 Switch	

Table 15: Chassis Viewer for EX4550 Switches *(Continued)*

Field	Description
Fan tray	Mouse over the fan tray icon to display the status of the fans and airflow direction information. For a Virtual Chassis, the status of the fans of the selected member switch is displayed.
Virtual Chassis port	Displayed only when switches are configured as a Virtual Chassis. In the image, the colors listed below denote the Virtual Chassis port (VCP) status: • Green—VCP is up and operational. • Yellow—VCP is up but is nonoperational. • Gray—VCP is down and nonoperational.
Power supplies	Mouse over the power supply icons to display name, status, and description information.
PIC2 slot	You can insert an uplink module or a Virtual Chassis module into the PIC2 slot. Mouse over to display the details of the module inserted (uplink or Virtual Chassis).

Table 16: Chassis Viewer for EX4650 Switches

Field	Description
Front View	
SFP28 and QSFP28 Ports	Displays 48 small form-factor pluggable (SFP28) ports and eight 100-Gbps quad small form-factor pluggable (QSFP28) ports. Mouse over the interface (port) to view more information.
Rear View	
Management port	The management port (em0) is used to connect the switch to a management device for out-of-band management.
Virtual Chassis ports	Not supported.

Table 16: Chassis Viewer for EX4650 Switches *(Continued)*

Field	Description
Console port	The Console port (RJ-45) is used to connect the switch to a management console or to a console server.
USB port	Indicates the USB port for the switch. **NOTE**: We recommend that you use USB flash drives purchased from Juniper Networks for your EX Series switch.
Fan Tray	Mouse over the fan tray icons to display name, status, and description information.
Power supply	Mouse over the power supply icon to display name, status, and description information.

Table 17: Chassis Viewer for EX6210 Switches

Field	Description
Front View	
Temperature	Mouse over the temperature icon to display the temperature of the CB or line card.

Table 17: Chassis Viewer for EX6210 Switches *(Continued)*

Field	Description
Interface status	Select the CB or line card. In the image, the colors listed below denote the interface status: • Green—Interface is up and operational. • Yellow—Interface is up but is nonoperational. • Gray—Interface is down and nonoperational. Mouse over the interface (port) to view more information. You can view status for the following ports on the SRE module: • USB port—Indicates the USB port for the switch. **NOTE**: We recommend that you use USB flash drives purchased from Juniper Networks for your EX Series switch. • Management (**me0**) port—The management port is used to connect the switch to a management device for out-of-band management. There are 2 management ports: fiber and copper. The same status is displayed for both the **me0** ports. • Console port—The console port is used to connect the switch to a management console or to a console server. (You might do this for initial switch configuration.) CBs support 4 SFP+ uplink ports. Mouse over the interface on the CB for more information. For SFP and SFP+ ports, the interfaces appear dimmed if no transceiver is inserted. The chassis viewer displays `Transceiver not plugged-in` when you mouse over the port icon.
Power supplies	Mouse over the power supply icons to display name, status, and description information.
LCD panel	LCD panel configured for the LEDs on the ports. Mouse over the icon to view the current character display of the primary Routing Engine. The EX6210 switch has 2 LCD panels, one for each Routing Engine. The backup Routing Engine LCD displays **Backup**.
Rear View of the EX6210 Switch	
Fan tray	Mouse over the fan tray icon to display information regarding the cooling fans.

Table 18: Chassis Viewer for EX8208 Switches

Field	Description
Front View	
Interface status	In the image, click any line card, SRE module, or SF module to view the front view of the selected component. In the image, the colors listed below denote the interface status: • Green—Interface is up and operational. • Yellow—Interface is up but is nonoperational. • Gray—Interface is down and nonoperational. Mouse over the interface (port) to view more information. You can view status for the following ports on the SRE module: • USB port—Indicates the USB port for the switch. **NOTE**: We recommend that you use USB flash drives purchased from Juniper Networks for your EX Series switch. • Auxiliary port—This port is unavailable. • Management (**me0**) port—The management port is used to connect the switch to a management device for out-of-band management. • Console port—The console port is used to connect the switch to a management console or to a console server. (You might do this for initial switch configuration.) Because the SF module has no ports, no status information is displayed.
Slot numbers	Slots on the switch are labeled, from the top of the switch down: • 0–3 (line cards) • SRE0, SF, SRE1 (SRE and SF modules) • 4–7 (line cards)
Temperature	The active slots contain a gray temperature icon. Mouse over the icon to display temperature information for the slot.

Table 18: Chassis Viewer for EX8208 Switches *(Continued)*

Field	Description
Fan status	Mouse over the fan tray icon to display name, status, and description information.
Power supplies	Mouse over the power supply icons to display name, status, and description information.
LCD panel	LCD panel configured for the LEDs on the ports. Mouse over the icon to view the current character display.
Rear View	The EX8208 switch does not have any components on the rear of the chassis.

Table 19: Chassis Viewer for EX8216 Switches

Field	Description
Front View	

Table 19: Chassis Viewer for EX8216 Switches *(Continued)*

Field	Description
Interface status	In the image, click any line card or RE module to display the front view of the selected component. In the image, the colors listed below denote the interface status: • Green—Interface is up and operational. • Yellow—Interface is up but is nonoperational. • Gray—Interface is down and nonoperational. Mouse over the interface (port) to view more information. You can view status for the following ports on the RE module: • USB port—Indicates the USB port for the switch. **NOTE**: We recommend that you use USB flash drives purchased from Juniper Networks for your EX Series switch. • Auxiliary port—This port is unavailable. • Management (**me0**) port—The management port is used to connect the switch to a management device for out-of-band management. • Console port—The console port is used to connect the switch to a management console or to a console server. (You might do this for initial switch configuration.)
Slot numbers	Slots on the switch are labeled, from the top of the switch down: • RE0 (RE module) • RE1 (RE module) • 0–15 (line cards)
Temperature	The active slots contain a gray temperature icon. Mouse over the icon to display temperature information for the slot.
Fan status	Mouse over the fan tray icon to display consolidated information about the fans.
Power supplies	Mouse over the power supply icons to display name, status, and description information.

Table 19: Chassis Viewer for EX8216 Switches *(Continued)*

Field	Description
LCD panel	LCD panel configured for the LEDs on the ports. Mouse over the icon to view the current character display.
Rear View	
SF modules	Mouse over the SF module icons in their respective slots to display information. Slots are numbered SF7–SF0, from left to right.

Table 20: Chassis Viewer for XRE200 External Routing Engines

Field	Description
Front View	
Interface status	In the image, the colors listed below denote the interface status: • Green—Interface is up and operational. • Yellow—Interface is up but is nonoperational. • Gray—Interface is down and nonoperational. Mouse over the interface (port) to view more information. For a Virtual Chassis configuration, select the switch to view the interface status.
Console port	The console port is used to connect the switch to a management console or to a console server.
Management (**me0**) port	The management port is used to connect the switch to a management device for out-of-band management. Use this port for initial switch configuration.

Table 20: Chassis Viewer for XRE200 External Routing Engines *(Continued)*

Field	Description
Virtual Chassis port	In the image, the colors listed below denote the Virtual Chassis port (VCP) status: • Green—VCP is up and operational. • Yellow—VCP is up but is nonoperational. • Gray—VCP is down and nonoperational. Mouse over the interface (port) to view more information.
LCD panel	LCD panel configured for the LEDs on the ports. Mouse over the icon to view the current character display.
Temperature	The active slots contain a gray temperature icon. Mouse over the icon to display temperature information for the slot.
USB port	Indicates the USB port for the switch. **NOTE**: We recommend that you use USB flash drives purchased from Juniper Networks for your EX Series switch.
PIC1 slot	You can install a Virtual Chassis module in the PIC1 slot. Mouse over the Virtual Chassis ports to display the port status details.
PIC2 slot	You can install a Virtual Chassis module in the PIC2 slot. Mouse over the Virtual Chassis ports to display the port status details.
Rear View of the XRE200 External Routing Engine	
Fan modules	Mouse over the fan modules to display status of the fans and airflow direction information. For a Virtual Chassis, the status of the fans of the selected member switch is displayed.
Power supplies	Mouse over the power supply icons to display name, status, and description information.

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
22.4A1	Starting in Junos OS Release 22.4R1 which aligns with the J-Web Application package release 22.4A1, J-Web supports EX4100 and EX4100-F switches.

RELATED DOCUMENTATION

- J-Web User Interface for EX Series Switches Overview
- EX2200 Switches Hardware Overview
- *EX2300 Switches Hardware Overview*
- EX3200 Switches Hardware Overview
- EX3300 Switches Hardware Overview
- *EX4200 Switches Hardware Overview*
- EX4500 Switches Hardware Overview
- EX6210 Switch Hardware Overview
- EX8208 Switch Hardware Overview
- EX8216 Switch Hardware Overview
- *Check Active Alarms with the J-Web Interface*
- XRE200 External Routing Engine Hardware Guide

Understanding J-Web Configuration Tools

NOTE: This topic applies only to the J-Web Application package.

The J-Web graphical user interface (GUI) enables you to monitor, configure, troubleshoot, and manage the switching platform by means of a Web browser with HTTP over Secure Sockets Layer (HTTPS) enabled. The J-Web interface provides access to all the configuration statements supported by the switch.

The J-Web interface provides three methods for configuring the switch:

- Configure menu
- Point & Click CLI Editor

- CLI Editor

Table 21 on page 51 gives a comparison of the three methods of configuration.

Table 21: Switching Platform Configuration Interfaces

Tool	Description	Function	Use
Configure menu	Web browser pages for setting up the switch quickly and easily without configuring each statement individually. For example, use the *Virtual Chassis* Configuration page to configure the Virtual Chassis parameters on the switch.	Configure basic switch platform services: • Interfaces • Switching • Virtual Chassis • Security • Services • System Properties • Routing	Use for basic configuration.
Point & Click CLI Editor	Web browser pages divided into panes in which you can do any of the following: • Expand the entire configuration hierarchy and click a *configuration statement* to view or edit. The work area displays all the options for the statement, with a text box for each option. • Paste a complete configuration hierarchy into a scrollable text box, or edit individual lines. • Upload or download a complete configuration. • Roll back to a previous configuration. • Create or delete a rescue configuration.	Configure all switching platform services: • System parameters • User Accounting and Access • Interfaces • VLAN properties • Virtual Chassis properties • Secure Access • Services • Routing protocols	Use for complete configuration if you are not familiar with the Junos OS CLI or prefer a graphical interface.

Table 21: Switching Platform Configuration Interfaces *(Continued)*

Tool	Description	Function	Use
CLI Editor	Interface in which you do any of the following: • Type commands on a line and press **Enter** to create a hierarchy of configuration statements. • Create an ASCII text file that contains the statement hierarchy. • Upload a complete configuration, or roll back to a previous configuration. • Create or delete a rescue configuration.	Configure all switching platform services: • System parameters • User Accounting and Access • Interfaces • VLAN properties • Virtual Chassis properties • Secure Access • Services • Routing protocols	Use for complete configuration if you know the Junos OS CLI or prefer a command interface.

RELATED DOCUMENTATION

- Understanding J-Web User Interface Sessions | **14**
- J-Web User Interface for EX Series Switches Overview | **2**
- *Connecting and Configuring an EX Series Switch (J-Web Procedure)*
- Configuration Files Terms

Understand Alarm Types and Severity Levels on EX Series Switches

NOTE: This topic applies only to the J-Web Application package.

Alarms alert you to conditions that might prevent normal operation of the switch. Before monitoring alarms on a Juniper Networks EX Series Ethernet switch, become familiar with the terms defined in Table 22 on page 53.

Table 22: Alarm Terms

Term	Definition
alarm	Signal alerting you to conditions that might prevent normal operation. On a switch, the alarm signal is the **ALM** LED lit on the front of the chassis.
alarm condition	Failure event that triggers an alarm.
alarm severity	Seriousness of the alarm. If the Alarm (**ALM**) LED is red, this indicates a major alarm. If the Alarm LED is yellow or amber, this indicates a minor alarm. If the Alarm LED is unlit, there is no alarm or the switch is halted.
chassis alarm	Preset alarm triggered by a physical condition on the switch such as a power supply failure, excessive component temperature, or media failure.
system alarm	Preset alarm triggered by a missing rescue configuration or failure to install a license for a licensed software feature. **NOTE**: On EX6200 switches, a system alarm can be triggered by an internal link error.

Alarm Types

The switch supports these alarms:

- Chassis alarms indicate a failure on the switch or one of its components. Chassis alarms are preset and cannot be modified.
- System alarms indicate a missing rescue configuration. System alarms are preset and cannot be modified, although you can configure them to appear automatically in the J-Web interface display or the CLI display.

Alarm Severity Levels

Alarms on switches have two severity levels:

- Major (red)—Indicates a critical situation on the switch that has resulted from one of the following conditions. A red alarm condition requires immediate action.
  - One or more hardware components have failed.
  - One or more hardware components have exceeded temperature thresholds.
  - An alarm condition configured on an interface has triggered a critical warning.

- Minor (yellow or amber)—Indicates a noncritical condition on the switch that, if left unchecked, might cause an interruption in service or degradation in performance. A yellow or amber alarm condition requires monitoring or maintenance.

  A missing rescue configuration generates a yellow or amber system alarm.

RELATED DOCUMENTATION

Dashboard for EX Series Switches

Using the Commit Options to Commit Configuration Changes (J-Web Procedure)

You can use the single-commit feature to commit all outstanding configuration changes in the J-Web interface on EX Series switches simultaneously. This helps in reducing the time J-Web takes for committing configurations because when changes are committed at every step, rollback configurations pile up.

For example, suppose you want to delete a firewall filter and add a new one. With immediate commits, you would need to commit your changes twice for this action. Using single commit, you can decrease the number of commits to one, thus saving time for working on other configurations.

When you edit a configuration, you work on a copy of the current configuration, which is your candidate configuration. The changes you make to the candidate configuration are visible through the user interface immediately, allowing other users to edit those configurations, but they do not take effect on the switch until you commit the changes. When you commit the configuration, the candidate file is checked for proper syntax, activated, and marked as the current, operational software configuration file. If multiple users are editing the configuration when you commit the candidate configuration, changes made by all users take effect.

You can configure the commit options to either commit all configuration changes together or commit each configuration change immediately using the J-Web Commit Preference page.

NOTE: There are some pages on which configuration changes must be committed immediately. For such pages, if you configure the commit options for a single commit, the system displays warning notifications that remind you to commit your changes immediately. An example of such a page is the Interface Page (**Configure** > **Interface**).

To configure the commit options on an EX Series switch using the J-Web interface:

1. Select **Commit Options**.

NOTE: All action links except **Preference** are disabled unless you edit, add, or delete a configuration.

2. Choose an action. See Table 23 on page 55 for details on the actions.
3. Configure the commit options by selecting **Preference**. See Table 24 on page 56 for details on preference options.

Table 23: Commit Options

Menu Item	Function	Your Action
Commit	Commits the candidate configuration of the current user session, along with changes from other user sessions.	1. Select **Commit Options** > **Commit**. Changes are committed after the system validates your configuration. A window displays that the configuration was successfully committed or that the commit failed. 2. Click **OK**. Click **Details** to view the commit log.
Compare	Displays the XML log of pending uncommitted configurations on the device.	1. Select **Commit Options** > **Compare**. The XML log of pending configurations on the devices are displayed similar to the CLI interface, in a “human-readable” form. 2. Click **Close**.
Discard	Discards the candidate configuration of your current session, along with changes from other user sessions.	1. Select **Commit Options** > **Discard**. 2. Click **OK** to confirm the discard action. Your changes are discarded after the system validates your configuration.
Preference	Indicates your choice of committing all global configurations together or committing each configuration change immediately.	1. Select **Commit Options** > **Preference**. The Commit Preference page is displayed. 2. Configure the commit options by selecting your preference. See Table 24 on page 56 for details on preference options.

Table 24: Commit Preference Options

Option	Function
Validate and commit configuration changes	Sets the system to validate and force an immediate commit on every screen after every configuration change.
Validate configuration changes	Loads all the configuration changes for an accumulated single commit. If there are errors in loading the configuration, the errors are logged. This is the default mode. Once you select this option, you need to select **Commit Options** > **Commit** to commit your changes.

RELATED DOCUMENTATION

J-Web User Interface for EX Series Switches Overview | 2

EX Series Switch Software Features Overview

PART 2

Configuration

Starting J-Web | 58

J-Web Configuration Tools | 59

System Basics Configuration | 66

Class of Service Configuration | 79

Security and Management Configuration | 97

Routing Policies and Packet Filtering Configuration | 108

Ethernet Switching Configuration | 123

Interfaces | 139

Configuring Services | 158

Configuring Layer 3 Protocols | 168

Configuring Real-Time Performance Monitoring | 191

Software Installation and Upgrades | 202

Configuration, Files, Users, Licenses, and Product Registration | 206

Virtual Chassis Configuration | 221

CHAPTER 2

Starting J-Web

IN THIS CHAPTER

- Starting the J-Web Interface | 58

Starting the J-Web Interface

You can use the J-Web interface to configure and manage the EX Series switch.

To start the J-Web interface:

1. Launch your HTTPS-enabled Web browser.

   To use HTTPS, you must have installed a certificate on the switch and enabled HTTPS.
2. After **https://** in your Web browser, type the hostname or IP address of the switch and press **Enter**.

   The J-Web login page appears.
3. On the login page, type your username and password, and click **Login**.

   NOTE: The default username is root with no password. You must change this during initial configuration or the system does not accept the configuration.

   If you are using an Application package of J-Web, the Dashboard information page appears; if you are using a Platform package of J-Web, the Configure Options page appears.

To explicitly terminate a J-Web session at any time, click **Logout** in the top pane.

RELATED DOCUMENTATION

J-Web User Interface for EX Series Switches Overview | 2

Dashboard for EX Series Switches

CHAPTER 3

J-Web Configuration Tools

IN THIS CHAPTER

- Using the Point and Click CLI Tool in the J-Web Interface to Edit Configuration Text | 59
- Using the CLI Editor in the J-Web Interface to Edit Configuration Text | 61
- Using the J-Web CLI Terminal | 62
- Using the CLI Viewer in the J-Web Interface to View Configuration Text | 64

Using the Point and Click CLI Tool in the J-Web Interface to Edit Configuration Text

NOTE: This topic applies only to the J-Web Application package.

To edit the configuration on a series of pages of clickable options that steps you through the hierarchy, select **Configure** > **CLI Tools** > **Point&Click CLI**. The side pane displays the top level of the configured hierarchy, and the work area displays configured hierarchy options and the Icon Legend.

To expand or hide the hierarchy of all the statements in the side pane, click **Expand all** or **Hide all**. To expand or hide an individual statement in the hierarchy, click the expand (+) or collapse (–) icon to the left of the statement.

TIP: Only those statements included in the committed configuration are displayed in the hierarchy.

The configuration information in the work area consists of configuration options that correspond to configuration statements. Configuration options that contain subordinate statements are identified by the term *Nested*.

To include, edit, or delete statements in the candidate configuration, click one of the links described in Table 25 on page 60. Then specify configuration information by typing in a field, selecting a value from a list, or selecting a check box (toggle).

Table 25: J-Web Edit Point & Click Configuration Links

Link	Function
Add new entry	Displays fields and lists for a statement identifier, allowing you to add a new identifier to a statement.
Configure	Displays information for a configuration option that has not been configured, allowing you to include a statement.
Delete	Deletes the corresponding statement or identifier from the configuration. All subordinate statements and identifiers contained within a deleted statement are also discarded.
Edit	Displays information for a configuration option that has already been configured, allowing you to edit a statement.
Identifier	Displays fields and lists for an existing statement identifier, allowing you to edit the identifier.

As you navigate through the configuration, the hierarchy level is displayed at the top of the work area. You can click a statement or identifier in the hierarchy to display the corresponding configuration options in the work area.

The work area includes icons that display information about statements and identifiers when you place your cursor over them. Table 26 on page 60 describes these icons.

Table 26: J-Web Edit Point & Click Configuration Icons

Icon	Function
C	Displays a comment about a statement.
I	Indicates that a statement is inactive.
M	Indicates that a statement has been added or modified but has not been committed.
*	Indicates that the statement or identifier is required in the configuration.
?	Provides online help information.

After typing or selecting your configuration edits, click a button in the work area (described in Table 27 on page 61) to apply your changes or cancel them, refresh the display, or discard parts of the candidate configuration. An updated configuration does not take effect until you commit it.

Table 27: J-Web Edit Point & Click Configuration Buttons

Button	Function
Refresh	Updates the display with any changes to the configuration made by other users.
Commit	Verifies edits and applies them to the current configuration file running on the switch.
Discard	Removes edits applied to or deletes existing statements or identifiers from the candidate configuration.

RELATED DOCUMENTATION

- CLI User Interface Overview
- Understanding J-Web Configuration Tools | 50

Using the CLI Editor in the J-Web Interface to Edit Configuration Text

NOTE: This topic applies only to the J-Web Application package.

Use the CLI Editor to edit configuration if you know the Junos OS CLI or prefer a command interface.

To edit the entire configuration in text format:

CAUTION: We recommend that you use this method to edit and commit the configuration only if you have experience editing configurations through the CLI.

1. Select **Configure** > **CLI Tools** > **CLI Editor**. The work area displays the configuration in a text editor.
2. Navigate to the hierarchy level you want to edit.

   You can edit the candidate configuration using standard text editor operations—insert lines (by using the Enter key), delete lines, and modify, copy, and paste text.

3. Click **Commit** to load and commit the configuration.

   The switching platform checks the configuration for the correct syntax before committing it.

RELATED DOCUMENTATION

- CLI User Interface Overview
- Understanding J-Web Configuration Tools | 50

Using the J-Web CLI Terminal

IN THIS SECTION

- Configuring the Web Browser | 62
- Setting Domain Name, Hostname, and Name Server | 63
- Enabling SSH on your system | 63
- Sample Configuration on an EX Series Switch | 63

NOTE: This topic applies only to the J-Web Application package.

The J-Web CLI terminal provides access to the Junos OS command-line interface (CLI) through the J-Web interface. The functionality and behavior of the CLI available through the CLI Terminal page is the same as that of the Junos OS CLI available through the switch console. The CLI terminal supports all CLI commands and other features such as CLI help and autocompletion. Using the CLI terminal page, you can fully configure, monitor, and manage the switch.

This topic covers:

Configuring the Web Browser

Configure your Web browser as follows:

- Install Java Runtime Environment (JRE) version 1.4 or later on your system. JRE is a software package that must be installed on the client system to run Java applications. You can download the latest version of JRE from the Java software website http://www.java.com/. Installing JRE installs Java plug-ins, which once installed, load automatically and transparently to render Java applets.

> **NOTE:** By default Mozilla Firefox has blocked JRE versions earlier than 1.6.0_31 and 1.7.0 through 1.7.0_2. However, Mozilla Firefox users can still click **Add-ons > Plugin** to enable Java.

- Set your browser to support and enable Java applets. To know more about checking the status of java applets in your browser see http://java.com/en/download/help/enable_browser.xml.

Setting Domain Name, Hostname, and Name Server

Configure the domain name and hostname of the switch on your system. Ensure that the DNS server setting is correct. DNS name resolution must happen properly. Ensure that there is connectivity between the client and the management device.

You can set the domain name, hostname, and the DNS name server either through the J-Web interface or the CLI:

- To set through the J-Web interface:

  See "Configuring System Identity for an EX Series Switch (J-Web Procedure)" on page 71 for more information.

- To set through the CLI:

  ```
  set system domain-name domain-name
  ```

  ```
  set system host-name host-name
  ```

  ```
  set system name-server dns-ip-address
  ```

Enabling SSH on your system

SSH provides a secure method of logging in to the switch, and encrypting traffic so that it is not intercepted. If SSH is not enabled on the system, the CLI terminal page displays the error message:

To enable SSH on your system, do the following:

```
set system services ssh
```

Sample Configuration on an EX Series Switch

1. Type the `configure` command to enter the configuration mode:

   ```
   user@switch> configure
   ```

2. Log in as host:

   ```
   user@switch# set system host-name host
   ```

3. Configure the encrypted password; for example:

```
user@switch# set system root-authentication encrypted-password "$1$mr3D4eVf$mc7y54e6hk4JuIpwWPao6."
```

4. Map the hostname to the IP address:

```
user@switch# set system static-host-mapping host inet 10.9.221.31
```

5. Configure the IP address for the DNS server:

```
user@switch# set system name-server 10.0.220.1
```

6. Enable the system services by using:

```
set system services:user@switch# set system services ssh
```

7. Select **Troubleshoot > CLI Terminal**. The password window is displayed.
8. Enter the password, and click **OK**. The CLI Terminal window appears on the J-Web page.

NOTE: If you exit from the CLI terminal, the connection is lost. Click **CLI Terminal** if you want to connect again.

RELATED DOCUMENTATION

CLI User Interface Overview

Understanding J-Web Configuration Tools | 50

Using the CLI Viewer in the J-Web Interface to View Configuration Text

NOTE: This topic applies only to the J-Web Application package.

To view the entire configuration file contents in text format, select **Configure** > **CLI Tools** > **CLI Viewer**. The main pane displays the configuration in text format.

Each level in the hierarchy is indented to indicate each statement's relative position in the hierarchy. Each level is generally set off with braces, with an open brace ({) at the beginning of each hierarchy level and a closing brace (}) at the end. If the statement at a hierarchy level is empty, the braces are not displayed. Each leaf statement ends with a semicolon (;), as does the last statement in the hierarchy.

This indented representation is used when the configuration is displayed or saved as an ASCII file. However, when you load an ASCII configuration file, the format of the file is not so strict. The braces and semicolons are required, but the indention and use of new lines are not required in ASCII configuration files.

RELATED DOCUMENTATION

Understanding J-Web Configuration Tools | 50

CHAPTER 4

System Basics Configuration

IN THIS CHAPTER

- Connecting and Configuring an EX Series Switch (J-Web Procedure) | 66
- Configuring Date and Time for the EX Series Switch (J-Web Procedure) | 70
- Configuring System Identity for an EX Series Switch (J-Web Procedure) | 71
- Configuring Management Access for the EX Series Switch (J-Web Procedure) | 73
- Generating SSL Certificates to Be Used for Secure Web Access (EX Series Switch) | 76
- Rebooting or Halting the EX Series Switch (J-Web Procedure) | 77

Connecting and Configuring an EX Series Switch (J-Web Procedure)

You can configure an EX Series switch using either the J-Web interface or the console using the CLI.

Starting in Junos OS Release 22.3R1, J-Web supports EX4400 switches.

Starting in Junos OS Release 22.4R1, J-Web supports EX4100 and EX4100-F switches.

Starting in Junos OS Release 23.1R1, J-Web supports EX4400-24X switches.

Starting in Junos OS Release 23.2R1, J-Web supports EX4400-EM-1C uplink module for EX4400 and EX4400-24X switches.

Starting in Junos OS Release 24.4R1, J-Web supports EX4100-H-12MP, EX4400-48XP, and EX4400-48MXP switches.

Have these values handy before you begin customizing settings for the switch:

- Hostname
- Root authentication password
- Management port IP address
- Default gateway IP address

- (Optional) DNS server and SNMP read community

Here's how to configure Junos OS for the first time starting from the factory default configuration:

1. Before you connect and configure a switch, set the following parameter values on the console server or PC:
   - Baud rate—9600
   - Flow control—None
   - Data—8
   - Parity—None
   - Stop bits—1
   - DCD state—Disregard
2. Power on the device.
3. Connect the Ethernet cable from the Ethernet port on the PC to the switch.
   - EX2200, EX3200, or EX4200 switch—Connect the cable to port 0 (ge-0/0/0) on the front panel of the switch.
   - EX2300 switches except the EX2300-C, EX2300-24MP, and EX2300-48MP switches, EX3300, EX4100, and EX4100-F switches—Connect the cable to the port labeled **MGMT** on the rear panel of the switch.
   - EX2300-C, EX2300-24MP, EX2300-48MP, EX4100-H, EX4400-24X, EX4500, or EX4550 switch—Connect the cable to the port labeled **MGMT** on the front panel (LCD panel side) of the switch.
   - EX4650 or EX4400 switches—Connect the cable to the port labeled **CON** on the rear panel of the switch.
   - EX6200 switch—Connect the cable to one of the ports labeled **MGMT** on the Switch Fabric and Routing Engine (SRE) module in slot 4 or 5 in an EX6210 switch.
   - EX8200 switch—Connect the cable to the port labeled **MGMT** on the Switch Fabric and Routing Engine (SRE) module in slot SRE0 in an EX8208 switch or on the Routing Engine (RE) module in slot RE0 in an EX8216 switch.
4. At the Junos OS login prompt, type **root** to log in.

   You don't need to enter a password. If the software boots before you connect your laptop or desktop PC to the console port, you might need to press the Enter key for the prompt to appear.

NOTE: EX switches running current Junos software are enabled for Zero Touch Provisioning (ZTP). However, when you configure an EX switch for the very first time, you'll need to disable ZTP. We show you how to do that here. If you see any ZTP-related messages on the console, just ignore them.

5. Start the CLI.

```
root@:RE:0% cli
{master:0} root>
```

6. Enter configuration mode.

```
{master:0} root> configure
{master:0}[edit]
root#
```

7. Delete the ZTP configuration. Factory default configurations can vary over different releases. You may see a message that the statement does not exist. Don't worry, it's safe to proceed.

```
{master:0}[edit]
root# delete chassis auto-image-upgrade
```

8. Add a password to the root administration user account. Enter a plain-text password, an encrypted password, or an SSH public key string. In this example, we show you how to enter a plain-text password.

```
{master:0}[edit]
root# set system root-authentication plain-text-password
New password: password
Retype new password: password
```

9. Activate the current configuration to stop ZTP messages on the console.

```
{master:0}[edit]
root# commit
configuration check succeeds
commit complete
```

10. Configure the hostname.

```
{master:0}[edit]
root# set system host-name name
```

11. Configure the IP address and prefix length for the management interface on the switch. As part of this step, you remove the factory default DHCP setting for the management interface.

```
{master:0}[edit]
root# delete interfaces vme
root# set interfaces vme unit 0 family inet address address/prefix-length
```

12. Configure the default gateway for the management network.

```
{master:0}[edit]
root# set routing-options static route 0/0 next-hop address
```

13. Configure the SSH service. By default, the root user cannot login remotely. In this step, you enable the SSH service and also enable root login through SSH.

```
{master:0}[edit]
root# set system services ssh root-login allow
```

14. Configure the Web management access.

```
{master:0}[edit]
root# set system services web-management https system-generated-certificate
```

15. Optional: Configure the IP address of a DNS server.

```
{master:0}[edit]
root# set system name-server address
```

16. Optional: Configure an SNMP read community.

```
{master:0}[edit]
root# set snmp community community_name
```

17. Optional: Continue customizing the configuration using the CLI.

18. Commit the configuration to activate it on the switch.

```
{master:0}[edit]
root# commit
```

19. When you've finished configuring the switch, exit configuration mode.

```
{master:0}[edit]
root# exit
{master:0}
root@name
```

20. From the laptop or PC, open a Web browser, type the IP address that you configured in the Step 11 in the address field, and then press **Enter**.
    The J-Web Login page appears.
21. Enter the root username and password and click **Login** to view the Configure Options page.
    You can continue to configure the switch.

Configuring Date and Time for the EX Series Switch (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

To configure date and time on an EX Series switch:

1. Select **Configure** > **System Properties** > **Date & Time**.
2. To modify the information, click **Edit**. Enter information into the Edit Date & Time page as described in Table 28 on page 71.
3. Click one of the following options:
   - To apply the configuration, click **OK**.
   - To cancel your entries and return to the System Properties page, click **Cancel**.

NOTE: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

Table 28: Date and Time Settings

Time	Function	Your Action
Time Zone	Identifies the timezone that the switching platform is located in.	Select the appropriate time zone from the list.
Set Time	Synchronizes the system time with that of the NTP server. You can also manually set the system time and date.	To immediately set the time, Click one of the following options: • **Synchronize with PC time**—The switch synchronizes the time with that of the PC. • **NTP Servers**—The switch sends a request to the NTP server and synchronizes the system time. • **Manual**—A pop-up window allows you to select the current date and time from a list.

RELATED DOCUMENTATION

J-Web User Interface for EX Series Switches Overview | 2

Configuring System Identity for an EX Series Switch (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

To configure identification details for an EX Series switch:

1. Select **Configure** > **System Properties** > **System Identity**. The System Identity page displays configuration details.
2. To modify the configuration, click **Edit**. Enter information into the System Identity page as described in Table 29 on page 72.

NOTE: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

Table 29: System Identity Configuration Summary

Field	Function	Your Action
Host Name	Defines the hostname of the switching platform.	Type the hostname.
Domain Name	Defines the network or subnetwork that the machine belongs to.	Type the domain name.
Root Password	Sets the root password that user *root* can use to log in to the switching platform.	Type a plain-text password. The system encrypts the password. **NOTE**: After a root password has been defined, it is required when you log in to the J-Web user interface or the CLI.
Confirm Root Password	Verifies that the root password has been typed correctly.	Retype the password.
DNS Name Servers	Specifies a DNS server for the switching platform to use to resolve hostnames into addresses.	To add an IP address, click **Add**. To edit an IP address, click **Edit**. To delete an IP address, click **Delete**.
Domain Search	Specifies the domains to be searched.	To add a domain, click **Add**. To edit a domain click **Edit**. To delete a domain, click **Delete**.

RELATED DOCUMENTATION

Configuring Date and Time for the EX Series Switch (J-Web Procedure) | 70

Configuring Management Access for the EX Series Switch (J-Web Procedure)

You can manage an EX Series switch remotely through the J-Web interface. To securely communicate with the switch, the J-Web interface uses HTTPS. You can enable HTTPS access on specific interfaces and ports as needed.

Navigate to the Secure Access Configuration page by selecting **Configure** > **System Properties** > **Management Access**. On this page, you can enable HTTPS access on interfaces for managing the EX Series switch through the J-Web interface. You can also install SSL certificates and enable Junos XML management protocol over SSL with the Secure Access page.

1. Click **Edit** to modify the configuration. Enter information into the Management Access Configuration page as described in Table 30 on page 73.
2. To verify that Web access is enabled correctly, connect to the switch using the appropriate method:
   - For HTTPS access—In your Web browser, type **https://** ***URL*** or **https://** ***IP address***.
   - For SSL Junos XML management protocol access—To use this option, you must have a Junos XML management protocol client such as Junos Scope. For information about how to log in to Junos Scope, see the *Junos Scope Software User Guide*.

NOTE: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

Table 30: Secure Management Access Configuration Summary

Field	Function	Your Action
Management Access tab		

Table 30: Secure Management Access Configuration Summary *(Continued)*

Field	Function	Your Action
Management Port IP/Management Port IPv6	Specifies the management port IP address. The software supports both IPv4 (displayed as IP) and IPv6 address. **NOTE**: IPv6 is not supported on EX2200 and EX 4500 switches.	To specify an IPv4 address: 1. Select the check box **IPv4 address**. 2. Type an IP address—for example: **10.10.10.10**. 3. Enter the subnet mask or address prefix. For example, 24 bits represents **255.255.255.0**. 4. Click **OK**. To specify an IPv6 address: 1. Select the check box **IPv6 address**. 2. Type an IP address—for example:**2001:ab8:85a3::8a2e:370:7334**. 3. Enter the subnet mask or address prefix. 4. Click **OK**.
Default Gateway	Defines a default gateway through which to direct packets addressed to networks that are not explicitly listed in the bridge table constructed by the switch.	For IPv4 address type a 32-bit IP address, in dotted decimal notation. Type a 128-bit IP address for IPv6 address type.
Loopback address	Specifies the IP address of the loopback interface.	Type an IP address.
Subnet Mask	Specifies the subnet mask for the loopback interface.	Enter the subnet mask or address prefix.
Services tab		
Services	Specifies services to be enabled: telnet and SSH.	Select to enable the required services.

Table 30: Secure Management Access Configuration Summary *(Continued)*

Field	Function	Your Action
Enable Junos XML management protocol over Clear Text	Enables clear text access to the Junos XML management protocol XML scripting API.	To enable clear text access, select the **Enable Junos XML management protocol over Clear Text** check box.
Enable Junos XML protocol over SSL	Enables secure SSL access to the Junos XML management protocol XML scripting API.	To enable SSL access, select the **Enable Junos XML management protocol over SSL** check box.
Junos XML management protocol Certificate	Specifies SSL certificates to be used for encryption. This field is available only after you create at least one SSL certificate.	To enable an SSL certificate, select a certificate from the Junos XML management protocol SSL Certificate list—for example, **new**.
Enable HTTPS	Enables HTTPS access on interfaces.	To enable HTTPS access, select the **Enable HTTPS access** check box. Select and deselect interfaces by clicking the direction arrows: • To enable HTTPS access on an interface, add the interface to the HTTPS Interfaces list. You can either select either all interfaces or specific interfaces. **NOTE**: Specify the certificate to be used for HTTPS access.

Table 30: Secure Management Access Configuration Summary *(Continued)*

Certificates tab

Certificates	Displays digital certificates required for SSL access to the switch. Allows you to add and delete SSL certificates.	To add a certificate: 1. Have a general SSL certificate available. See Generating SSL Certificates for more information. 2. Click **Add**. The Add a Local Certificate page opens. 3. Type a name in the Certificate Name box—for example, **new**. 4. Open the certificate file and copy its contents. 5. Paste the generated certificate and RSA private key in the Certificate box. To edit a certificate, select it and click **Edit**. To delete a certificate, select it and click **Delete**.

RELATED DOCUMENTATION

Port Security Features

Understanding J-Web User Interface Sessions | 14

Enabling HTTPS and XNM-SSL Services on Switches Using Self-Signed Certificates (CLI Procedure)

Generating SSL Certificates to Be Used for Secure Web Access (EX Series Switch)

You can set up secure Web access for an EX Series switch. To enable secure Web access, you must generate a digital Secure Sockets Layer (SSL) certificate and then enable HTTPS access on the switch.

To generate an SSL certificate:

1. Enter the following `openssl` command in your SSH command-line interface on a BSD or Linux system on which **openssl** is installed. The `openssl` command generates a self-signed SSL certificate in the privacy-enhanced mail (PEM) format. It writes the certificate and an unencrypted 1024-bit RSA private key to the specified file.

   % openssl req –x509 –nodes –newkey rsa:1024 –keyout *filename*.pem -out *filename*.pem

   where ***filename*** is the name of a file in which you want the SSL certificate to be written—for example, `my-certificate`.
2. When prompted, type the appropriate information in the identification form. For example, type **US** for the country name.
3. Display the contents of the file that you created.

   cat my-certificate.pem

You can use the J-Web Configuration page to install the SSL certificate on the switch. To do this, copy the file containing the certificate from the BSD or Linux system to the switch. Then open the file, copy its contents, and paste them into the Certificate box on the J-Web Secure Access Configuration page.

You can also use the following CLI statement to install the SSL certificate on the switch:

```
[edit]
user@switch# set security certificates local my-signed-cert load-key-file my-certificate.pem
```

For more information on installing certificates, see *Example: Configuring Secure Web Access*.

RELATED DOCUMENTATION

> Configuring Management Access for the EX Series Switch (J-Web Procedure)
>
> *Overview of Port Security*

Rebooting or Halting the EX Series Switch (J-Web Procedure)

You can use the J-Web interface to schedule a reboot or to halt the switching platform.

To reboot or halt the switching platform by using the J-Web interface:

1. In the J-Web interface, select **Maintain** > **Reboot**.
2. Select one:
   - **Reboot Immediately**—Reboots the switching platform immediately.

- **Reboot in *number of* minutes**—Reboots the switch in the number of minutes from now that you specify.
- **Reboot when the system time is *hour:minute*** —Reboots the switch at the absolute time that you specify, on the current day. You must select a 2-digit hour in 24-hour format and a 2-digit minute.
- **Halt Immediately**— Stops the switching platform software immediately. After the switching platform software has stopped, you can access the switching platform through the console port only.

3. (Optional) In the Message box, type a message to be displayed to any users on the switching platform before the reboot occurs.
4. Click **Schedule**. The J-Web interface requests confirmation to perform the reboot or halt.
5. Click **OK** to confirm the operation.
   - If the reboot is scheduled to occur immediately, the switch reboots. You cannot access the J-Web interface until the switch has restarted and the boot sequence is complete. After the reboot is complete, refresh the browser window to display the J-Web interface login page.
   - If the reboot is scheduled to occur in the future, the Reboot page displays the time until reboot. You have the option to cancel the request by clicking **Cancel Reboot** on the J-Web interface Reboot page.
   - If the switch is halted, all software processes stop and you can access the switching platform through the console port only. Reboot the switch by pressing any key on the keyboard.

RELATED DOCUMENTATION

Starting the J-Web Interface | 58

CHAPTER 5

Class of Service Configuration

IN THIS CHAPTER

- Defining CoS Drop Profiles (J-Web Procedure) | 79
- Defining CoS Classifiers (J-Web Procedure) | 80
- Defining CoS Code-Point Aliases (J-Web Procedure) | 83
- Assigning CoS Components to Interfaces (J-Web Procedure) | 84
- Defining CoS Forwarding Classes (J-Web Procedure) | 86
- Defining CoS Rewrite Rules (J-Web Procedure) | 87
- Defining CoS Schedulers (J-Web Procedure) | 90
- Defining CoS Scheduler Maps (J-Web Procedure) | 95

Defining CoS Drop Profiles (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

To configure CoS drop profiles:

1. Select **Configure** > **Class of Service** > **Drop Profile**.

   NOTE: After you make changes to the configuration on this page, you must commit the changes immediately for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes (J-Web Procedure) for details about all commit options.

2. Select one of the following options:

   - **Add**—Adds a drop profile. Enter information into the drop profiles page as described in Table 31 on page 80.

- **Edit**—Modifies an existing drop file. Enter information into the drop profiles page as described in Table 31 on page 80.
- **Delete**—Deletes an existing drop profile.

Table 31: Drop Profiles Configuration parameters

Field	Function	Your Action
Drop Profile Name	Specifies the name for a drop profile.	Type the name.
Drop profile graph	Specifies the drop profile graph type	Select one: **Segmented** or **Interpolated**.
Drop profile values	Specifies values for the following two parameters of the drop profile: the queue fill level and the drop probability. The queue fill level represents a percentage of the memory used to store packets in relation to the total amount that has been allocated for that specific queue. The drop probability is a percentage value that correlates to the likelihood that an individual packet is dropped from the network.	To add new values: 1. Click **Add**. 2. Enter the fill level. 3. Enter the drop probability. 4. Click **OK**. To edit an existing value, click **Edit** and modify the fill level and drop probability. To delete a value, select it and click **Delete**.

RELATED DOCUMENTATION

Monitoring CoS Drop Profiles

Example: Configuring CoS on EX Series Switches

Defining CoS Classifiers (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

You can use the J-Web interface to define CoS classifiers on an EX Series switch. Classifiers examine the CoS value or alias of an incoming packet and assign the packet a level of service by setting its forwarding class and loss priority.

To define CoS classifiers:

1. Select **Configure** > **Class of Service** > **Classifiers**.

   NOTE: After you make changes to the configuration on this page, you must commit the changes immediately for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes (J-Web Procedure) for details about all commit options.

2. Click one of the following options:
   - **Add**—Adds a classifier. Enter information into the classifier page as described in Table 32 on page 81.
   - **Edit**—Modifies an existing classifier. Enter information into the classifier page as described in Table 32 on page 81.
   - **Delete**—Deletes an existing classifier.

Table 32: Classifiers Configuration Fields

Field	Function	Your Action
Classifier Name	Specifies the name for a classifier.	To name a classifier, type the name—for example, **ba-classifier**.
Classifier Type	Specifies the type of classifier: **dscp**, **ieee-802.1**, or **inet-precedence**.	Select a value from the list.

Table 32: Classifiers Configuration Fields *(Continued)*

Field	Function	Your Action
Code Point Mapping	Sets the forwarding classes and the packet loss priorities (PLPs) for specific CoS values and aliases.	To add a code point mapping: 1. Click **Add**. 2. Select the code point. 3. Select a forwarding class from the following list: • **expedited-forwarding**—Provides low loss, low delay, low jitter, assured bandwidth, and end-to-end service. Packets can be forwarded out of sequence or dropped. • **best-effort**—Provides no special CoS handling of packets. Typically, RED drop profile is aggressive and no loss priority is defined. • **assured-forwarding**—Provides high assurance for packets within the specified service profile. Excess packets are dropped. • **network-control**—Packets can be delayed but not dropped. 4. Select the loss priority. To assign a loss priority, select one: • **high**—Packet has a high loss priority. • **low**—Packet has a low loss priority.

RELATED DOCUMENTATION

Defining CoS Classifiers (CLI Procedure)

Example: Configuring CoS on EX Series Switches

Monitoring CoS Classifiers

Defining CoS Code-Point Aliases (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

You can use the J-Web interface to define CoS code-point aliases on an EX Series switch. By defining aliases, you can assign meaningful names to a particular set of bit values and refer to them when configuring CoS components.

To define CoS code-point aliases:

1. Select **Configure** > **Class of Service** > **CoS Value Aliases**.

   NOTE: After you make changes to the configuration on this page, you must commit the changes immediately for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes (J-Web Procedure) for details about all commit options.

2. Click one of the following options:

   - **Add**—Adds a code-point alias. Enter information into the code point alias page as described in Table 33 on page 83.
   - **Edit**—Modifies an existing code-point alias. Enter information into the code point alias page as described in Table 33 on page 83.
   - **Delete**—Deletes an existing code-point alias.

Table 33 on page 83 describes the related fields.

Table 33: CoS Value Aliases Configuration Fields

Field	Function	Your Action
Code point name	Specifies the name for a code-point—for example, **af11** or **be**.	Enter a name.
Code point type	Specifies a code-point type. The code-point type can be DSCP or IP precedence.	Select a value.

Table 33: CoS Value Aliases Configuration Fields *(Continued)*

Field	Function	Your Action
Code point value bits	Specifies the CoS value for which an alias is defined. Changing this value alters the behavior of all classifiers that refer to this alias.	To specify a CoS value, type it in the appropriate format: • For DSCP CoS values, use the format xxxxxx, where x is 1 or 0—for example, **101110**. • For IP precedence CoS values, use the format xxx, where x is 1 or 0—for example, **111**.

RELATED DOCUMENTATION

- *Defining CoS Code-Point Aliases (CLI Procedure)*
- *Monitoring CoS Value Aliases*
- *Example: Configuring CoS on EX Series Switches*

Assigning CoS Components to Interfaces (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

After you have defined CoS components on an EX Series switch, you must assign them to logical or physical interfaces. You can use the J-Web interface to assign scheduler maps to physical or logical interfaces and to assign forwarding classes or classifiers to logical interfaces.

To assign CoS components to interfaces:

1. Select **Configure** > **Class of Service** > **Assign to Interface**.

   NOTE: After you make changes to the configuration on this page, you must commit the changes immediately for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes (J-Web Procedure) for details about all commit options.

2. To configure an interface association, select an interface from the list and click **Edit**.

3. Select one of the following:
   - **Associate system default scheduler map**—Associates the interface with the default scheduler map.
   - **Select the scheduler map**—Associates the interface with a configured scheduler map. Select the scheduler map from the list.
4. Click **OK**.
5. To manage a CoS assignment on a logical interface, Click one of the following options:
   - **Add**—Adds a CoS service to a logical interface on a specified physical interface. Enter information as described in Table 34 on page 85.
   - **Edit**—Modifies a CoS service assignment to a logical interface. Enter information as described in Table 34 on page 85.
   - **Delete**—Deletes the CoS service assignment to a logical interface.

Table 34: Assigning CoS Components to Logical Interfaces

Field	Function	Your Action
Unit	Specifies the name of a logical interface. Enables you to assign CoS components when you configure a logical interface on a physical interface.	Type the interface name. To assign CoS to all logical interfaces configured on this physical interface, type the wildcard character (*).
Forwarding Class	Assigns a predefined forwarding class to incoming packets on a logical interface.	To assign a forwarding class to an interface, select the forwarding class.
Classifiers	Enables you to apply classification maps to a logical interface. Classifiers assign a forwarding class and loss priority to an incoming packet based on its CoS value.	To assign a classification map to an interface, select an appropriate classifier for each CoS value type used on the interface.
Rewrite Rules	Enables you to alter the CoS values in outgoing packets to meet the requirements of the targeted peer. A rewrite rule examines the forwarding class and loss priority of a packet and sets its bits to a corresponding value specified in the rule.	To assign rewrite rules to the interface, select the appropriate rewrite rule for each CoS value type used on the interface.

RELATED DOCUMENTATION

Assigning CoS Components to Interfaces (CLI Procedure)

Example: Configuring CoS on EX Series Switches

Monitoring Interfaces That Have CoS Components

Defining CoS Forwarding Classes (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

You can define CoS forwarding classes on an EX Series switch using the J-Web interface. Assigning a forwarding class to a queue number affects the scheduling and marking of a packet as it transits a switch.

To define forwarding classes:

1. Select **Configure** > **Class of Service** > **Forwarding Classes**.

   NOTE: After you make changes to the configuration on this page, you must commit the changes immediately for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes (J-Web Procedure) for details about all commit options.

2. Select one of the following options:

   - **Add**—Adds a forwarding class. Enter information into the forwarding class page as described in Table 35 on page 86.
   - **Edit**—Modifies an existing forwarding class. Enter information into the forwarding class page as described in Table 35 on page 86.
   - **Delete**—Deletes an existing forwarding class.

Table 35: Forwarding Classes Configuration Fields

Field	Function	Your Action
Forwarding Class Summary		

Table 35: Forwarding Classes Configuration Fields *(Continued)*

Field	Function	Your Action
Queue #	Specifies the internal queue numbers to which forwarding classes are assigned. By default, if a packet is not classified, it is assigned to the class associated with queue 0. You can have more than one forwarding class to a queue number.	To specify an internal queue number, select an integer from 0 through 11, appropriate for your platform as follows: **NOTE**: For EX2300 and EX2300-C switches, a maximum of eight egress queues are supported per port. To specify an internal queue number select an integer from 0 through 7.
Forwarding Class Name	Specifies the forwarding class names assigned to specific internal queue numbers. By default, four forwarding classes are assigned to queue numbers 0 (best-effort), 1 (assured-forwarding), 5 (expedited-forwarding), and 7 (network-connect).	Type the name—for example, `be-class`.

RELATED DOCUMENTATION

- *Defining CoS Forwarding Classes (CLI Procedure)*
- *Example: Configuring CoS on EX Series Switches*
- *Example: Prioritizing Snooped and Inspected Packet*
- *Monitoring CoS Forwarding Classes*
- *Assigning CoS Components to Interfaces (J-Web Procedure)*
- *Understanding CoS Forwarding Classes*

Defining CoS Rewrite Rules (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

You can use the J-Web interface to define CoS rewrite rules. Use the rewrite rules to alter the CoS values in outgoing packets to meet the requirements of the targeted peer. A rewrite rule examines the forwarding class and loss priority of a packet and sets its bits to a corresponding value specified in the rule.

To define rewrite rules:

1. Select **Configure** > **Class of Service** > **Rewrite Rules**.

   NOTE: After you make changes to the configuration on this page, you must commit the changes immediately for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes (J-Web Procedure) for details about all commit options.

2. Select one of the following options:

   - **Add**—Adds a rewrite rule. Enter information into the rewrite rule page as described in Table 36 on page 88.
   - **Edit**—Modifies an existing rewrite rule. Enter information into the rewrite rule page as described in Table 36 on page 88.
   - **Delete**—Deletes an existing rewrite rule.

Table 36: Rewrite Rules Configuration Page Summary

Field	Function	Your Action
Rewrite Rule Name	Specifies the name for the rewrite rule.	To name a rule, type the name—for example, **rewrite-dscps**.
Rewrite rule type	Specifies the type of rewrite rule: **dscp**, **ieee-802.1**, or **inet-precedence**.	Select a value from the list.

Table 36: Rewrite Rules Configuration Page Summary *(Continued)*

Field	Function	Your Action
Code Point Mapping	Rewrites outgoing CoS values of a packet based on the forwarding class and loss priority. Allows you to remove a code point mapping entry.	To configure a CoS value assignment, follow these steps: To add a code point mapping: 1. Click **Add**. 2. Select the code point. 3. Select a forwarding class from the following list: • **expedited-forwarding**—Provides low loss, low delay, low jitter, assured bandwidth, and end-to-end service. Packets can be forwarded out of sequence or dropped. • **best-effort**—Provides no special CoS handling of packets. Typically, RED drop profile is aggressive and no loss priority is defined. • **assured-forwarding**—Provides high assurance for packets within the specified service profile. Excess packets are dropped. • **network-control**—Packets can be delayed but not dropped. 4. Select the loss priority. To assign a loss priority, select one: • **high**—Packet has a high loss priority. • **low**—Packet has a low loss priority. To edit an existing code point mapping, select it and click **Edit**. To remove a code point mapping entry, select it and click **Remove**.

RELATED DOCUMENTATION

Defining CoS Rewrite Rules (CLI Procedure)

Understanding CoS Rewrite Rules

Monitoring CoS Rewrite Rules

Example: Configuring CoS on EX Series Switches

Defining CoS Schedulers (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

You can use the J-Web interface to define CoS schedulers on an EX Series switch. Using schedulers, you can assign attributes to queues and thereby provide congestion control for a particular class of traffic. These attributes include the amount of interface bandwidth, memory buffer size, transmit rate, and schedule priority.

To configure schedulers:

1. Select **Configure** > **Class of Service** > **Schedulers**.

   NOTE: After you make changes to the configuration on this page, you must commit the changes immediately for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes (J-Web Procedure) for details about all commit options.

2. Select one of the following options:

   - **Add**—Adds a scheduler. Enter information into the Schedulers page as described in Table 37 on page 91.
   - **Edit**—Modifies an existing scheduler. Enter information into the Schedulers page as described in Table 37 on page 91.
   - **Delete**—Deletes an existing scheduler.

Table 37: Schedulers Configuration Page

Field	Function	Your Action
Scheduler name	Specifies the name for a scheduler.	To name a scheduler, type the name—for example, **be-scheduler**.
Scheduling priority	Sets the transmission priority of the scheduler, which determines the order in which an output interface transmits traffic from the queues. You can set the scheduling priority at different levels in the order of increasing priority from low to high. A high-priority queue with a high transmission rate might lock out lower-priority traffic.	To set a priority, select one: • **low**—Packets in this queue are transmitted last. • **strict-high**—Packets in this queue are transmitted first. To specify no scheduling priority, select the blank check box.

Table 37: Schedulers Configuration Page *(Continued)*

Field	Function	Your Action
Buffer size	Defines the size of the delay buffer. By default, queues 0 through 11 are allotted the following percentages of the total available buffer space: • Queue 0—75 percent • Queue 1—0 percent • Queue 2—0 percent • Queue 3—5 percent • Queue 4—0 percent • Queue 5—0 percent • Queue 6—0 percent • Queue 7—0 percent • Queue 8—15 percent • Queue 9—0 percent • Queue 10—0 percent • Queue 11—5 percent **NOTE**: A large buffer size value correlates with a greater possibility of packet delays. Such a value might not be practical for sensitive traffic such as voice or video.	To define a delay buffer size for a scheduler, select the appropriate option: • To specify no buffer size, select the blank check box. • To specify buffer size as a percentage of the total buffer, select **Percent** and type an integer from 1 through 100. • To specify buffer size as the remaining available buffer, select **Remainder**.

Table 37: Schedulers Configuration Page *(Continued)*

Field	Function	Your Action
Shaping rate	Specifies the rate at which queues transmit packets.	• To specify shaping rate as a percentage, select **Percent** and type an integer from 1 through 100. • To specify shaping rate as a number, select **Rate** and enter a value. • To specify no shaping rate, select the blank check box.

Table 37: Schedulers Configuration Page *(Continued)*

Field	Function	Your Action
Transmit rate	Defines the transmission rate of a scheduler. The transmit rate determines the traffic bandwidth from each forwarding class you configure. By default, queues 0 through 11 are allotted the following percentages of the transmission capacity: • Queue 0—75 percent • Queue 1—0 percent • Queue 2—0 percent • Queue 3—5 percent • Queue 4—0 percent • Queue 5—0 percent • Queue 6—0 percent • Queue 7—0 percent • Queue 8—15 percent • Queue 9—0 percent • Queue 10—0 percent • Queue 11—5 percent	To define a transmit rate, select the appropriate option: • To enforce the exact transmission rate, select **Rate** and enter a value. • To specify the remaining transmission capacity, select **Remainder Available**. • To specify a percentage of transmission capacity, select **Percent** and type an integer from 1 through 100. • To specify no transmit rate, select the blank check box.

RELATED DOCUMENTATION

Defining CoS Schedulers and Scheduler Maps (CLI Procedure)

Example: Configuring CoS on EX Series Switches

Monitoring CoS Scheduler Maps

Defining CoS Scheduler Maps (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

You can use the J-Web interface to configure CoS scheduler maps on an EX Series switch.

NOTE: On EX Series switches, you cannot configure a scheduler map on an individual interface that is a member of a link aggregation group (LAG). Instead, you must configure the scheduler map on the LAG itself—that is, on the aggregated Ethernet (**ae**) interface.

To configure scheduler maps:

1. Select **Configure** > **Class of Service** > **Scheduler Maps**.

   NOTE: After you make changes to the configuration on this page, you must commit the changes immediately for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes (J-Web Procedure) for details about all commit options.

2. Select one of the following options:

   - **Add**—Adds a scheduler map. Enter information into the scheduler map page as described in Table 38 on page 95.
   - **Edit**—Modifies an existing scheduler map. Enter information into the scheduler map page as described in Table 38 on page 95.
   - **Delete**—Deletes an existing scheduler map.

Table 38: Scheduler Maps Configuration Fields

Field	Function	Your Action
Scheduler Map Name	Specifies the name for a scheduler map.	To name a map, type the name—for example, **be-scheduler-map**.

Table 38: Scheduler Maps Configuration Fields *(Continued)*

Field	Function	Your Action
Scheduler Mapping	Enables you to associate a preconfigured scheduler with a forwarding class. After scheduler maps have been applied to an interface, they affect the hardware queues and packet schedulers.	To associate a scheduler with a forwarding class, locate the forwarding class and select the scheduler in the box next to it. For example, for the **best-effort** forwarding class, select the configured scheduler from the list.

RELATED DOCUMENTATION

- *Defining CoS Schedulers (J-Web Procedure)*
- *Defining CoS Schedulers and Scheduler Maps (CLI Procedure)*
- *Example: Configuring CoS on EX Series Switches*
- *Monitoring CoS Scheduler Maps*

CHAPTER 6

Security and Management Configuration

IN THIS CHAPTER

- Configuring 802.1X Authentication (J-Web Procedure) | 97
- Configuring LLDP (J-Web Procedure) | 100
- Configuring Port Mirroring to Analyze Traffic (J-Web Procedure) | 102
- Configuring Port Security (J-Web Procedure) | 104

Configuring 802.1X Authentication (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

To configure 802.1X settings on an EX Series switch using the J-Web interface:

1. Select **Configure** > **Security** > **802.1X**.

   The 802.1X screen displays a list of interfaces, whether 802.1X security has been enabled, and the assigned port role.

   When you select an interface, the **Details of 802.1x configuration on port** section displays 802.1X details for that interface.

   NOTE: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Select one of the following options:

   - RADIUS Servers—Specifies the RADIUS server to be used for authentication. Select the corresponding check box to specify a server. Click **Add** or **Edit** to add or modify the RADIUS server settings. Enter information as specified in Table 39 on page 98.

- Exclusion List—Excludes hosts from the 802.1X authentication list by specifying the MAC address. Click **Add** or **Edit** in the Exclusion List screen to include or modify the MAC addresses. Enter information as specified in Table 40 on page 99.
- Edit—Specifies 802.1X settings for the selected interface
  - Apply 802.1X Profile—Applies an 802.1X profile based on the port role. If a message appears asking whether you want to configure a RADIUS server, click **Yes**.
  - 802.1X Configuration—Configures custom 802.1X settings for the selected interface. If a message appears asking whether you want to configure a RADIUS server, click **Yes**. Enter information as specified in Table 39 on page 98. To configure 802.1X port settings, enter information as specified in Table 41 on page 99.
- Delete—Deletes 802.1X authentication configuration on the selected interface.

Table 39: RADIUS Server Settings

Field	Function	Your Action
IP Address	Specifies the IP address of the server.	Enter the IP address in dotted decimal notation.
Password	Specifies the login password.	Enter the password.
Confirm Password	Verifies the login password for the server.	Reenter the password.
Server Port Number	Specifies the port with which the server is associated.	Type the port number.
Source Address	Specifies the source address of the switch using which the switch can communicate with the server.	Type the IP address in dotted decimal notation.
Retry Attempts	Specifies the number of login retries allowed after a login failure.	Type the number.
Timeout	Specifies the time interval to wait before the connection to the server is closed.	Type the interval in seconds.

Table 40: 802.1X Exclusion List

Field	Function	Your Action
MAC Address	Specifies the MAC address to be excluded from 802.1X authentication.	Enter the MAC address.
Exclude if connected through the port	Specifies that the host can bypass authentication if it is connected through a particular interface.	Select to enable the option. Select the port through which the host is connected.
Move the host to the VLAN	Specifies moving the host to a specific VLAN once the host is authenticated.	Select to enable the option. Select the VLAN from the list.

Table 41: 802.1X Port Settings

Field	Function	Your Action
Supplicant Mode		
Supplicant Mode	Specifies the mode to be adopted for supplicants: • Single—Allows only one host for authentication. • Multiple—Allows multiple hosts for authentication. Each host is checked before being admitted to the network. • Single authentication for multiple hosts—Allows multiple hosts, but only the first host is authenticated.	Select a mode.
Authentication		
Enable re-authentication	Specifies enabling reauthentication on the selected interface.	1. Select to enable reauthentication. 2. Enter the timeout for reauthentication in seconds.

Table 41: 802.1X Port Settings *(Continued)*

Field	Function	Your Action
Action on authentication failure	Specifies the action to be taken if the host does not respond, leading to an authentication failure.	Select one: • Move to the Guest VLAN—Select the VLAN to move the interface to. • Deny—The host is not permitted access.
Timeouts	Specifies timeout values for each action.	Enter the value in seconds for: • Port waiting time after an authentication failure • EAPOL retransmitting interval • Maximum number of EAPOL requests • Maximum number of retries • Port timeout value for the response from the supplicant • Port timeout value for the response from the RADIUS server

RELATED DOCUMENTATION

Configuring 802.1X Interface Settings (CLI Procedure)

Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch

Understanding Authentication on Switches

Configuring LLDP (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

Use the LLDP Configuration page to configure LLDP global and port settings for an EX Series switch on the J-Web interface.

To configure LLDP:

1. Select **Configure** > **Switching** > **LLDP**.

   The LLDP Configuration page displays LLDP Global Settings and Port Settings.

   The second half of the screen displays operational details for the selected port.

   NOTE: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. For an EX8200 Virtual Chassis configuration, select the member and the slot (FPC) from the list.
3. To modify LLDP Global Settings, click **Global Settings**.

   Enter information as described in Table 42 on page 101.
4. To modify Port Settings, click **Edit** in the Port Settings section.

   Enter information as described in Table 43 on page 102.

Table 42: Global Settings

Field	Function	Your Action
Advertising interval	Specifies the frequency of outbound LLDP advertisements. You can increase or decrease this interval.	Type the number of seconds.
Hold multiplier	Specifies the multiplier factor to be used by an LLDP-enabled switch to calculate the time-to-live (TTL) value for the LLDP advertisements it generates and transmits to LLDP neighbors.	Type the required number in the field.
Fast start count	Specifies the number of LLDP advertisements sent in the first second after the device connects. The default is 3. Increasing this number results in the port initially advertising LLDP–MED at a faster rate for a limited time.	Type the Fast start count.

Table 43: Edit Port Settings

Field	Function	Your Action
LLDP Status	Specifies whether LLDP has been enabled on the port.	Select one: **Enabled**, **Disabled**, or **None**.
LLDP-MED Status	Specifies whether LLDP–MED has been enabled on the port.	Select **Enable** from the list.

Configuring Port Mirroring to Analyze Traffic (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

EX Series switches allow you to configure port mirroring to send copies of packets to either a local interface for local monitoring or to a VLAN for remote monitoring. You can use port mirroring to copy these packets:

- Packets entering or exiting a port
- Packets entering a VLAN on EX2200, EX3200, EX3300, EX4200, EX4500, EX6200 switches
- Packets exiting a VLAN on EX8200 switches

To configure port mirroring on an EX Series switch using the J-Web interface:

1. Select **Configure** > **Security** > **Port Mirroring**.

   The top of the screen displays analyzer details such as the name, status, analyzer port, ratio, and loss priority.

   The bottom of the screen lists ingress and egress ports of the selected analyzer.

   NOTE: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Click one of the following options:

- Add—Add an analyzer. Enter information as specified in Table 44 on page 103.
- Edit—Modify details of the selected analyzer. Enter information as specified in Table 44 on page 103.
- Delete—Delete the selected analyzer.
- Enable/Disable—Enable or disable the selected analyzer (toggle).

NOTE: On EX2200, EX3200, EX4200, and EX4500 switches, only one analyzer can be enabled at a time. On EX8200 switches, a maximum of seven analyzers can be enabled.

NOTE: When an analyzer is deleted or disabled, any filter association is removed.

Table 44: Port Mirroring Configuration Settings

Field	Function	Your Action
Analyzer Name	Specifies the name of the analyzer.	Type a name for the analyzer.
Ratio	Specifies the ratio of packets to be mirrored. For example: • A ratio of 1 sends copies of all packets. • A ratio of 2047 sends copies of 1 out of every 2047 packets.	Enter a number from 0 through 2047.
Loss Priority	Specifies the loss priority of the mirrored packets. By default, the switch applies a lower priority to mirrored data than to regular port-to-port data—mirrored traffic is dropped in preference to regular traffic when capacity is exceeded. For port-mirroring configurations with output to an analyzer VLAN, set the loss priority to high.	Keep the default of low, unless the output is to a VLAN.

Table 44: Port Mirroring Configuration Settings *(Continued)*

Field	Function	Your Action
Analyzer Port	Specifies a local interface or VLAN to which mirrored packets are sent. **NOTE**: A VLAN must have only one associated interface to be specified as an analyzer interface.	Click **Select**. In the Select Analyzer Port/ VLAN window, select either port or VLAN as the **Analyzer Type**. Next, select the required port or VLAN. For an EX8200 Virtual Chassis configuration, select the member, FPC, and the port (interface) from the list.
Ingress	Specifies interfaces or VLANs for which entering traffic is mirrored.	Click **Add**. For an EX8200 Virtual Chassis configuration, select the member, FPC, and the interface from the list. Click **Remove** to delete an ingress interface or VLAN.
Egress	Specifies interfaces for which exiting traffic is mirrored.	Click **Add** and select **Port** or **VLAN**. For an EX8200 Virtual Chassis configuration, select the member, FPC, and the interface from the list. Click **Remove** to remove egress interfaces.

RELATED DOCUMENTATION

Configuring Port Mirroring to Analyze Traffic (CLI Procedure)

Example: Configuring Port Mirroring for Local Monitoring of Employee Resource Use on EX Series Switches

Understanding Port Mirroring on EX2200, EX3200, EX3300, EX4200, EX4500, EX4550, EX6200, and EX8200 Series Switches

Configuring Port Security (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

To configure port security on an EX Series switch using the J-Web interface:

1. Select **Configure** > **Security** > **Port Security**.

   The VLAN List table lists all the VLAN names, VLAN identifiers, port members, and port security VLAN features.

   The Interface List table lists all the ports and indicates whether security features have been enabled on the ports.

   > **NOTE**: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Click one of the following options:

   - **Edit**—Click this option to modify the security features for the selected port or VLAN.

     Enter information as specified in Table 45 on page 105 to modify port security settings on VLANs.

     Enter information as specified in Table 46 on page 106 to modify port security settings on interfaces.

   - **Activate/Deactivate**—Click this option to enable or disable security on the switch.

Table 45: Port Security Settings on VLANs

Field	Function	Your Action
General tab		
Enable DHCP Snooping on VLAN	Allows the switch to monitor and control DHCP messages received from untrusted devices connected to the switch. Builds and maintains a database of valid IP addresses/MAC address bindings. (By default, access ports are untrusted and trunk ports are trusted.)	Select to enable DHCP snooping on a specified VLAN or all VLANs. **TIP**: For private VLANs (P-VLANs), enable DHCP snooping on the primary VLAN. If you enable DHCP snooping only on a community VLAN, DHCP messages coming from P-VLAN trunk ports are not snooped.

Table 45: Port Security Settings on VLANs *(Continued)*

Field	Function	Your Action
Enable ARP Inspection on VLAN	Uses information in the DHCP snooping database to validate ARP packets on the LAN and protect against ARP cache poisoning.	Select to enable ARP inspection on a specified VLAN or all VLANs. (Configure any port on which you do not want ARP inspection to occur as a trusted DHCP server port.)
MAC movement	Number of MAC movements allowed on the given VLAN.	Enter a number. The default is unlimited.
MAC movement action	Specifies the action to be taken if the MAC movement limit is exceeded.	Select one of the following options: • **log**—Generate a system log entry, an SNMP trap, or an alarm. • **drop**—Drop the packets and generate a system log entry, an SNMP trap, or an alarm (default). • **shutdown**—Shut down the VLAN and generate an alarm. You can mitigate the effect of this option by configuring autorecovery from the disabled state and specifying a **disable timeout** value. See *Configuring Autorecovery for Port Security Events*. • **none**—Take no action.

Table 46: Port Security on Interfaces

Field	Function	Your Action
Trust DHCP	Specifies trusting DHCP packets on the selected interface. By default, trunk ports are **dhcp-trusted**.	Select to enable DHCP trust.
MAC Limit	Specifies the number of MAC addresses that can be learned on a single Layer 2 access port. This option is not valid for trunk ports.	Enter a number.

Table 46: Port Security on Interfaces *(Continued)*

Field	Function	Your Action
MAC Limit Action	Specifies the action to be taken if the MAC limit is exceeded. This option is not valid for trunk ports.	Select one of the following: • **log**—Generate a system log entry, an SNMP trap, or an alarm. • **drop**—Drop the packets and generate a system log entry, an SNMP trap, or an alarm. (Default) • **shutdown**—Shut down the interface and generate an alarm. You can mitigate the effect of this option by configuring autorecovery from the disabled state and specifying a **disable timeout** value. See *Configuring Autorecovery for Port Security Events* • **none**—Take no action.
Allowed MAC List	Specifies the MAC addresses that are allowed for the interface.	To add a MAC address: 1. Click **Add**. 2. Enter the MAC address. 3. Click **OK**.

RELATED DOCUMENTATION

Configuring Port Security (non-ELS)

Example: Configuring Port Security (non-ELS)

Monitoring Port Security | 304

Port Security Features

CHAPTER 7

Routing Policies and Packet Filtering Configuration

IN THIS CHAPTER

- Configuring Routing Policies (J-Web Procedure) | 108
- Configuring Firewall Filters (J-Web Procedure) | 116

Configuring Routing Policies (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

All routing protocols use the Junos OS routing table to store the routes that they learn and to determine which routes are advertised in the protocol packets. Routing policy allows you to control which routes the routing protocols store in and retrieve from the routing table on the routing device.

To configure routing policies for an EX Series switch using the J-Web interface:

1. Select **Configure** > **Routing** > **Policies**.

   NOTE: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Click one of the following options:

   - **Global Options**—Configures global options for policies. Enter information into the configuration page as described in Table 47 on page 109.
   - **Add**—Configures a new policy. Select **New** and specify a policy name. To add terms, enter information into the configuration page as described in Table 48 on page 110. Select **Clone** to create a copy of an existing policy.
   - **Edit**—Edits an existing policy. To modify an existing term, enter information into the configuration page as described in Table 48 on page 110.

- **Term Up**—Moves a term up in the list.
- **Term Down**—Moves a term down in the list.
- **Delete**—Deletes the selected policy.
- **Test Policy**—Tests the policy. Use this option to check whether the policy produces the results that you expect.

Table 47: Policies Global Configuration Parameters

Field	Function	Your Action
Prefix List	Specifies a list of IPv4 address prefixes for use in a routing policy statement.	To add a prefix list: 1. Click **Add**. 2. Enter a name for the prefix list. 3. To add an IP address, click **Add**. 4. Enter the IP address and the subnet mask and click **OK**. 5. Click **OK**. To edit a prefix list, click **Edit**. Edit the settings and click **OK**. To delete a prefix list, select it and click **Delete**.
BGP Community	Specifies a BGP community.	To add a BGP community: 1. Click **Add**. 2. Enter a name for the community. 3. To add a community, click **Add**. 4. Enter the community ID and click **OK**. 5. Click **OK**. To edit a BGP community, click **Edit**. Edit the settings and click **OK**. To delete a BGP community, select it and click **Delete**.

Table 47: Policies Global Configuration Parameters *(Continued)*

Field	Function	Your Action
AS Path	Specifies an AS path. This is applicable to BGP only.	To add an AS path: 1. Click **Add**. 2. Enter the AS path name. 3. Enter the regular expression and click **OK**. 4. Click **OK**. To edit an AS path, click **Edit**. Edit the settings and click **OK**. To delete an AS path, select it and click **Delete**.

Table 48: Terms Configuration Parameters

Field	Function	Your Action
Term Name	Specifies a term name.	Type or select and edit the name.
Source tab		
Family	Specifies an address family protocol.	Select a value from the list.
Routing Instance	Specifies a routing instance.	Select a value from the list.
RIB	Specifies the name of a routing table.	Select a value from the list
Preference	Specifies the individual preference value for the route.	Type or select and edit the value.
Metric	Specifies a metric value. You can specify up to four metric values.	Type or select and edit the value.

Table 48: Terms Configuration Parameters *(Continued)*

Field	Function	Your Action
Interface	Specifies a name or IP address of one or more routing device interfaces. Do not use this qualifier with protocols that are not interface-specific, such as internal BGP (IBGP).	To add an interface, select **Add** > **Interface**. Select the interface from the list. For an EX8200 Virtual Chassis configuration, select the member, FPC, and the interface from the list. To add an address, select **Add** > **Address**. Select the address from the list. To remove an interface, select it and click **Remove**.
Prefix List	Specifies a named list of IP addresses. You can specify an exact match with incoming routes.	Click **Add**. Select the prefix list from the list and click **OK**. To remove a prefix list, select it and click **Remove**.
Protocol	Specifies the name of the protocol from which the route was learned or to which the route is being advertised.	Click **Add** and select the protocol from the list. To remove a protocol, select it and click **Remove**.
Policy	Specifies the name of a policy to evaluate as a subroutine.	Click **Add**. Select the policy from the list. To remove a policy, select it and click **Remove**.
More	Specifies advanced configuration options for policies.	Click **More** for advanced configuration.
OSPF Area ID	Specifies the area identifier.	Type the IP address.
BGP Origin	Specifies the origin of the AS path information.	Select a value from the list.

Table 48: Terms Configuration Parameters *(Continued)*

Field	Function	Your Action
Local Preference	Specifies the BGP local preference.	Type a value.
Route	Specifies the type of route.	Select **External**. Select the OSPF type from the list.
AS Path	Specifies the name of an AS path regular expression.	Click **Add**. Select the AS path from the list.
Community	Specifies the name of one or more communities.	Click **Add**. Select the community from the list.
Destination tab		
Family	Specifies an address family protocol.	Select a value from the list.
Routing Instance	Specifies a routing instance.	Select a value from the list.
RIB	Specifies the name of a routing table.	Select a value from the list.
Preference	Specifies the individual preference value for the route.	Type a value.
Metric	Specifies a metric value.	Type a value.

Table 48: Terms Configuration Parameters *(Continued)*

Field	Function	Your Action
Interface	Specifies a name or IP address of one or more routing device interfaces. Do not use this qualifier with protocols that are not interface-specific, such as internal BGP (IBGP).	To add an interface, select **Add** > **Interface**. Select the interface from the list. For an EX8200 Virtual Chassis configuration, select the member, FPC, and the interface from the list. To add an address, select **Add** > **Address**. Select the address from the list. To delete an interface, select it and click **Remove**.
Protocol	Specifies the name of the protocol from which the route was learned or to which the route is being advertised.	Click **Add** and select the protocol from the list. To delete a protocol, select it and click **Remove**.
Action tab		
Action	Specifies the action to take if the conditions match.	Select a value from the list.
Default Action	Specifies that any action that is intrinsic to the protocol is overridden. This action is also nonterminating, so that various policy terms can be evaluated before the policy is terminated.	Select a value from the list.
Next	Specifies the default control action if a match occurs, and there are no further terms in the current routing policy.	Select a value from the list.
Priority	Specifies a priority for prefixes included in an OSPF import policy. Prefixes learned through OSPF are installed in the routing table based on the priority assigned to the prefixes.	Select a value from the list.

Table 48: Terms Configuration Parameters *(Continued)*

Field	Function	Your Action
BGP Origin	Specifies the BGP origin attribute.	Select a value from the list.
AS Path Prepend	Affixes an AS number at the beginning of the AS path. The AS numbers are added after the local AS number has been added to the path. This action adds an AS number to AS sequences only, not to AS sets. If the existing AS path begins with a confederation sequence or set, the affixed AS number is placed within a confederation sequence. Otherwise, the affixed AS number is placed with a nonconfederation sequence.	Enter a value.
AS Path Expand	Extracts the last AS number in the existing AS path and affixes that AS number to the beginning of the AS path *n* times, where *n* is a number from 1 through 32. The AS number is added before the local AS number has been added to the path. This action adds AS numbers to AS sequences only, not to AS sets. If the existing AS path begins with a confederation sequence or set, the affixed AS numbers are placed within a confederation sequence. Otherwise, the affixed AS numbers are placed within a nonconfederation sequence. This option is typically used in non-IBGP export policies.	Select the type and type a value.
Load Balance Per Packet	Specifies that all next-hop addresses in the forwarding table must be installed and have the forwarding table perform per-packet load balancing. This policy action allows you to optimize VPLS traffic flows across multiple paths.	Select the check box to enable the option.
Tag	Specifies the tag value. The tag action sets the 32-bit tag field in OSPF external link-state advertisement (LSA) packets.	Select the action and type a value.
Metric	Changes the metric (MED) value by the specified negative or positive offset. This action is useful only in an external BGP (EBGP) export policy.	Select the action and type a value.

Table 48: Terms Configuration Parameters *(Continued)*

Field	Function	Your Action
Route	Specifies whether the route is external.	Select the **External** check box to enable the option, and select the OSPF type.
Preference	Specifies the preference value.	Select the preference action and type a value.
Local Preference	Specifies the BGP local preference attribute.	Select the action and type a value.
Class of Service	Specifies and applies the class-of-service parameters to routes installed into the routing table. • Source class The value entered here maintains the packet counts for a route passing through your network, based on the source address. • Destination class The value entered here maintains packet counts for a route passing through your network, based on the destination address in the packet. • Forwarding class	Type the source class. Type the destination class. Type the forwarding class.

RELATED DOCUMENTATION

- Configuring BGP Sessions (J-Web Procedure) | **168**
- Configuring an OSPF Network (J-Web Procedure) | **176**
- Configuring a RIP Network for EX Series Switches (J-Web Procedure) | **183**
- Configuring Static Routing (J-Web Procedure) | **188**
- Supported Standards for IS-IS

Configuring Firewall Filters (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

You configure firewall filters on EX Series switches to control traffic that enters ports on the switch or enters and exits VLANs on the network and Layer 3 (routed) interfaces. To configure a firewall filter, you must configure the filter and then apply it to a port, VLAN, or Layer 3 interface.

To configure firewall filter settings by using the J-Web interface:

1. Select **Configure** > **Security** > **Filters**.

   The Firewall Filter Configuration page displays a list of all configured ports or VLANs or router filters and the ports or VLANs associated with a particular filter.

   NOTE: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Click one of the following options:

   - **Add**—Select this option to create a new filter. Enter information as specified in Table 49 on page 116.
   - **Edit**—Select this option to edit an existing filter. Enter information as specified in Table 49 on page 116.
   - **Delete**—Select this option to delete a filter.
   - **Term Up**—Select this option to move a term up in the filter term list.
   - **Term Down**—Select this option to move a term down in the filter term list.

Table 49: Create a New Filter

Field	Function	Your Action
Filter tab		
Filter type	Specifies the filter type: port or VLAN firewall filter or router firewall filter.	Select the filter type.

Table 49: Create a New Filter *(Continued)*

Field	Function	Your Action
Filter name	Specifies the name for the filter.	Enter a name.
Select terms to be part of the filter	Specifies the terms to be associated with the filter. Add new terms or edit existing terms.	Click **Add** to add new terms. Enter information as specified in Table 50 on page 117 and Table 51 on page 119.
Association tab		
Port Associations	Specifies the ports with which the filter is associated. **NOTE**: For a port or VLAN filter type, only Ingress direction is supported for port association.	1. Click **Add**. 2. Select the direction: Ingress or Egress. 3. Select the ports. For an EX8200 Virtual Chassis configuration, select the member, FPC, and the available ports from the list. 4. Click **OK**.
VLAN Associations	Specifies the VLANs with which the filter is associated. **NOTE**: Because router firewall filters can be associated with ports only, this section is not displayed for a router firewall filter.	1. Click **Add**. 2. Select the direction: Ingress or Egress. 3. Select the VLANs. 4. Click **OK**.

Table 50: Create a New Term

Field	Function	Your Action
Term Name	Specifies the name of the term.	Enter a name.

Table 50: Create a New Term *(Continued)*

Field	Function	Your Action
Protocols	Specifies the protocols to be associated with the term.	1. Click **Add**. 2. Select the protocols. 3. Click **OK**.
Source	Specifies the source IP address, MAC address, and available ports. **NOTE**: MAC address is specified only for port or VLAN filters.	To specify the IP address, click **Add** > **IP** and enter the IP address. To specify the MAC address, click **Add** > **MAC** and enter the MAC address. To specify the ports (interfaces), click **Add** > **Ports** and enter the port number. To delete the IP address, MAC address, or port details, select it and click **Remove**.
Destination	Specifies the destination IP address, MAC address, and available ports. **NOTE**: MAC address is specified only for port or VLAN filters.	To specify the IP address, click **Add** > **IP** and enter the IP address. To specify the MAC address, click **Add** > **MAC** and enter the MAC address. To specify the ports (interfaces), click **Add** > **Ports** and enter the port number. To delete the IP address, MAC address, or port details, select it and click **Remove**.
Action	Specifies the packet action for the term.	Select one of the following options: • Accept • Discard
More	Specifies advanced configuration options for the filter.	Select the match conditions as specified in Table 51 on page 119. Select the packet action for the term as specified in Table 51 on page 119.

Table 51: Advanced Options for Terms

Table	Function	Your Action
ICMP Type	Specifies the ICMP packet type field. Typically, you specify this match condition in conjunction with the protocol match condition to determine which protocol is being used on the port.	Select the option from the list.
ICMP Code	Specifies more specific information than the ICMP type. Because the value's meaning depends upon the associated ICMP type, you must specify **icmp-type** along with **icmp-code.** The keywords are grouped by the ICMP type with which they are associated.	Select a value from the list.
DSCP	Specifies the Differentiated Services code point (DSCP). The DiffServ protocol uses the type-of-service (ToS) byte in the IP header. The most significant six bits of this byte form the DSCP.	Select the DSCP number from the list.
Precedence	Specifies the IP precedence. **NOTE**: The IP precedence and the DSCP number cannot be specified together for the same term.	Select the option from the list.
IP Options	Specifies the presence of the options field in the IP header.	Select the option from the list.
Interface	Specifies the interface on which the packet is received.	Select the interface from the list.
Ether type	Specifies the Ethernet type field of a packet. **NOTE**: This option is not applicable for a routing filter.	Select a value from the list.

Table 51: Advanced Options for Terms *(Continued)*

Table	Function	Your Action
Dot 1q user priority	Specifies the user-priority field of the tagged Ethernet packet. User-priority values can be 0–7. In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed) : • background (1)—Background • best-effort (0)—Best effort • controlled-load (4)—Controlled load • excellent-load (3)—Excellent load • network-control (7)—Network control reserved traffic • standard (2)—Standard or spare • video (5)—Video • voice (6)—Voice **NOTE**: This option is not applicable for a routing filter.	Select a value from the list.
VLAN	Specifies the VLAN to be associated with the packet. **NOTE**: This option is not applicable for a routing filter.	Select the VLAN from the list.
TCP Flags	Specifies one or more TCP flags. **NOTE**: TCP flags are supported on ingress ports, VLANs, and router interfaces.	Select the option **TCP Initial** or enter a combination of TCP flags.
Fragmentation Flags	Specifies the IP fragmentation flags. **NOTE**: Fragmentation flags are supported on ingress ports, VLANs, and router interfaces.	Select either the option **is-fragment** or enter a combination of fragment action flags.

Table 51: Advanced Options for Terms *(Continued)*

Table	Function	Your Action
Dot1q tag	Specifies the value for the tag field in the Ethernet header. The value can be from 1 through 4095. **NOTE**: This option is not applicable for a routing filter.	Enter the value.
Action		
Counter name	Specifies the count of the number of packets that pass this filter, term, or policer.	Enter a value.
Forwarding class	Classifies the packet into one of the following forwarding classes: • assured-forwarding • best-effort • expedited-forwarding • network-control • None	Select the option from the list.
Loss priority	Specifies the packet loss priority. **NOTE**: Forwarding class and loss priority must be specified together for the same term.	Enter the value.
Analyzer	Specifies whether to perform port mirroring on packets. Port mirroring copies all packets entering one switch port to a network- monitoring connection on another switch port.	Select the analyzer (port mirroring configuration) from the list.

RELATED DOCUMENTATION

Configuring Firewall Filters (CLI Procedure)

Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches

Verifying That Firewall Filters Are Operational

Firewall Filters for EX Series Switches Overview

Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches

CHAPTER 8

Ethernet Switching Configuration

IN THIS CHAPTER

- Configuring VLANs for EX Series Switches (J-Web Procedure) | 123
- Configuring Spanning Tree Protocols on EX Series Switches (J-Web Procedure) | 127
- Configuring IGMP Snooping on EX Series Switches (J-Web Procedure) | 133
- Configuring Redundant Trunk Groups on EX Series Switches (J-Web Procedure) | 137

Configuring VLANs for EX Series Switches (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

You can use the VLAN Configuration page to add a new VLAN or to edit or delete an existing VLAN on an EX Series switch.

To access the VLAN Configuration page:

1. Select **Configure** > **Switching** > **VLAN**.

   The VLAN Configuration page displays a list of existing VLANs. If you select a specific VLAN, the specific VLAN details are displayed in the Details section.

   NOTE: After you make changes to the configuration on this page, you must commit the changes immediately for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Click one of the following options:

   - **Add**—Creates a VLAN.
   - **Edit**—Edits an existing VLAN configuration.
   - **Delete**—Deletes an existing VLAN.

NOTE: If you delete a VLAN, the VLAN configuration for all the associated interfaces is also deleted.

When you are adding or editing a VLAN, enter information as described in Table 52 on page 124.

Table 52: VLAN Configuration Details

Field	Function	Your Action
General tab		
VLAN Name	Specifies a unique name for the VLAN.	Enter a name.
VLAN ID/Range/VLAN ID/List	Specifies the identifier or range for the VLAN.	Select one of the following options: • VLAN ID—Type a unique identification number from **1** through **4094**. If no value is specified, the ID defaults to 0. • VLAN Range/List—Type a number range to create VLANs with IDs corresponding to the numbers in the range. For example, the range 2–3 creates two VLANs with the IDs 2 and 3.
Description	Describes the VLAN.	Enter a brief description for the VLAN.
MAC-Table-Aging-Time	Specifies the maximum time that an entry can remain in the forwarding table before it *ages out*.	Type the number of seconds from **60** through **1000000**.
Input filter	Specifies the VLAN firewall filter that is applied to incoming packets.	To apply an input firewall filter, select the firewall filter from the list.

Table 52: VLAN Configuration Details *(Continued)*

Field	Function	Your Action
Output filter	Specifies the VLAN firewall filter that is applied to outgoing packets.	To apply an output firewall filter, select the firewall filter from the list.
Ports tab		
Ports	Specifies the ports (interfaces) to be associated with this VLAN for data traffic. You can also remove the port association.	Click one of the following options: • **Add**—Select the ports from the available list. For an EX8200 Virtual Chassis configuration, select the member, FPC, and the interface from the list. • **Remove**—Select the port that you do not want to associated with the VLAN.
IP address tab		

Table 52: VLAN Configuration Details *(Continued)*

Field	Function	Your Action
IPv4 address	Specifies IPv4 address options for the VLAN.	Select **IPv4 address** to enable the IPv4 address options. To configure IPv4: 1. Enter the IP address. 2. Enter the subnet mask—for example, **255.255.255.0**. You can also specify the address prefix. 3. To apply an input firewall filter to an interface, select the firewall filter from the list. 4. To apply an output firewall filter to an interface, select the firewall filter from the list. 5. Click the **ARP/MAC Details** button. Enter the static IP address and MAC address in the window that is displayed.
IPv6 address	Specifies IPv6 address options for the VLAN.	Select **IPv6 address**s to enable the IPv6 address options. To configure IPv6: 1. Enter the IP address—for example: **2001:ab8:85a3::8a2e:370:7334**. 2. Specify the subnet mask.
Voip tab		

Table 52: VLAN Configuration Details *(Continued)*

Field	Function	Your Action
Ports	Specifies the ports to be associated with this VLAN for voice traffic. You can also remove the port association.	Click one of the following options: • **Add**—Select the ports from the list of available ports. For an EX8200 Virtual Chassis configuration, select the member, FPC, and the interface from the list. • **Remove**—Select the port that you do not want to associated with the VLAN.

RELATED DOCUMENTATION

- Configuring VLANs for EX Series Switches with ELS Support (CLI Procedure)
- *Configuring VLANs for EX Series Switches*
- *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch with ELS Support*
- *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*
- *Understanding Bridging and VLANs on Switches*
- *Configuring Integrated Routing and Bridging Interfaces on Switches (CLI Procedure)*
- Configuring Routed VLAN Interfaces on Switches (CLI Procedure)

Configuring Spanning Tree Protocols on EX Series Switches (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

EX Series switches provide Layer 2 loop prevention through Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP), and VLAN Spanning Tree Protocol (VSTP). You can configure STP, RSTP, and MSTP by using the J-Web interface. You can

configure bridge protocol data unit (BPDU) protection on interfaces to prevent them from receiving BPDUs that could result in STP misconfigurations, which could lead to network outages.

To configure STP, MSTP, or RSTP for an EX Series switch by using the J-Web interface:

1. Select **Configure** > **Switching** > **Spanning Tree**.

   The Spanning Tree Configuration page displays the spanning-tree protocol configuration parameters and a list of interfaces configured for each spanning-tree protocol configuration.

   NOTE: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Click one of the following options:

   - **Add**—Creates a spanning-tree protocol configuration.

     a. Select a protocol name.

     b. Enter information as described in Table 53 on page 128.

     c. Click **OK** to apply changes to the configuration or click **Cancel** to cancel without saving changes.

   - **Edit**—Modifies a selected spanning-tree protocol configuration.

     a. Enter information as described in Table 53 on page 128.

     b. Click **OK** to apply changes to the configuration or click **Cancel** to cancel without saving changes.

   - **Delete**—Deletes a selected spanning-tree protocol configuration.

Table 53: Spanning-Tree Protocol Configuration Parameters

Field	Function	Your Action
General		
Protocol Name	Specifies the spanning-tree protocol type: STP, MSTP, or RSTP.	None.

Table 53: Spanning-Tree Protocol Configuration Parameters *(Continued)*

Field	Function	Your Action
Disable	Disables spanning-tree protocols on the interface.	To enable this option, select the check box.
BPDU Protect	Specifies BPDU protection on all edge interfaces on the switch.	To enable this option, select the check box.
Bridge Priority	Specifies the bridge priority. The bridge priority determines which bridge is elected as the root bridge. If two bridges have the same path cost to the root bridge, the bridge priority determines which bridge becomes the designated bridge for a LAN segment.	Select a value from the list.
Forward Delay	Specifies the number of seconds an interface waits before changing from spanning-tree learning and listening states to the forwarding state.	Type a value.
Hello Time	Specifies the time interval in seconds at which the root bridge transmits configuration BPDUs.	Type a value.
Max Age	Specifies the maximum-aging time in seconds for all MST instances. The maximum aging time is the number of seconds a switch waits without receiving spanning-tree configuration messages before attempting a reconfiguration.	Type a value.
Max Hops	(MSTP only) Specifies the number of hops in a region before the BPDU is discarded.	Type a value.
Configuration Name	(MSTP only) Specifies the MSTP region name carried in the MSTP BPDUs.	Type a name.

Table 53: Spanning-Tree Protocol Configuration Parameters *(Continued)*

Field	Function	Your Action
Revision Level	(MSTP only) Specifies the revision number of the MSTP configuration.	Type a value.
Ports		
Interface Name	Specifies an interface for the spanning-tree protocol.	1. Click the **Ports** tab. 2. Choose one of the following options: • Click **Add** and select an interface from the list. For an EX8200 Virtual Chassis configuration, select the member, FPC, and the interface from the list. • Select an interface in the **Port/State** table and click **Edit**. • To delete an interface from the configuration, select it in the **Port/State** table and click **Remove**.
Cost	Specifies the link cost to determine which bridge is the designated bridge and which interface is the designated interface.	Type a value.
Priority	Specifies the interface priority to determine which interface is elected as the root port.	Select a value from the list.
Disable Port	Disables the spanning-tree protocol on the interface.	To enable the option, select the check box.
Edge	Configures the interface as an edge interface. Edge interfaces immediately transition to a forwarding state.	To enable the option, select the check box.

Table 53: Spanning-Tree Protocol Configuration Parameters *(Continued)*

Field	Function	Your Action
No Root Port	Specifies an interface as a spanning-tree designated port. If the bridge receives superior STP BPDUs on a root-protected interface, that interface transitions to a root-prevented STP state (inconsistency state) and the interface is blocked. This blocking prevents a bridge that should not be the root bridge from being elected the root bridge. When the bridge stops receiving superior STP BPDUs on the root-protected interface, interface traffic is no longer blocked.	To enable the option, select the check box.
Interface Mode	Specifies the link mode.	1. To enable the option, select the check box. 2. Select one of the following: • **Point to Point**—For a full-duplex link, the default link mode is point-to-point. • **Shared**—For a half-duplex link, the default link mode is shared.
BPDU Timeout Action	Specifies the BPDU timeout action for the interface.	Select one of the following options: • **Log** • **Block**
MSTI (MSTP only)		

Table 53: Spanning-Tree Protocol Configuration Parameters *(Continued)*

Field	Function	Your Action
MSTI Name	Specifies a name (an MSTI ID) for the MST instance.	1. Click the **MSTI** tab. 2. Choose one of the following options: • Click **Add**. • Select an MSTI ID and click **Edit**. • To delete an MSTI from the configuration, select the MSTI ID and click **Remove**.
Bridge Priority	Specifies the bridge priority. The bridge priority determines which bridge is elected as the root bridge. If two bridges have the same path cost to the root bridge, the bridge priority determines which bridge becomes the designated bridge for a LAN segment.	Select a value from the list.
VLAN ID	Specifies the VLAN for the MST instance.	In the VLAN box, choose one of the following options: • Click **Add**, select a VLAN from the list, and click **OK**. • To remove a VLAN association, select the VLAN ID, click **Remove**, and click **OK**.

Table 53: Spanning-Tree Protocol Configuration Parameters *(Continued)*

Field	Function	Your Action
Interfaces	Specifies an interface for the MST instance.	1. In the Interfaces box, click **Add** and select an interface from the list, or select an interface from the list and click **Edit**. 2. Specify the link cost to determine which bridge is the designated bridge and which interface is the designated interface. 3. Specify the interface priority to determine which interface is elected as the root port. 4. If you want to disable the interface, select the check box. 5. Click OK. To delete an interface configuration, select the interface, click **Remove**, and click **OK**.

RELATED DOCUMENTATION

- *Monitoring Spanning Tree Protocols on Switches*
- *Unblocking an Interface on non-ELS EX Series Switches That Receives BPDUs in Error (CLI Procedure)*
- *BPDU Protection for Spanning-Tree Protocols*
- *Example: Configuring BPDU Protection on Switch Edge Interfaces With ELS to Prevent STP Miscalculations*
- *Example: Configuring Network Regions for VLANs with MSTP on Switches*
- *Example: Configuring Faster Convergence and Network Stability on ELS Switches with RSTP*

Configuring IGMP Snooping on EX Series Switches (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

IGMP snooping regulates multicast traffic in a switched network. With IGMP snooping enabled, the EX Series switch monitors the IGMP transmissions between a host (a network device) and a multicast router, keeping track of the multicast groups and associated member interfaces. The switch uses that information to make intelligent multicast-forwarding decisions and forward traffic to the intended destination interfaces.

You can configure IGMP snooping on one or more VLANs to allow the switch to examine IGMP packets and make forwarding decisions based on packet content. By default, IGMP snooping is enabled on EX Series switches.

To enable IGMP snooping and configure individual options by using the J-Web interface:

1. Select **Configure** > **Switching** > **IGMP Snooping**.

   NOTE: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Click one of the following options:
   - **Add**—Creates an IGMP snooping configuration for the VLAN.
   - **Edit**—Modifies an IGMP snooping configuration for the VLAN.
   - **Delete**—Deletes a selected VLAN from the IGMP snooping configuration.

   When you are adding or editing an IGMP snooping configuration, enter information as described in Table 54 on page 134.
3. Click **OK** to apply changes to the configuration or click **Cancel** to cancel without saving changes.

To disable IGMP snooping on a VLAN, select the VLAN from the list and click **Disable**.

Table 54: IGMP Snooping Configuration Fields

Field	Function	Your Action
VLAN Name	Specifies the VLAN on which to enable IGMP snooping.	Select a VLAN from the list to add it to the snooping configuration.

Table 54: IGMP Snooping Configuration Fields *(Continued)*

Field	Function	Your Action
Immediate Leave	Immediately removes a multicast group membership from an interface when it receives a leave message from that interface without waiting for any other IGMP messages to be exchanged (IGMP version 2 and IGMP version 3 only).	To enable the option, select the check box. To disable the option, clear the check box.
Robust Count	Specifies the number of timeout intervals the switch waits before timing out a multicast group.	Type a value.

Table 54: IGMP Snooping Configuration Fields *(Continued)*

Field	Function	Your Action
Interfaces List	Statically configures an interface as a switching interface toward a multicast router or as a member of a multicast group.	Click one of the following options: • Add—Adds an interface to the IGMP snooping configuration. 1. Select an interface from the list. For an EX8200 Virtual Chassis configuration, select the member, FPC, and the interface from the list. 2. Select **Multicast Router Interface**. 3. Type the maximum number of groups an interface can join. 4. In **Static**, choose one: • Click **Add**, type a group IP address, and click **OK**. • Select a group and click **Remove** to remove the group membership. • Edit—Edits the interface settings for the IGMP snooping configuration. • Remove—Deletes an interface configured for IGMP snooping.

RELATED DOCUMENTATION

Example: Configuring IGMP Snooping on EX Series Switches

Configuring Redundant Trunk Groups on EX Series Switches (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

A redundant trunk link provides a simple solution for network recovery when a trunk interface goes down. Traffic is routed to another trunk interface, keeping network convergence time to a minimum. You can configure redundant trunk groups (RTGs) with a primary link and a secondary link on trunk interfaces, or configure dynamic selection of the active interface. If the primary link fails, the secondary link automatically takes over without waiting for normal Spanning Tree Protocol (STP) convergence. An RTG can be created only if the following conditions are satisfied:

- A minimum of two trunk interfaces that are not part of any RTG are available.
- All the selected trunk interfaces to be added to the RTG have the same VLAN configuration.
- The selected trunk interfaces are not part of a spanning-tree configuration.

To configure an RTG by using the J-Web interface:

1. Select **Configure** > **Switching** > **RTG**.

   The RTG Configuration page displays a list of existing RTGs. If you select a specific RTG, the details of the selected RTG are displayed in the Details of group section.

   NOTE: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Click one of the following options:
   - **Add**—Creates an RTG.
   - **Edit**—Modifies an RTG.
   - **Delete**—Deletes an RTG.

   When you are adding or editing an RTG, enter information as described in Table 55 on page 138.
3. Click **OK** to apply changes to the configuration or click **Cancel** to cancel without saving changes.

Table 55: RTG Configuration Fields

Field	Function	Your Action
Group Name	Specifies a unique name for the RTG.	Enter a name.
Member Interface 1	Specifies a logical interface containing multiple trunk interfaces.	Select a trunk interface from the list.
Member Interface 2	Specifies a trunk interface containing multiple VLANs.	Select a trunk interface from the list.
Select Primary Interface	Enables you to specify one of the interfaces in the RTG as the primary link. The interface without this option is the secondary link in the RTG.	1. Select the option button. 2. Select the primary interface.
Dynamically select my active interface	Specifies that the system dynamically select the active interface.	Select the option button.

RELATED DOCUMENTATION

Example: Configuring Redundant Trunk Links for Faster Recovery on Devices with ELS Support

Example: Configuring Redundant Trunk Links for Faster Recovery on EX Series Switches

Understanding Redundant Trunk Links (Legacy RTG Configuration)

CHAPTER 9

Interfaces

IN THIS CHAPTER

- Configuring Gigabit Ethernet Interfaces (J-Web Procedure) | 139
- Configuring Aggregated Ethernet Interfaces (J-Web Procedure) | 148
- Configuring PoE (J-Web Procedure) | 153

Configuring Gigabit Ethernet Interfaces (J-Web Procedure)

You can configure specific properties on your Ethernet interface to ensure optimal performance of your network in a high-traffic environment.

To configure properties on a Gigabit Ethernet interface, a 10-Gigabit Ethernet interface, and a 40-Gigabit Ethernet interface on an EX Series switch:

1. Select **Interfaces** > **Ports**.

   The page that is displayed lists Gigabit Ethernet, 10-Gigabit Ethernet interfaces, and 40-Gigabit Ethernet interfaces, and their link statuses.

   NOTE: After you make changes to the configuration on this page, you must commit the changes immediately for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See "Using the Commit Options to Commit Configuration Changes (J-Web Procedure)" on page 54 for details about all commit options.

2. Select the interface you want to configure. For an EX8200 Virtual Chassis configuration, select the member and the FPC slot if the interface you want to configure is not listed under **Ports** in the top table on the page.

   Details for the selected interface, such as administrative status, link status, speed, duplex, and flow control, are displayed in the **Details of port** table on the page.

NOTE: You can select multiple interfaces and modify their settings at the same time. However, while doing this, you cannot modify the IP address or enable or disable the administrative status of the selected interfaces.

NOTE: In the J-Web interface, you cannot configure interface ranges and interface groups.

3. Click **Edit** and select the set of options you want to configure first:

   - Port Role—Enables you to assign a profile for the selected interface.

     NOTE: When you select a particular port role, preconfigured port security parameters are set for the VLAN that the interface belongs to. For example, if you select the port role **Desktop**, the port security options **examine-dhcp** and **arp-inspection** are enabled on the VLAN that the interface belongs to. If there are interfaces in the VLAN that have static IP addresses, those interfaces might lose connectivity because those static IP addresses might not be present in the DHCP pool. Therefore, when you select a port role, ensure that the corresponding port security settings for the VLAN are applicable to the interface.

     For basic information about port security features such as DHCP snooping (CLI option **examine-dhcp**) or dynamic ARP inspection (DAI) (CLI option **arp-inspection**), see "Configuring Port Security (J-Web Procedure)" on page 104. For detailed descriptions of port security features, see the Port Security topics in the EX Series documentation at https://www.juniper.net/documentation/.

     Click **Details** to view the configuration parameters for the selected port role.

   - VLAN—Enables you to configure VLAN options for the selected interface.

   - Link—Enables you to modify the following link options for the selected interface:

     - Speed
     - MTU
     - Autonegotiation
     - Flow Control
     - Duplex
     - Media Type

- IP—Enables you to configure an IP address for the interface.

4. Configure the interface by configuring options in the selected option set. See Table 56 on page 141 for details of the options.
5. Repeat Steps 3 and 4 for the remaining option sets that you want to configure for the interface.

> **NOTE**: To enable or disable the administrative status of a selected interface, click **Enable Port** or **Disable Port**.

Table 56: Port Edit Options

Field	Function	Your Action
Port Role Options		

Port Role	Specifies a profile (role) to assign to the interface.
	NOTE:
	• After a port role is configured on the interface, you cannot specify VLAN options or IP options.
	• Port roles are not supported by the et interfaces (40-Gigabit Ethernet interfaces) on EX4550 switches.
	• Only the following port roles can be applied on EX8200 switch interfaces:
	  • Default
	  • Layer 2 uplink
	  • Routed uplink	

Table 56: Port Edit Options *(Continued)*

Field	Function	Your Action
Default	Applies the default role. The interface family is set to **ethernet-switching**, port mode is set to **access**, and RSTP is enabled. To enable security configuration, select the **Enable Security Configuration** check box. The `forwarding-options dhcp-security-arp-inspection` will be configured.	1. Click **Details** to view CLI commands for this role. 2. Click **OK**.
Desktop	Applies the desktop role. The interface family is set to **ethernet-switching**, port mode is set to **access**, RSTP is enabled with the **edge** and **point-to-point** options, and port security parameters (MAC limit =1; dynamic ARP inspection and DHCP snooping enabled) are set. To enable security configuration, select the **Enable Security Configuration** check box. The `forwarding-options dhcp-security groups` and `forwarding-options dhcp-security-arp-inspection` will be configured.	1. Select an existing VLAN configuration or type the name of a new VLAN configuration to be associated with the interface. 2. Click **Details** to view CLI commands for this role. 3. Click **OK**.

Table 56: Port Edit Options *(Continued)*

Field	Function	Your Action
Desktop and Phone	Applies the desktop and phone role. The interface family is set to **ethernet-switching**, port mode is set to **access**, port security parameters (MAC limit =1; dynamic ARP Inspection and DHCP snooping enabled) are set, and recommended class-of-service (CoS) parameters are specified for forwarding classes, schedulers, and classifiers. See Table 57 on page 147 for more CoS information. To enable security configuration, select the **Enable Security Configuration** check box. The `forwarding-options dhcp-security groups` and `forwarding-options dhcp-security-arp-inspection` will be configured.	1. Select an existing VLAN configuration or type the name of a new VLAN configuration to be associated with the interface. You can also select an existing VoIP VLAN configuration or a new VoIP VLAN configuration to be associated with the interface. **NOTE**: VoIP is not supported on EX8200 switches. 2. Click **Details** to view CLI commands for this role. 3. Click **OK**.
Wireless Access Point	Applies the wireless access point role. The interface family is set to **ethernet-switching**, port mode is set to **access**, and RSTP is enabled with the **edge** and **point-to-point** options.	1. Select an existing VLAN configuration or type the name of a new VLAN configuration to be associated with the interface. Type the VLAN ID for a new VLAN. 2. Click **Details** to view CLI commands for this role. 3. Click **OK**.

Table 56: Port Edit Options *(Continued)*

Field	Function	Your Action
Routed Uplink	Applies the routed uplink role. The interface family is set to **inet**, and recommended CoS parameters are set for schedulers and classifiers. See Table 57 on page 147 for more CoS information.	To specify an IPv4 address: 1. Select the **IPv4 address** check box. 2. Type an IP address—for example: **10.10.10.10**. 3. Enter the subnet mask or address prefix. For example, 24 bits represents **255.255.255.0**. 4. Click **OK**. To specify an IPv6 address: 1. Select the **IPv6 address** check box. 2. Type an IP address—for example: **2001:ab8:85a3::8a2e:370:7334**. 3. Enter the subnet mask or address prefix. 4. Click **OK**. **NOTE**: IPv6 is not supported on EX2200 VC switches.
Layer 2 Uplink	Applies the Layer 2 uplink role. The interface family is set to **ethernet-switching**, port mode is set to **trunk**, RSTP is enabled with the **point-to-point** option, and trusted DHCP is configured for port security.	1. For this port role, you can select a VLAN member and associate a native VLAN with the interface. 2. Click **Details** to view CLI commands for this role. 3. Click **OK**.
None	Specifies that no port role is configured for the selected interface.	
NOTE: For an EX8200 switch, dynamic ARP inspection and DHCP snooping parameters are not configured.		
VLAN Options		

Table 56: Port Edit Options *(Continued)*

Field	Function	Your Action
Port Mode	Specifies the mode of operation for the interface: trunk or access.	If you select **Trunk**, you can: 1. Click **Add** to add a VLAN member. 2. Select the VLAN and click **OK**. 3. (Optional) Associate a native VLAN with the interface. 4. Click **OK**. If you select **Access**, you can: 1. Select the VLAN member to be associated with the interface. 2. (Optional) Associate a VoIP VLAN with the interface. Only a VLAN with a VLAN ID can be associated as a VoIP VLAN. **NOTE**: VoIP is not supported on EX8200 switches. 3. Click **OK**.
Link Options		
MTU (bytes)	Specifies the maximum transmission unit size (MTU) for the interface.	Type a value from **256** through **9216**. The default MTU size for Gigabit Ethernet interfaces is **1514**.
Speed	Specifies the speed for the mode.	Select one of the following values: **10 Mbps**, **100 Mbps**, **1000 Mbps**, or **Auto-Negotiation.** EX4400, EX4100, and EX4100-F switches support **10 Gbps**, **40 Gbps**, and **100 Gbps** apart from the values mentioned above. Specific switch supported speeds are displayed. **NOTE**: The switches with **mge** ports also supports **2.5 Gbps** and **5 Gbps** apart from the values mentioned above.

Table 56: Port Edit Options *(Continued)*

Field	Function	Your Action
Duplex	Specifies the link mode.	Select one: **automatic**, **half**, or **full**.
Description	Describes the link. **NOTE**: If the interface is part of a link aggregation group (LAG), only the **Description** option is enabled. Other Port Edit options are unavailable.	Enter a brief description for the link.
Enable Auto Negotiation	Enables or disables autonegotiation.	Select the check box to enable autonegotiation, or clear the check box to disable it. By default, autonegotiation is enabled.
Enable Flow Control	Enables or disables flow control.	Select the check box to enable flow control to regulate the amount of traffic sent out of the interface, or clear the check box to disable flow control and permit unrestricted traffic. Flow control is enabled by default.
Media Type	Specifies the media type selected.	Select the check box to enable the media type. Then select **Copper** or **Fiber**.
IP Options		
IPv4 Address	Specifies an IPv4 address for the interface. **NOTE**: If the IPv4 Address check box is cleared, the interface still belongs to the **inet** family.	1. Select the **IPv4 address** check box to specify an IPv4 address. 2. Type an IP address—for example: **10.10.10.10**. 3. Enter the subnet mask or address prefix. For example, 24 bits represents **255.255.255.0**. 4. Click **OK**.

Table 56: Port Edit Options *(Continued)*

Field	Function	Your Action
IPv6 Address	Specifies an IPv6 address for the interface. **NOTE**: If the IPv6 Address check box is cleared, the interface still belongs to the **inet** family.	1. Select the **IPv6 address** check box to specify an IPv6 address. 2. Type an IP address—for example: **2001:ab8:85a3::8a2e:370:7334**. 3. Enter the subnet mask or address prefix. 4. Click **OK**. **NOTE**: IPv6 address is not supported on EX2200 and EX4500 switches.

Table 57: Recommended CoS Settings for Port Roles

CoS Parameter	Recommended Settings
Forwarding Classes	There are four forwarding classes: • **voice**—Queue number is set to 7. • **expedited-forwarding**—Queue number is set to 5. • **assured-forwarding**—Queue number is set to 1. • **best-effort**—Queue number is set to 0.
Schedulers	The schedulers and their settings are: • Strict-priority—Transmission rate is set to 10 percent and buffer size to 5 percent. • Expedited-scheduler—Transmission rate is set to 30 percent, buffer size to 30 percent, and priority to **low**. • Assured-scheduler—Transmission rate is set to 25 percent, buffer size to 25 percent, and priority to **low**. • Best-effort scheduler—Transmission rate is set to 35 percent, buffer size to 40 percent, and priority to **low**.

Table 57: Recommended CoS Settings for Port Roles *(Continued)*

CoS Parameter	Recommended Settings
Scheduler maps	When a desktop and phone, routed uplink, or Layer 2 uplink role is applied on an interface, the forwarding classes and schedulers are mapped using the scheduler map.
ieee-802.1 classifier	Imports the default **ieee-802.1** classifier configuration and sets the loss priority to **low** for the code point 101 for the **voice** forwarding class.
dscp classifier	Imports the default **dscp** classifier configuration and sets the loss priority to **low** for the code point 101110 for the **voice** forwarding class.

RELATED DOCUMENTATION

- Configuring Gigabit Ethernet Interfaces (CLI Procedure)
- *Configuring Gigabit Ethernet Interfaces for EX Series Switches with ELS support*
- Monitoring Interface Status and Traffic | **250**
- *Interfaces Overview for Switches*
- *Junos OS CoS for EX Series Switches Overview*
- *Understanding Interface Naming Conventions*

Configuring Aggregated Ethernet Interfaces (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

Use the link aggregation feature to aggregate one or more Ethernet interfaces to form a virtual link or LAG on an EX Series switch. The MAC client can treat this virtual link as if it were a single link. Link aggregation increases bandwidth, provides graceful degradation when failure occurs, and increases availability. You can use the J-Web interface to configure LAGs, on the switch.

NOTE: Interfaces that are already configured with MTU, duplex, flow control, or logical interfaces are listed but are not available for aggregation.

To configure a LAG:

1. Select **Configure** > **Interfaces** > **Link Aggregation**.

   The list of aggregated interfaces is displayed.

   NOTE: After you make changes to the configuration on this page, you must commit the changes immediately for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See "Using the Commit Options to Commit Configuration Changes (J-Web Procedure)" on page 54 for details about all commit options.

2. Select one of the following:

   - **Add**—Creates a LAG. Enter information as specified in Table 58 on page 150.
   - **Edit**—Modifies a selected LAG.
     - **Aggregation**—Modifies settings for the selected LAG. Enter information as specified in Table 58 on page 150.
     - **VLAN**—Specifies VLAN options for the selected LAG. Enter information as specified in Table 59 on page 151.
     - **IP Option**—Specifies IP options for the selected LAG. Enter information as specified in Table 60 on page 152.
   - **Delete**—Deletes the selected LAG.
   - **Disable Port** or **Enable Port**—Disables or enables the administrative status on the selected interface.
   - **Device Count**—Configures the number of aggregated logical devices available to the switch. Select the number and click **OK**.

Table 58: Aggregated Ethernet Interface Options

Field	Function	Your Action
Aggregated Interface	Specifies the name of the aggregated interface.	None. The name is supplied by the software.
LACP Mode	Specifies the mode in which Link Aggregation Control Protocol (LACP) packets are exchanged between the interfaces. The modes are: • **None**—Indicates that no mode is applicable. • **Active**—Indicates that the interface initiates transmission of LACP packets • **Passive**—Indicates that the interface responds only to LACP packets.	Select from the list.
Description	Specifies a description for the LAG.	Enter a description.
Interface	Specifies the interfaces in the LAG.	To add interfaces to the LAG, select the interfaces and click **Add**. For an EX8200 Virtual Chassis configuration, select the member, FPC, and the interface from the list. Click **OK**. To remove an interface from the LAG, select the interface and click **Remove**. **NOTE**: Only interfaces that are configured with the same speed can be selected together for a LAG.

Table 58: Aggregated Ethernet Interface Options *(Continued)*

Field	Function	Your Action
Enable Log	Specifies whether to enable generation of log entries for the LAG.	Select the check box to enable log generation, or clear the check box to disable log generation.

Table 59: VLAN Options

Field	Function	Your Action
Port Mode	Specifies the mode of operation for the port: trunk or access.	If you select **Trunk**, you can: 1. Click **Add** to add a VLAN member. 2. Select the VLAN and click **OK**. 3. (Optional) Associate a native VLAN ID with the port. If you select **Access**, you can: 1. Select the VLAN member to be associated with the port. 2. (Optional) Associate a VoIP VLAN with the interface. Only a VLAN with a VLAN ID can be associated as a VoIP VLAN. Click **OK**.

Table 60: IP Options

Field	Function	Your Action
IPv4 Address	Specifies an IPv4 address for the selected LAG.	1. Select the check box **IPv4 address**. 2. Type an IP address—for example, **10.10.10.10**. 3. Enter the subnet mask or address prefix. For example, 24 bits represents **255.255.255.0**. 4. Click **OK**.
IPv6 Address	Specifies an IPv6 address for the selected LAG.	1. Select the check box **IPv6 address**. 2. Type an IP address—for example, **2001:ab8:85a3::8a2e:370:7334**. 3. Enter the subnet mask or address prefix. 4. Click **OK**.

RELATED DOCUMENTATION

- Configuring Aggregated Ethernet Links (CLI Procedure)
- *Example: Configuring Aggregated Ethernet High-Speed Uplinks Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch*
- *Example: Configuring Aggregated Ethernet High-Speed Uplinks with LACP Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch*
- Verifying the Status of a LAG Interface
- *Configuring Aggregated Ethernet LACP (CLI Procedure)*

Configuring PoE (J-Web Procedure)

IN THIS SECTION

- Configuring PoE on EX2200, EX2200-C, EX3200, EX3300, EX4100, EX4100-F, EX4100-H, EX4200, and EX4400 Switches | **153**
- Configuring PoE on EX6200 Switches | **155**

NOTE: This topic applies only to the J-Web Application package.

PoE (and PoE+) ports supply electric power over the same ports that are used to connect network devices to EX Series switches. You can use these ports to plug in devices that require both network connectivity and electric power, such as VoIP phones, wireless access points, and some IP cameras. Using the Power over Ethernet (PoE) Configuration page in the J-Web interface, you can modify the settings of all interfaces that are PoE-enabled.

NOTE: For EX4400 switches, only EX4400-48MP and EX4400-24MP switches support PoE.

This topic includes:

Configuring PoE on EX2200, EX2200-C, EX3200, EX3300, EX4100, EX4100-F, EX4100-H, EX4200, and EX4400 Switches

To configure PoE:

NOTE: For EX4400 switches, only EX4400-48MP, EX4400-24MP, EX4400-48XP, and EX4400-48MXP switches support PoE.

1. Select **Configure** > **Power over Ethernet**.

   The page displays a list of all PoE-capable interfaces except uplink ports. Specific operational details about an interface are displayed in the Details section of the page. The details include the PoE operational status and port class.

NOTE: If you are configuring a Virtual Chassis, the PoE configuring option is displayed if any member of the Virtual Chassis supports PoE, even if the Virtual Chassis primary does not support PoE.

NOTE: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Select one of the following options:
   - **Edit**—Changes PoE settings for the selected port as described in Table 61 on page 154.
   - **System Settings**—Modifies general PoE settings as described in Table 62 on page 155.

Table 61: PoE Edit Settings

Field	Description	Your Action
Enable PoE	Specifies that PoE is enabled on the interface.	Select this option to enable PoE or PoE+ on the interface.
Priority	Lists the power priority (low or high) configured on the interface enabled for PoE.	Set the priority as **High** or **Low**.
Maximum Power	Specifies the maximum PoE wattage available to provision the active PoE interface on the switch.	Select a value in watts. If no value is specified, the default is 15.4 for PoE interfaces and 30.0 for PoE+ interfaces. EX4400-48MP, EX4400-24MP, EX4400-24X, EX4400-48XP, and EX4400-48MXP, and EX4100-H switches support up to 90 W using 802.3 bt. **NOTE**: EX4100 and EX4100-F switches does not support this option.

Table 62: System Settings

Field	Description	Your Action
PoE Management	Specifies the power management mode. The options are: **static** and **class**. **NOTE**: When the power management mode is set to **class**, the maximum power value is overridden by the maximum power value of the class of the powered device that is connected to the switch on the PoE port. When the power management mode is set to **static**, you can specify the maximum power for each PoE interface.	By default, the power management mode is **class**. Select **static** to change the power management mode.
Guard Band (watts)	Specifies the amount of power reserved for power spikes from the PoE power budget of the switch.	Enter a value to set the guard band value in watts. The default value is 0.

Configuring PoE on EX6200 Switches

To configure PoE:

1. Select **Configure** > **Power over Ethernet**.

   The page displays a list of all PoE-capable interfaces for each FPC. Specific operational details about an interface are displayed in the Details section of the page. The details include the PoE operational status and port class.

   NOTE: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See "Using the Commit Options to Commit Configuration Changes (J-Web Procedure)" on page 54 for details about all commit options.

2. Select one of the following options:

   - **Edit**—Changes PoE settings for the selected port as described in Table 63 on page 156.
   - **FPC Settings**—Changes PoE settings of PoE-capable FPCs.

     To configure FPC settings, select one of the following options:

     - **Add**—Adds a PoE setting for an FPC as described in Table 64 on page 156.
     - **Edit**—Modifies a PoE setting for an FPC as described in Table 64 on page 156.

- **Delete**—Deletes an existing PoE settings for an FPC.

Table 63: Edit PoE Settings

Field	Description	Your Action
Enable PoE	Specifies that PoE is enabled on the interface.	Select this option to enable PoE or PoE+ on the interface.
Type	Specifies whether the interface is PoE or PoE+.	Select an option from the list.
Priority	Lists the power priority (low or high) configured on the interface enabled for PoE.	Set the priority as **High** or **Low**.
Maximum Power	Specifies the maximum PoE wattage available to provision active PoE ports on the switch.	Select a value in watts. If no value is specified, the default is 15.4 for PoE interfaces and 30.0 for PoE+ interfaces.

Table 64: FPC PoE Settings

Field	Description	Your Action
FPC	Specifies the FPC number.	Select a value from the list.
PoE Management	Specifies the power management mode. The options are **static** and **class**. **NOTE**: When the power management mode is set to **class**, the maximum power value is overridden by the maximum power value for the interface that is connected to the switch on the PoE port. When the power management mode is set to **static**, you can specify the maximum power for each PoE interface.	By default, the power management mode is **class**. Select **static** to change the power management mode.
Guard Band (watts)	Specifies the amount of power reserved for power spikes from the PoE power budget of the switch.	Enter a value to set the guard band value in watts. The default value is 0.

Table 64: FPC PoE Settings *(Continued)*

Field	Description	Your Action
Maximum Power	Specifies the maximum PoE wattage available to provision active PoE ports on the FPC. For example, if you specify 1000 W, the PoE controller is limited to a power budget of 1000 W to distribute to the PoE ports.	Select a value in watts.

RELATED DOCUMENTATION

Configuring PoE Interfaces on EX Series Switches

Understanding PoE on EX Series Switches

CHAPTER 10

Configuring Services

IN THIS CHAPTER

- Configuring DHCP Services (J-Web Procedure) | 158
- Configuring SNMP (J-Web Procedure) | 162

Configuring DHCP Services (J-Web Procedure)

IN THIS SECTION

- Configuring DHCP Services (J-Web Procedure) on EX Series Switches | 158

Configuring DHCP Services (J-Web Procedure) on EX Series Switches

NOTE: This topic applies only to the J-Web Application package.

Use the J-Web DHCP Configuration pages to configure DHCP pools for subnets and static bindings for DHCP clients on an ACX Series Universal Access Gateway router or an EX Series Ethernet Switch. If DHCP pools or static bindings are already configured, use the Configure Global DHCP Parameters Configuration page to add settings for these pools and static bindings. Settings that have been previously configured for DHCP pools or static bindings are not overridden when you use the Configure Global DHCP Parameters Configuration page.

To configure the DHCP server:

1. Select **Configure** > **Services** > **DHCP**
2. Access a DHCP Configuration page:
   - To configure a DHCP pool for a subnet, click **Add** in the DHCP Pools box.

- To configure a static binding for a DHCP client, click **Add** in the DHCP Static Binding box.
- To globally configure settings for existing DHCP pools and static bindings, click **Configure Global DHCP Parameters**.

3. Enter information into the DHCP Service Configuration pages as described in Table 65 on page 159
4. To apply the configuration, click **Apply**.

> **NOTE**: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

Table 65: DHCP Service Configuration Pages Summary

Field	Function	Your Action
DHCP Pool Information		
DHCP Subnet (required)	Specifies the subnet on which DHCP is configured.	Type an IP address prefix.
Address Range (Low) (required)	Specifies the lowest address in the IP address pool range.	Type an IP address that is part of the subnet specified in DHCP Subnet field .
Address Range (High) (required)	Specifies the highest address in the IP address pool range.	Type an IP address that is part of the subnet specified in DHCP Subnet. This address must be greater than the address specified in the Address Range (Low) field.
Exclude Addresses	Specifies addresses to exclude from the IP address pool.	• To add an excluded address, type the address next to the **Add** button, and click **Add**. • To delete an excluded address, select the address in the Exclude Addresses box, and click **Delete**.
Lease Time		

Table 65: DHCP Service Configuration Pages Summary *(Continued)*

Field	Function	Your Action
Maximum Lease Time (Seconds)	Specifies the maximum length of time a client can hold a lease. (Dynamic BOOTP lease lengths can exceed this maximum time.)	Type a number from 60 through 4,294,967,295 (seconds). You can also type **infinite** to specify a lease that never expires.
Default Lease Time (Seconds)	Specifies the length of time a client can hold a lease for clients that do not request a specific lease length.	Type a number from 60 through 2,147,483,647 (seconds). You can also type **infinite** to specify a lease that never expires.
Server Information		
Server Identifier	Specifies the IP address of the DHCP server reported to a client.	Type the IP address of the server. If you do not specify a server identifier, the primary address of the interface on which the DHCP exchange occurs is used.
Domain Name	Specifies the domain name that clients must use to resolve hostnames.	Type the name of the domain.
Domain Search	Specifies the order—from top to bottom—in which clients must append domain names when resolving hostnames using DNS.	• To add a domain name, type the name next to the **Add** button, and click **Add**. • To delete a domain name, select the name in the Domain Search box, and click **Delete**.
DNS Name Servers	Defines a list of DNS servers that the client can use, in the specified order—from top to bottom.	• To add a DNS server, type an IP address next to the **Add** button, and click **Add**. • To remove a DNS server, select the IP address in the DNS Name Servers box, and click **Delete**.

Table 65: DHCP Service Configuration Pages Summary *(Continued)*

Field	Function	Your Action
Gateway Routers	Defines a list of relay agents on the subnet, in the specified order—from top to bottom.	• To add a relay agent, type an IP address next to the **Add** button, and click **Add**. • To remove a relay agent, select the IP address in the Gateway Routers box, and click **Delete**.
WINS Servers	Defines a list of NetBIOS name servers, in the specified order—from top to bottom.	• To add a NetBIOS name server, type an IP address next to the **Add** button, and click **Add**. • To remove a NetBIOS name server, select the IP address in the WINS Servers box, and click **Delete**.
Boot Options		
Boot File	Specifies the path and filename of the initial boot file to be used by the client.	Type a path and filename.
Boot Server	Specifies the Trivial File Transfer Protocol (TFTP) server that the client uses to obtain the client configuration file.	Type the IP address or hostname of the TFTP server.
DHCP Static Binding Information		
DHCP MAC Address (required)	Specifies the MAC address of the client to be permanently assigned a static IP address.	Type the hexadecimal MAC address of the client.
Fixed IP Addresses (required)	Defines a list of IP addresses permanently assigned to the client. A static binding must have at least one fixed address assigned to it, but multiple addresses are also allowed.	• To add an IP address, type it next to the **Add** button, and click **Add**. • To remove an IP address, select it in the Fixed IP Addresses box, and click **Delete**.

Table 65: DHCP Service Configuration Pages Summary *(Continued)*

Field	Function	Your Action
Host Name	Specifies the name of the client used in DHCP messages exchanged between the server and the client. The name must be unique to the client within the subnet on which the client resides.	Type a client hostname.
Client Identifier	Specifies the name of the client used by the DHCP server to index its database of address bindings. The name must be unique to the client within the subnet on which the client resides.	Type a client identifier in string form.
Hexadecimal Client Identifier	Specifies the name of the client, in hexadecimal form, used by the DHCP server to index its database of address bindings. The name must be unique to the client within the subnet on which the client resides.	Type a client identifier in hexadecimal form.

RELATED DOCUMENTATION

Monitoring DHCP Services | 259

Configuring SNMP (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

You can use the J-Web interface to define system identification information, create SNMP communities, create SNMP trap groups, and configure health monitor options for EX Series switches.

To configure SNMP features:

1. Select **Configure** > **Services** > **SNMP**.
2. Enter information into the configuration page for SNMP as described in Table 66 on page 163.

3. To apply the configuration click **Apply**.

> **NOTE**: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

Table 66: SNMP Configuration Page

Field	Function	Your Action
Identification		
Contact Information	Free-form text string that specifies an administrative contact for the system.	Type contact information for the administrator of the system (such as name and phone number).
System Description	Free-form text string that specifies a description for the system.	Type information that describes the system
Local Engine ID	Provides an administratively unique identifier of an SNMPv3 engine for system identification. The local engine ID contains a prefix and a suffix. The prefix is formatted according to specifications defined in RFC 3411. The suffix is defined by the local engine ID. Generally, the local engine ID suffix is the MAC address of Ethernet management port 0.	Type the MAC address of Ethernet management port 0.
System Location	Free-form text string that specifies the location of the system.	Type location information for the system (lab name or rack name, for example).
System Override Name	Free-form text string that overrides the system hostname.	Type the hostname of the system.

Table 66: SNMP Configuration Page *(Continued)*

Field	Function	Your Action
Communities To add a community, click **Add**		
Community Name	Specifies the name of the SNMP community.	Type the name of the community being added.
Authorization	Specifies the type of authorization (either read-only or read-write) for the SNMP community being configured.	Select the authorization (either read-only or read-write) from the list.
Traps To add a trap group, click **Add**.		
Trap Group Name	Specifies the name of the SNMP trap group being configured.	Type the name of the group being added.

Table 66: SNMP Configuration Page *(Continued)*

Field	Function	Your Action
Categories	Specifies which trap categories are added to the trap group being configured.	• To generate traps for authentication failures, select **Authentication**. • To generate traps for chassis and environment notifications, select **Chassis**. • To generate traps for configuration changes, select **Configuration**. • To generate traps for link-related notifications (up-down transitions), select **Link**. • To generate traps for remote operation notifications, select **Remote operations**. • To generate traps for remote network monitoring (RMON), select **RMON alarm**. • To generate traps for routing protocol notifications, select **Routing**. • To generate traps on system warm and cold starts, select **Startup**. • To generate traps on Virtual Router Redundancy Protocol (VRRP) events (such as new-primary or authentication failures), select **VRRP events**.
Targets	Specifies one or more hostnames or IP addresses for the systems to receive SNMP traps generated by the trap group being configured.	1. Enter the hostname or IP address, in dotted decimal notation, of the target system to receive the SNMP traps. 2. Click **Add**.
Health Monitoring		

Table 66: SNMP Configuration Page *(Continued)*

Field	Function	Your Action
Enable Health Monitoring	Enables the SNMP health monitor on the switch. The health monitor periodically (over the time you specify in the interval field) checks the following key indicators of switch health: • Percentage of file storage used • Percentage of Routing Engine CPU used • Percentage of Routing Engine memory used • Percentage of memory used for each system process • Percentage of CPU used by the forwarding process • Percentage of memory used for temporary storage by the forwarding process	Select the check box to enable the health monitor and configure options. Clear the check box to disable the health monitor. **NOTE**: If you select the **Enable Health Monitoring** check box and do not specify options, then SNMP health monitoring is enabled with default values.
Interval	Specifies the sampling frequency, in seconds, over which the key health indicators are sampled and compared with the rising and falling thresholds. For example, if you configure the interval as 100 seconds, the values are checked every 100 seconds.	Enter an interval time, in seconds, from **1** through **2147483647**. The default value is 300 seconds (5 minutes).
Rising Threshold	Specifies the value at which SNMP generates an event (trap and system log message) when the value of a sampled indicator is increasing. For example, if the rising threshold is 90 (the default), SNMP generates an event when the value of any key indicator reaches or exceeds 90 percent.	Enter a value from **0** through **100**. The default value is **90**.

Table 66: SNMP Configuration Page *(Continued)*

Field	Function	Your Action
Falling Threshold	Specifies the value at which SNMP generates an event (trap and system log message) when the value of a sampled indicator is decreasing. For example, if the falling threshold is 80 (the default), SNMP generates an event when the value of any key indicator falls back to 80 percent or less.	Enter a value from **0** through **100**. The default value is **80**. **NOTE**: The falling threshold value must be less than the rising threshold value.

RELATED DOCUMENTATION

Monitoring System Process Information | **245**

Monitoring System Properties | **241**

CHAPTER 11

Configuring Layer 3 Protocols

IN THIS CHAPTER

- Configuring BGP Sessions (J-Web Procedure) | 168
- Configuring an OSPF Network (J-Web Procedure) | 176
- Configuring a RIP Network for EX Series Switches (J-Web Procedure) | 183
- Configuring Static Routing (J-Web Procedure) | 188

Configuring BGP Sessions (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

You can use the J-Web interface to create BGP peering sessions on a routing device.

NOTE: To configure BGP sessions, you must have a license for BGP installed on the EX Series switch.

To configure a BGP peering session:

1. Select **Configure** > **Routing** > **BGP**.

   NOTE: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Click one of the following options:

   - **Add**—Adds a BGP group. Enter information into the configuration page as described in Table 67 on page 169.

- **Edit**—Modifies an existing BGP group. Enter information into the configuration page as described in Table 67 on page 169.
- **Delete**—Deletes an existing BGP group.
- **Disable**—Disables BGP configuration.

3. To modify BGP global settings, click **Edit** in the Global Information section. Enter information as described in Table 68 on page 172.

Table 67: BGP Routing Configuration Summary

Field	Function	Your Action
General tab		
Group Type	Specifies whether the group is an internal BGP (IBGP) group or an external BGP (EBGP) group.	Select the option: **Internal** or **External**.
Group Name	Specifies the name for the group.	Type a new name or select and edit the name.
ASN	Sets the unique numeric identifier of the AS in which the routing device is configured.	Type the routing device's 32-bit AS number, in dotted decimal notation. If you enter an integer, the value is converted to a 32-bit equivalent. For example, if you enter **3**, the value assigned to the AS is **0.0.0.3**.
Preference	Specifies the degree of preference for an external route. The route with the highest local preference value is preferred.	Type or select and edit the value.
Cluster Id	Specifies the cluster identifier to be used by the route reflector cluster in an internal BGP group.	Type or select and edit the IPv6 or IPv4 address to be used as the identifier.
Description	Specifies the text description of the global, group, or neighbor configuration.	Type or select and edit the description.

Table 67: BGP Routing Configuration Summary *(Continued)*

Field	Function	Your Action
Damping	Specifies whether route flap damping is enabled or not.	To enable route flap damping, select the check box. To disable route flap damping do not select the check box.
Advertise Inactive Routes	Specifies whether BGP advertises the best route even if the routing table did not select it to be an active route.	To enable advertising inactive routes, select the check box. To disable advertising inactive routes, do not select the check box.
Advertise Peer AS Routes	Specifies whether to disable the default behavior of suppressing AS routes.	To enable advertising peer AS routes, select the check box. To disable advertising peer AS routes, do not select the check box.
Neighbors tab		
Dynamic Neighbors	Configures a neighbor (peer).	Type the IPv4 address of the peer.

Table 67: BGP Routing Configuration Summary *(Continued)*

Field	Function	Your Action
Static Neighbors	Configures the system's peers statically.	To configure a static neighbor: **1.** Specify the IP address. **2.** Specify the address of the local end of a BGP session. **3.** Specify the degree of preference for an external route. **4.** Enter a description. **5.** Specify the hold-time value to use when negotiating a connection with the peer. **6.** Specify how long a route must be present in the routing table before it is exported to BGP. Use this time delay to help bundle routing updates. **7.** Select **Passive** if you do not want to send active open messages to the peer. **8.** Select the option to compare the AS path of an incoming advertised route with the AS number of the BGP peer under the group and replace all occurrences of the peer AS number in the AS path with its own AS number before advertising the route to the peer. **9.** Specify an import policy and export policy. **10.** Click **OK**.
Policies tab		
Import Policy	Specifies one or more routing policies to routes being imported into the routing table from BGP.	Click **Add** to add an import policy. Select the policy and click **OK**. Click **Move up** or **Move down** to move the selected policy up or down the list of policies. Select the policy and click **Remove**.

Table 67: BGP Routing Configuration Summary *(Continued)*

Field	Function	Your Action
Export Policy	Specifies one or more policies to routes being exported from the routing table into BGP.	Click **Add** to add an export policy. Select the policy and click **OK**. Click **Move up** or **Move down** to move the selected policy up or down the list of policies. Select the policy and click **Remove**.

Table 68: BGP Global Settings

Field	Function	Your Action
General tab		
Router ASN	Specifies the routing device's AS number.	Type or select and edit the value.
Router Identifier	Specify the routing device's IP address.	Type or select and edit the IP address.
BGP Status	Enables or disables BGP.	• To enable BGP, select **Enabled**. • To disable BGP, select **Disabled**.
Description	Describes of the global, group, or neighbor configuration.	Type or select and edit the description.
Confederation Number	Specifies the routing device's confederation AS number.	Type or select and edit the value.

Table 68: BGP Global Settings *(Continued)*

Field	Function	Your Action
Confederation Members	Specifies the AS numbers for the confederation members.	To add a member AS number, click **Add** and enter the number in the **Member ASN** box. Click **OK**. To modify a confederation member's AS number, select the member click **Edit** and, enter the number and click **OK**. To delete a confederation member, select the member and click **Remove**.

Table 68: BGP Global Settings *(Continued)*

Field	Function	Your Action
Advance Options	You can configure the following: • **Keep routes**—Specifies whether routes learned from a BGP peer must be retained in the routing table even if they contain an AS number that was exported from the local AS. • **TCP MSS**—Configures the maximum segment size (MSS) for the TCP connection for BGP neighbors. • **MTU Discovery**—Select to configure MTU discovery. • **Remove Private ASN**—Select to have the local system strip private AS numbers from the AS path when advertising AS paths to remote systems. • **Graceful Restart**—Specifies the time period when the restart is expected to be complete. Specify the maximum time that stale routes are kept during restart. • **Multihop**—Configures the maximum time-to-live (TTL) value for the TTL in the IP header of BGP packets. • **Authentication Type**—Select the authentication algorithm: None, MD5, SHA1, AES.	Select **All** or **None** to configure Keep Routes. Enter a value in the **TCP MSS** box. Click to enable **MTU Discovery**. Click to enable **Remove Private ASN**. Enter the time period for a graceful restart and the maximum time that stale routes must be kept. To configure Multihop, select **Nexthop Change** to allow unconnected third-party next hops. Enter a TTL value. Select the authentication algorithm. If you select None, specify an authentication key (password).
Policies tab		

Table 68: BGP Global Settings *(Continued)*

Field	Function	Your Action
Import Policy	Specifies one or more routing policies to routes being imported into the routing table from BGP.	Click **Add** to add an import policy. Click **Move up** or **Move down** to move the selected policy up or down the list of policies. Click **Remove** to remove an import policy.
Export Policy	Specifies one or more policies to routes being exported from the routing table into BGP.	Click **Add** to add an export policy. Click **Move up** or **Move down** to move the selected policy up or down the list of policies. Click **Remove** to remove an export policy.
Trace Options tab		
File Name	Specifies the name of the file to receive the output of the tracing operation.	Type or select and edit the name.
Number of Files	Specifies the maximum number of trace files.	Type or select and edit the value.
File Size	Specifies the maximum size for each trace file.	Type or select and edit the value.
World Readable	Specifies whether the trace file can be read by any user or not.	Select **True** to allow any user to read the file. Select **False** to disallow all users being able to read the file.
Flags	Specifies the tracing operation to perform.	Select a value from the list.

RELATED DOCUMENTATION

Monitoring BGP Routing Information | 271

Supported Standards for IS-IS

Configuring an OSPF Network (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

You can use the J-Web interface to create multiarea OSPF networks on an EX Series switch.

NOTE: You cannot configure OSPF using J-Web in EX2200 switches except EX2200-C switch.

To configure a multiarea OSPF network:

1. Select **Configure** > **Routing** > **OSPF**.

   NOTE: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Click one of the following options:
   - **Add**—Adds an OSPF area. Enter information into the configuration page as described in Table 69 on page 176.
   - **Edit**—Modifies an existing OSPF area. Enter information into the configuration page as described in Table 69 on page 176.
   - **Delete**—Deletes an existing OSPF area.
3. To modify OSPF global settings, click **Edit**. Enter information as described in Table 70 on page 180.
4. To disable OSPF, click **Disable**.

Table 69: OSPF Routing Configuration Summary

Field	Function	Your Action
General tab		

Table 69: OSPF Routing Configuration Summary *(Continued)*

Field	Function	Your Action
Area Id	Uniquely identifies the area within its AS.	Type a 32-bit numeric identifier for the area. Type an integer or select and edit the value. If you enter an integer, the value is converted to a 32-bit equivalent. For example, if you enter 3, the value assigned to the area is **0.0.0.3**.
Area Ranges	Specifies a range of IP addresses for an area when sending summary link advertisements (within an area).	To add a range: 1. Click **Add**. 2. Type the area range. 3. Specify the subnet mask. 4. To override the metric for the IP address range, type a specific metric value. 5. If you do not want to display the routes that are contained within a summary, select **Restrict advertisements of this area range**. 6. If you want a summary of a route to be advertised only when an exact match is made with the configured summary range, select **Enforce exact match for advertisement of this area range**. 7. Click **OK**. To modify an existing area range, select the area range, click **Edit**, and edit the value. Click **OK**. To delete an area range, select the area range and click **Delete**.

Table 69: OSPF Routing Configuration Summary *(Continued)*

Field	Function	Your Action
Area Type	Designates the type of OSPF area. • **regular**—A regular OSPF area, including the backbone area • **stub**—A stub area • **nssa**—A not-so-stubby area (NSSA)	Select the type of OSPF area you are creating from the list. If you select **stub**: 1. Enter the default metric. 2. To flood summary LSAs into the stub area, select the check box. If you select **nssa**: 1. Specify the metric type. 2. Enter the default metric. 3. To flood summary LSAs into the nssa area, select the check box. 4. To flood Type-7 LSAs into the nssa area, select the check box.
Interfaces tab		

Table 69: OSPF Routing Configuration Summary *(Continued)*

Field	Function	Your Action
Interfaces	Specifies the interfaces to be associated with the OSPF configuration	To associate an interface with the configuration, select the interface from the list, select **Associate** and click **OK**. To edit an interface's configuration: 1. Select the interface from the list and click **Edit**. 2. Specify the cost of an OSPF interface. 3. Specify the traffic engineering metric. 4. Specify how often the routing device sends hello packets from the interface. 5. Specify how long the routing device waits to receive a link-state acknowledgment packet before retransmitting link-state advertisements to an interface's neighbors. 6. To enable OSPF on the interface, select the check box. 7. To inform other protocols about neighbor down events, select the check box. 8. To treat the interface as a secondary interface, select the check box. 9. To only advertise OSPF, select the check box. 10. Click **OK**.
Policies tab		
Import Policy	Specifies one or more policies to control which routes learned from an area are used to generate summary link-state advertisements (LSAs) into other areas.	Click **Add** to add an import policy. Click **Move up** or **Move down** to move the selected policy up or down the list of policies. Click **Remove** to remove an import policy.

Table 69: OSPF Routing Configuration Summary *(Continued)*

Field	Function	Your Action
Export Policy	Specifies one or more policies to control which summary LSAs are flooded into an area.	Click **Add** to add an export policy. Click **Move up** or **Move down** to move the selected policy up or down the list of policies. Click **Remove** to remove an export policy.

Table 70: Edit OSPF Global Settings

Field	Function	Your Action
General tab		
Router Id	Specifies the ID for the routing device.	Type or select and edit the value.
RIB Group	Installs the routes learned from OSPF routing instances into routing tables in the OSPF routing table group.	Select a value.
Internal Route Preference	Specifies the route preference for internal groups.	Type or select and edit the value.
External Route Preference	Specifies the route preference for external groups.	Type or select and edit the value.

Table 70: Edit OSPF Global Settings *(Continued)*

Field	Function	Your Action
Graceful Restart	Configures graceful restart for OSPF.	To configure graceful restart: 1. Specify the estimated time to send out purged grace LSAs over all the interfaces. 2. Specified the estimated time to reacquire a full OSPF neighbor from each area. 3. To disable **No Strict LSA Checking**, select the check box. 4. To disable graceful restart helper capability, select the check box. Helper mode is enabled by default. 5. Click **OK**.
SPF Options	Configure options for running the shortest-path-first (SPF) algorithm. You can configure a delay for when to run the SPF algorithm after a network topology change is detected, the maximum number of times the SPF algorithm can run in succession, and a hold-down interval after the SPF algorithm runs the maximum number of times.	To configure SPF: 1. Specify the time interval between the detection of a topology change and when the SPF algorithm runs. 2. Specify the time interval to hold down, or wait before a subsequent SPF algorithm runs after the SPF algorithm has run the configured maximum number of times in succession. 3. Specify the maximum number of times the SPF algorithm can run in succession. After the maximum is reached, the hold-down interval begins.
Policies tab		
Import Policy	Specifies one or more policies to control which routes learned from an area are used to generate summary link-state advertisements (LSAs) into other areas.	Click **Add** to add an import policy. Click **Move up** or **Move down** to move the selected policy up or down the list of policies. Click **Remove** to remove an import policy.

Table 70: Edit OSPF Global Settings *(Continued)*

Field	Function	Your Action
Export Policy	Specifies one or more policies to control which summary LSAs are flooded into an area.	Click **Add** to add an export policy. Click **Move up** or **Move down** to move the selected policy up or down the list of policies. Click **Remove** to remove an export policy.
Trace Options tab		
File Name	Specifies the name of the file to receive the output of the tracing operation.	Type or select and edit the name.
Number of Files	Specifies the maximum number of trace files.	Type or select and edit the name.
File Size	Specifies the maximum size for each trace file.	Type or select and edit the name.
World Readable	Specifies whether the trace file can be read by any user or not.	Select **True** to allow any user to read the file. Select **False** to disallow all users being able to read the file.
Flags	Specifies the tracing operation to perform.	Select a value from the list.

RELATED DOCUMENTATION

Monitoring OSPF Routing Information | 264

Supported Standards for IS-IS

Configuring a RIP Network for EX Series Switches (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

You can use the J-Web interface to create RIP networks.

To configure a RIP network:

1. Select **Configure** > **Routing** > **RIP**.

   NOTE: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Click one of the following options:
   - **Add**—Configures a RIP instance. Enter information into the RIP Configuration page as described in Table 71 on page 183.
   - **Edit**—Modifies an existing RIP instance. Enter information into the configuration page for RIP as described in Table 71 on page 183.
   - **Delete**—Deletes an existing RIP instance.
3. To modify RIP global settings, click **Edit**. Enter information in the configuration as described in Table 72 on page 185.

Table 71: RIP Routing Configuration Summary

Field	Function	Your Action
General tab		
Routing instance name	Specifies a name for the routing instance.	Type or select and edit the name.
Preference	Specifies the preference of external routes learned by RIP as compared to those learned from other routing protocols.	Type or select and edit the value.

Table 71: RIP Routing Configuration Summary *(Continued)*

Field	Function	Your Action
Metric Out	Specifies the metric value to add to routes transmitted to the neighbor.	Type or select and edit the value.
Update interval	Specifies an update time interval to periodically send out routes learned by RIP to neighbors.	Type or select and edit the value.
Route timeout	Specifies the route timeout interval for RIP.	Type or select and edit the value.
Policies tab		
Import Policy	Applies one or more policies to routes being imported into the local routing device from the neighbors.	Click **Add** to add an import policy. Click **Move up** or **Move down** to move the selected policy up or down the list of policies. Click **Remove** to remove an import policy.
Export Policy	Applies a policy to routes being exported to the neighbors.	Click **Add** to add an export policy. Click **Move up** or **Move down** to move the selected policy up or down the list of policies. Click **Remove** to remove an export policy.
Neighbors tab		
RIP-Enabled Interfaces	Selects the interfaces to be associated with the RIP instance.	To enable RIP on an interface, click the check box next to the interface name. Click Edit if you want to modify an interface's settings.

Table 72: Edit RIP Global Settings

Field	Function	Your Action
General tab		
Send	Specifies RIP send options.	Select a value.
Receive	Configure RIP receive options.	Select a value.
Route timeout (sec)	Specifies the route timeout interval for RIP.	Type a value.
Update interval (sec)	Specifies the update time interval to periodically send out routes learned by RIP to neighbors.	Type or select and edit the value.
Hold timeout (sec)	Specifies the time period the expired route is retained in the routing table before being removed.	Type or select and edit the value.
Metric in	Specifies the metric to add to incoming routes when advertising into RIP routes that were learned from other protocols.	Type or select and edit the value.
RIB Group	Specifies a routing table group to install RIP routes into multiple routing tables.	Select and edit the name of the routing table group.
Message size	Specifies the number of route entries to be included in every RIP update message.	Type or select and edit the value.

Table 72: Edit RIP Global Settings *(Continued)*

Field	Function	Your Action
Check Zero	Specifies whether the reserved fields in a RIP packet are zero. Options are: • **check-zero**—Discard version 1 packets that have nonzero values in the reserved fields and version 2 packets that have nonzero values in the fields that must be zero. This default behavior implements the RIP version 1 and version 2 specifications. • **no-check-zero**—Receive RIP version 1 packets with nonzero values in the reserved fields or RIP version 2 packets with nonzero values in the fields that must be zero. This is in spite of the fact that they are being sent in violation of the specifications in RFC 1058 and RFC 2453.	Select a value.
Graceful switchover	Configures graceful switchover for OSPF.	To disable graceful restart, select **Disable**. Type or select and edit the estimated time for the restart to finish, in seconds.
Authentication Type	Specifies the type of authentication for RIP route queries received on an interface. Options are: • None • MD5 • Simple	Select the authentication type. Enter the authentication key for MD5.
Policies tab		

Table 72: Edit RIP Global Settings *(Continued)*

Field	Function	Your Action
Import Policy	Applies one or more policies to routes being imported into the local routing device from the neighbors.	Click **Add** to add an import policy. Click **Move up** or **Move down** to move the selected policy up or down the list of policies. Click **Remove** to remove an import policy.
Export Policy	Applies a policy to routes being exported to the neighbors.	Click **Add** to add an export policy. Click **Move up** or **Move down** to move the selected policy up or down the list of policies. Click **Remove** to remove an export policy.
Trace Options tab		
File Name	Specifies the name of the file to receive the output of the tracing operation.	Type or select and edit the name.
Number of Files	Specifies the maximum number of trace files.	Type or select and edit the name.
File Size	Specifies the maximum size for each trace file.	Type or select and edit the name.
World Readable	Specifies whether the trace file can be read by any user or not.	Select **True** to allow any user to read the file. Select **False** to disallow all users being able to read the file.
Flags	Specifies the tracing operation to perform.	Select a value from the list.

RELATED DOCUMENTATION

Monitoring RIP Routing Information

Supported Standards for IS-IS

Configuring Static Routing (J-Web Procedure)

You can use the J-Web interface to configure static routes for EX Series switches.

To configure static routes:

1. Select **Configure** > **Routing** > **Static Routing**. The Static Routing page displays details of the configured routes.

   NOTE: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Click one of the following options:
   - **Add**—To configure a route. Enter information into the routing page as described in Table 73 on page 188.
   - **Edit**—To modify an existing route. Enter information into the routing page as described in Table 73 on page 188.
   - **Delete**—To delete an existing route.

Table 73: Static Routing Configuration Summary

Field	Function	Your Action
Default Route		

Table 73: Static Routing Configuration Summary *(Continued)*

Field	Function	Your Action
Default Route	Specifies the default gateway for the switch. **NOTE**: IPv6 is not supported on EX2200 and EX4500 switches.	To specify an IPv4 address: 1. Select **IPv4**. 2. Type an IP address—for example, **10.10.10.10**. 3. Enter the subnet mask or address prefix. For example, 24 bits represents **255.255.255.0**. To specify an IPv6 address: 1. Select **IPv6**. 2. Type an IP address—for example, **2001:ab8:85a3::8a2e:370:7334**. 3. Enter the subnet mask or address prefix.
Static Routes		
Nexthop	Specifies the next-hop address or addresses to be used when routing traffic to the static route.	To add an address: 1. Click **Add**. 2. In the IP address dialog, enter the IP address. **NOTE**: If a route has multiple next-hop addresses, traffic is routed across each address in round-robin fashion. 3. Click **OK**. To delete a next-hop address, select it from the list and click **Delete**.

RELATED DOCUMENTATION

Configuring Static Routing (CLI Procedure)

Monitoring Routing Information | **275**

Supported Standards for IS-IS

CHAPTER 12

Configuring Real-Time Performance Monitoring

IN THIS CHAPTER

- Configuring Real-Time Performance Monitoring (J-Web Procedure) | 191
- Viewing Real-Time Performance Monitoring Information | 201

Configuring Real-Time Performance Monitoring (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

Real-time performance monitoring (RPM) in EX Series switches enables you to configure and send probes to a specified target and monitor the analyzed results to determine packet loss, round-trip time, and jitter. Jitter is the difference in relative transit time between two consecutive probes. You can set up probe owners and configure one or more performance probe tests under each probe owner.

The ways in which you can use RPM include:

- Monitor time delays between devices.
- Monitor time delays at the protocol level.
- Set thresholds to trigger SNMP traps when threshold values are exceeded. You can configure thresholds for round-trip time, ingress or egress delay, standard deviation, jitter, successive lost probes, and total lost probes per test.
- Determine automatically whether a path exists between a host switch and its configured Border Gateway Protocol (BGP) neighbors. You can view the results of the discovery using an SNMP client.
- Use the history of the most recent 50 probes to analyze trends in your network and predict future needs.

Probes collect packets per destination and per application, including PING Internet Control Message Protocol (ICMP) packets, User Datagram Protocol and Transmission Control Protocol (UDP/TCP) packets

with user-configured ports, user-configured Differentiated Services code point (DSCP) type-of-service (ToS) packets, and Hypertext Transfer Protocol (HTTP) packets.

EX Series switches support the following tests and probe types:

- Ping tests:
  - ICMP echo
  - ICMP timestamp
- HTTP tests:
  - HTTP get (not available for BGP RPM services)
- UDP and TCP tests with user-configured ports:
  - UDP echo
  - TCP connection
  - UDP timestamp

To account for latency in the communication of probe messages, you can enable timestamping of the probe packets. You must configure both the requester and the responder to timestamp the RPM packets. The RPM features provides an additional configuration option to set one-way hardware timestamps. Use one-way timestamps when you want information about one-way, rather than round-trip, times for packets to traverse the network between the requester and the responder.

NOTE:

- EX Series switches support hardware timestamps for UDP and ICMP probes. EX Series switches do not support hardware timestamps for HTTP or TCP probes.
- If the responder does not support hardware timestamps, RPM can only report the round-trip measurements, it cannot calculate round-trip jitter.
- In EX Series switches timestamps apply only to IPv4 traffic.

To configure RPM using the J-Web interface:

1. Select **Troubleshoot** > **RPM** > **Configure RPM** .
2. In the **Configure RPM** page, enter information as specified in Table 74 on page 193.
   a. Click **Add** to set up the **Owner Name** and **Performance Probe Tests**.
   b. Select a probe owner from **Probe Owners** list and click **Delete** to remove the selected probe owner

c. Double-click one of the probe owners in **Probe Owners** list to display the list of performance probe tests.

d. Double-click one of the performance probe tests to edit the test parameters.

3. Enter the **Maximum Number of Concurrent Probes** and specify the **Probe Servers**.
4. Click **Apply** to apply the RPM probe settings.

Table 74: RPM Probe Owner, Concurrent Probes, and Probe Servers Configuration Fields

Field	Function	Your Action
Probe Owners	Identifies a owner for whom one or more RPM tests are configured. In most implementations, the owner name identifies a network on which a set of tests is being run.	1. Click **Add** and type an owner name. 2. In **Performance Probe Tests**, click **Add** to define the RPM test parameters. See Table 75 on page 194 for information on configuring RPM test parameters. 3. Click **OK** to save the settings or **Cancel** to exit from the window without saving the changes.
Maximum Number of Concurrent Probes	Specifies the maximum number of concurrent probes allowed.	Type a number from 1 through 500.

Table 74: RPM Probe Owner, Concurrent Probes, and Probe Servers Configuration Fields *(Continued)*

Field	Function	Your Action
Probe Servers	Specifies the servers that act as receivers and transmitters for the probes.	Set up the following servers: • TCP Probe Server—Specifies the port on which the device is to receive and transmit TCP probes. Type the number 7 (a standard TCP port number) or a port number from 49160 through 65535. • UDP Probe Server—Specifies the port on which the device is to receive and transmit UDP probes. Type the number 7 (a standard TCP port number) or a port number from 49160 through 65535.

Table 75: Performance Probe Tests Configuration Fields

Field	Function	Your Action
Identification		
Test Name	Identifies the RPM test.	Type a test name.
Target (Address or URL)	Specifies the IP address or the URL of the probe target.	Type the IP address in dotted decimal notation or the URL of the probe target. If the target is a URL, type a fully formed URL that includes **http://**.
Source Address	Specifies the IP address to be used as the probe source address.	Type the source address to be used for the probe. If you do not supply this value, the packet uses the outgoing interface's address as the probe source address.

Table 75: Performance Probe Tests Configuration Fields *(Continued)*

Field	Function	Your Action
Routing Instance	Specifies the routing instance over which the probe is sent.	Type the routing instance name. The routing instance applies only to **icmp-ping** and **icmp-ping-timestamp** probe types. The default routing instance is **inet.0**.
History Size	Specifies the number of probe results to be saved in the probe history.	Type a number from 0 through 255. The default history size is 50.
Request Information		
Probe Type	Specifies the type of probe to send as part of the test.	Select a probe type from the list: • **http-get** • **http-get-metadata** • **icmp-ping** • **icmp-ping-timestamp** • **tcp-ping** • **udp-ping** • **udp-ping-timestamp**
Interval	Sets the wait time (in seconds) between probe transmissions.	Type a number from 1 through 255 .
Test Interval	Sets the wait time (in seconds) between tests.	Type a number from 0 through 86400 .
Probe Count	Sets the total number of probes to be sent for each test.	Type a number from 1 through 15.

Table 75: Performance Probe Tests Configuration Fields *(Continued)*

Field	Function	Your Action
Moving Average Size	Specifies the number of samples to be used in the statistical calculation operations to be performed across a number of the most recent samples.	Type a number from 0 through 255.
Destination Port	Specifies the TCP or UDP port to which probes are sent. To use TCP or UDP probes, you must configure the remote server as a probe receiver. Both the probe server and the remote server must be Juniper Networks network devices configured to receive and transmit RPM probes on the same TCP or UDP port.	Type the number 7 (a standard TCP or UDP port number) or a port number from 49160 through 65535.
DSCP Bits	Specifies the Differentiated Services code point (DSCP) bits. This value must be a valid 6-bit pattern.	Type a valid 6-bit pattern.
Data Size	Specifies the size (in bytes) of the data portion of the ICMP probes.	Type a number from 0 through 65507.
Data Fill	Specifies the hexadecimal value of the data portion of the ICMP probes.	Type a hexadecimal value from 1h through 800h .
Hardware Timestamp		
One Way Hardware Timestamp	Enables one-way hardware timestamp.	To enable timestamping, select the check box.
Destination Interface	Enables hardware timestamp on the specified interface.	Select an interface from the list.

Table 75: Performance Probe Tests Configuration Fields *(Continued)*

Field	Function	Your Action
Maximum Probe Thresholds		
Successive Lost Probes	Sets the number of probes that can be lost successively, if exceeded, triggers a probe failure and generates a system log message.	Type a number from 0 through 15.
Lost Probes	Sets the number of probes that can be lost , if exceeded, triggers a probe failure and generates a system log message.	Type a number from 0 through 15.
Round Trip Time	Sets the round-trip time (in microseconds), from the switch to the remote server, if exceeded, triggers a probe failure and generates a system log message.	Type a number from 0 through 60000000.
Jitter	Sets the jitter (in microseconds), if exceeded, triggers a probe failure and generates a system log message.	Type a number from 0 through 60000000.
Standard Deviation	Sets the maximum allowable standard deviation (in microseconds), if exceeded, triggers a probe failure and generates a system log message.	Type a number from 0 through 60000000.
Egress Time	Sets the one-way time (in microseconds), from the switch to the remote server, if exceeded, triggers a probe failure and generates a system log message.	Type a number from 0 through 60000000.

Table 75: Performance Probe Tests Configuration Fields *(Continued)*

Field	Function	Your Action
Ingress Time	Sets the one-way time (in microseconds), from the remote server to the switch, if exceeded, triggers a probe failure and generates a system log message.	Type a number from 0 through 60000000 (microseconds).
Jitter Egress Time	Sets the outbound-time jitter (in microseconds), if exceeded triggers a probe failure and generates a system log message.	Type a number from 0 through 60000000.
Jitter Ingress Time	Sets the inbound-time jitter (in microseconds), if exceeded, triggers a probe failure and generates a system log message.	Type a number from 0 and 60000000.
Egress Standard Deviation	Sets the maximum allowable standard deviation of outbound times (in microseconds), if exceeded, triggers a probe failure and generates a system log message.	Type a number from 0 through 60000000.
Ingress Standard Deviation	Sets the maximum allowable standard deviation of inbound times (in microseconds), if exceeded, triggers a probe failure and generates a system log message.	Type a number from 0 through 60000000.
Traps		
Egress Jitter Exceeded	Generates SNMP traps when the threshold for jitter in outbound time is exceeded.	• To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.

Table 75: Performance Probe Tests Configuration Fields *(Continued)*

Field	Function	Your Action
Egress Standard Deviation Exceeded	Generates SNMP traps when the threshold for standard deviation in outbound times is exceeded.	• To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.
Egress Time Exceeded	Generates SNMP traps when the threshold for maximum outbound time is exceeded.	• To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.
Ingress Jitter Exceeded	Generates SNMP traps when the threshold for jitter in inbound time is exceeded.	• To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.
Ingress Standard Deviation Exceeded	Generates SNMP traps when the threshold for standard deviation in inbound times is exceeded.	• To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.
Ingress Time Exceeded	Generates SNMP traps when the threshold for maximum inbound time is exceeded.	• To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.
Jitter Exceeded	Generates SNMP traps when the threshold for jitter in round-trip time is exceeded.	• To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.

Table 75: Performance Probe Tests Configuration Fields *(Continued)*

Field	Function	Your Action
Probe Failure	Generates SNMP traps when the threshold for the number of successive lost probes is exceeded.	• To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.
RTT Exceeded	Generates SNMP traps when the threshold for maximum round-trip time is exceeded.	• To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.
Standard Deviation Exceeded	Generates SNMP traps when the threshold for standard deviation in round-trip times is exceeded.	• To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.
Test Completion	Generates SNMP traps when a test is completed.	• To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.
Test Failure	Generates SNMP traps when the threshold for the total number of lost probes is exceeded.	• To enable SNMP traps for this condition, select the check box. • To disable SNMP traps, clear the check box.

RELATED DOCUMENTATION

Configuring SNMP (J-Web Procedure) | **162**

Viewing Real-Time Performance Monitoring Information | **201**

Viewing Real-Time Performance Monitoring Information

NOTE: This topic applies only to the J-Web Application package.

Real-time performance monitoring (RPM) on EX Series switches enables you to configure and send probes to a specified target and monitor the analyzed results to determine packet loss, round-trip time, and jitter. The J-Web interface provides a graphical view of RPM information for EX Series switches.

To view the RPM information using the J-Web interface:

1. Select **Troubleshoot** >**RPM** >**View RPM**.
2. Select the **Round Trip Time** check box to display the graph with round-trip time included. Clear the check-box to view the graph without the round-trip time.
3. From the **Refresh Time** list, select a refresh time interval for the graph.

CHAPTER 13

Software Installation and Upgrades

IN THIS CHAPTER

- Updating J-Web Interface on EX Series Switches (J-Web Procedure) | 202
- Upgrading Junos OS on EX Series Switches (J-Web Procedure) | 204

Updating J-Web Interface on EX Series Switches (J-Web Procedure)

IN THIS SECTION

- Installing J-Web Application Package by Using Auto Update | 202
- Installing J-Web Application Package by Using Manual Update | 203

You can update the J-Web software packages on a single fixed-configuration switch or for all members of a Virtual Chassis.

You can use the J-Web interface to install the latest Application package that is associated with the installed Junos OS, from a server by using FTP or HTTPS, or by uploading the file to the switch.

There are two ways in which you can use the J-Web interface to download and install the J-Web Application package:

- Auto update
- Manual update

Installing J-Web Application Package by Using Auto Update

To *automatically* check for and install the latest version of the J-Web Application package:

1. Click **Update Now** in the Update Available window that appears when you log in to the J-Web interface.

NOTE:

- For the Update Available window to appear when you log in, your switch or computer should be connected to the Internet.
- The Update Available window appears only if there is a latest update available on the Juniper Networks server.
- For the Update Available window to appear when you log in, the **Check for updates automatically on every login** in the *Update Preference* section in the **Maintain > Update J-Web** side pane must be selected.
- If you choose *Update Later*, you can update to the latest J-Web Application package by clicking the orange icon next to *Update Available* on the top pane of the J-Web interface or through **Maintain > Update J-Web**.

2. If the switch is connected to the Internet, the Update J-Web window appears. Enter the authentication details to download from the Juniper Networks download server. The J-Web Application package downloads and installs on the switch.

   If the switch is not connected to the Internet and your computer is connected to the Internet, download the latest version of the J-Web Application package to your computer and install it on your switch. Click **Download Application Package** in the Update J-Web window, enter authentication details to download from the Juniper Networks download server, and download the file to your computer. Select the file and click **Update**.

NOTE: You can also download the file to your computer and update it on the switch later by clicking *Select Application Package* in the Maintain > Update J-Web side pane, and selecting where the package is located.

SEE ALSO

Upgrading Junos OS on EX Series Switches (J-Web Procedure) | 204

Installing J-Web Application Package by Using Manual Update

To *manually* check for and install the latest J-Web Application package:

1. Go to **Maintain > Update J-Web** in the side pane, and click **Check for updates**.

   If the latest update is available on the Juniper Networks server, the Update Available window appears.
2. Click **Update Now** in the Update Available window.

3. If the switch is connected to the Internet, the Update J-Web window appears. Enter the authentication details to download from the Juniper Networks download server, and click **Update**. The J-Web Application package downloads and installs on the switch.

   If the switch is not connected to the Internet and your computer is connected to the Internet, download the latest version of the J-Web Application package to your local computer and install it on your switch. Click **Download Application Package** in the Update J-Web window, enter authentication details to download from the Juniper Networks download server, and download the file to your local system. Select the file, and click **Update**.

   NOTE: You can also download the file to your computer and update it on the switch later by clicking *Select Application Package* in the Maintain > Update J-Web side pane, and selecting where the downloaded package is located.

SEE ALSO

Upgrading Junos OS on EX Series Switches (J-Web Procedure) | 204

Upgrading Junos OS on EX Series Switches (J-Web Procedure)

IN THIS SECTION

- Installing Junos OS Upgrades by Uploading File from Local Computer | 204

You can upgrade the Junos OS package on a single fixed-configuration switch or for all members of a Virtual Chassis.

You can use the J-Web interface to download and install Junos OS upgrades by copying the file to the EX Series switch.

Installing Junos OS Upgrades by Uploading File from Local Computer

To install software upgrades by uploading files:

1. Download the software package.
2. In the J-Web interface, select **Maintain > Update Junos**.

3. In the *Update Junos* section, select **Local File**. The *Upload Package* section appears below the Update Junos section.
4. In the Upload Package section, enter information into the fields described in Table 76 on page 205.
5. Click **Upload and Install Package**. The software is activated after the switching platform completes the installation procedure.

Table 76: Upload Package Summary

Field	Function	Your Action
File to Upload (required)	Specifies the location of the software package.	Type the location of the software package, or click **Browse** to navigate to the location.
Reboot If Required	Specifies that the switching platform is automatically rebooted when the upgrade is complete.	Select the check box if you want the switching platform to reboot automatically when the upgrade is complete.

SEE ALSO

Updating J-Web Interface on EX Series Switches (J-Web Procedure) | 202

CHAPTER 14

Configuration, Files, Users, Licenses, and Product Registration

IN THIS CHAPTER

- Managing Configuration Files Through the Configuration History (J-Web Procedure) | **206**
- Setting or Deleting the Rescue Configuration (J-Web Procedure) | **210**
- Uploading a Configuration File (J-Web Procedure) | **211**
- Managing Log, Temporary, and Crash Files on the Switch (J-Web Procedure) | **212**
- Managing Users (J-Web Procedure) | **214**
- Managing Licenses for the EX Series Switch (J-Web Procedure) | **217**
- Registering the EX Series Switch with the J-Web Interface | **219**
- Generating Support Information Reports for EX Series Switches Using the J-Web Interface | **219**

Managing Configuration Files Through the Configuration History (J-Web Procedure)

IN THIS SECTION

- Displaying Configuration History | **207**
- Displaying Users Editing the Configuration | **208**
- Comparing Configuration Files with the J-Web Interface | **209**
- Downloading a Configuration File with the J-Web Interface | **209**
- Loading a Previous Configuration File with the J-Web Interface | **210**

NOTE: This topic applies only to the J-Web Application package.

Use the Configuration History function to manage configuration files.

Displaying Configuration History

To manage configuration files with the J-Web interface, select **Maintain** > **Config Management** > **History**. The main pane displays History — Database Information page.

Table 77 on page 207 summarizes the contents of the display.

The configuration history display allows you to:

- View a configuration.
- Compare two configurations.
- Download a configuration file to your local system.
- Roll back the configuration to any of the previous versions stored on the switch.

Table 77: J-Web Configuration History Summary

Field	Description
Number	Version of the configuration file.
Date/Time	Date and time the configuration was committed.
User	Name of the user who committed the configuration.
Client	Method by which the configuration was committed: • **cli**—A user entered a Junos OS CLI command. • **junoscript**—A Junos XML protocol client performed the operation. Commit operations performed by users through the J-Web interface are identified in this way. • **snmp**—An SNMP **set** request started the operation. • **other**—Another method was used to commit the configuration.

Table 77: J-Web Configuration History Summary *(Continued)*

Field	Description
Comment	Comment.
Log Message	Method used to edit the configuration: • Imported via paste— Configuration was edited and loaded with the **Configure** > **CLI Tools** > **Edit Configuration Text** option. • Imported upload [*filename*]—Configuration was uploaded with the **Configure** > **CLI Tools** > **Point Click Editor** option. • Modified via J-Web Configure — Configuration was modified with the J-Web Configure menu. • Rolled back via *user-interface*— Configuration was rolled back to a previous version through the user interface specified by *user-interface*, which can be Web Interface or CLI.
Action	Action to perform with the configuration file. The action can be **Download** or **Rollback**.

Displaying Users Editing the Configuration

To display a list of users editing the switching platform configuration, select **Config Management** > **History**. The list is displayed as Database Information in the main pane. Table 78 on page 208 summarizes the Database Information display.

Table 78: J-Web Configuration Database Information Summary

Field	Description
User Name	Name of user editing the configuration.
Start Time	Time of day the user logged in to the switch.
Idle Time	Elapsed time since the user issued a configuration command from the CLI.
Terminal	Terminal on which the user is logged in.

Table 78: J-Web Configuration Database Information Summary *(Continued)*

Field	Description
PID	Process identifier assigned to the user by the switching platform.
Edit Flags	Designates a private or exclusive edit.
Edit Path	Level of the configuration hierarchy that the user is editing.

SEE ALSO

> *Understanding Configuration Files*
>
> Understanding J-Web Configuration Tools | 50

Comparing Configuration Files with the J-Web Interface

To compare any two of the past 50 committed configuration files:

1. Select **Config Management** > **History**. A list of the current and the previous 49 configurations is displayed as Configuration History in the main pane.
2. Select the check boxes to the left of the two configuration versions you want to compare.
3. Click **Compare**.

   The main pane displays the differences between the two configuration files at each hierarchy level as follows:

   - Lines that have changed are highlighted side by side in green.
   - Lines that exist only in the more recent configuration file are displayed in red on the left.
   - Lines that exist only in the older configuration file are displayed in blue on the right.

Downloading a Configuration File with the J-Web Interface

To download a configuration file from the switch to your local system:

1. Select **Config Management** > **History**. A list of current and previous 49 configurations is displayed as Configuration History in the main pane.
2. In the Action column, click **Download** for the version of the configuration you want to download.
3. Select the options your Web browser provides that allow you to save the configuration file to a target directory on your local system.

The file is saved as an ASCII file.

Loading a Previous Configuration File with the J-Web Interface

To load (roll back) and commit a previous configuration file stored on the switching platform:

1. Select **Config Management** > **History**. A list of current and previous 49 configurations is displayed as Configuration History in the main pane.
2. In the Action column, click **Rollback** for the version of the configuration you want to load.

   The main pane displays the results of the rollback operation.

> **NOTE**: When you click **Rollback**, the switch loads and commits the selected configuration. This behavior is different from the switch's behavior that occurs after you enter the **rollback** configuration mode command from the CLI. In the latter case, the configuration is loaded but not committed.

RELATED DOCUMENTATION

Understanding Configuration Files

Understanding J-Web Configuration Tools | 50

Setting or Deleting the Rescue Configuration (J-Web Procedure)

> **NOTE**: This topic applies only to the J-Web Application package.

A rescue configuration is a well-known configuration that recovers a switch from a configuration that denies management access. You set a current committed configuration to be the rescue configuration through the J-Web interface or CLI.

If someone inadvertently commits a configuration that denies management access to an EX Series switch and the console port is not accessible, you can overwrite the invalid configuration and replace it with the rescue configuration by using the LCD panel on the switch. The rescue configuration is a previously committed, valid configuration. We recommend that the rescue configuration include the IP address (accessible from the network) for the management port.

To view, set, or delete the rescue configuration using the J-Web interface, select **Maintain** > **Config Management** > **Rescue**. On the Rescue page, you can perform the following tasks:

- View the current rescue configuration—Click **View rescue configuration**.
- Set the current running configuration as the rescue configuration—Click **Set rescue configuration**.
- Delete the current rescue configuration—Click **Delete rescue configuration**.

RELATED DOCUMENTATION

Rescue Configuration

Configuration Files Terms

Uploading a Configuration File (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

You can create a configuration file on your local system, copy the file to the EX Series switch and then load the file into the CLI. After you have loaded the configuration file, you can commit it to activate the configuration on the switch. You can also edit the configuration interactively using the CLI and commit it at a later time.

To upload a configuration file from your local system:

1. Select **Maintain** > **Config Management** > **Upload**.
   The work area displays the File to Upload box.
2. Specify the name of the file to upload using one of the following methods:
   - Type the absolute path and filename in the File to Upload box.
   - Click **Browse** to navigate to the file.
3. Click **Upload and Commit** to upload and commit the configuration.
   The switch checks the configuration for the correct syntax before committing it.

RELATED DOCUMENTATION

Uploading a Configuration File (CLI Procedure)

Understanding J-Web Configuration Tools | 50

Understanding Configuration Files

Managing Log, Temporary, and Crash Files on the Switch (J-Web Procedure)

IN THIS SECTION

- Cleaning Up Files | 212
- Downloading Files | 213
- Deleting Files | 213

NOTE: This topic applies only to the J-Web Application package.

You can use the J-Web interface to rotate log files and delete unnecessary log, temporary, and crash files on the switch.

Cleaning Up Files

If you are running low on storage space, use the file cleanup procedure to quickly identify files to delete.

The file cleanup procedure performs the following tasks:

- Rotates log files—Archives the current log files, and creates fresh log files.
- Deletes log files in **/var/log**—Deletes files that are not currently being written to.
- Deletes temporary files in **/var/tmp**—Deletes files that have not been accessed within two days.
- Deletes all crash files in **/var/crash**—Deletes core files that the switch has written during an error.

To rotate log files and delete unnecessary files with the J-Web interface:

1. Select **Maintain** > **Files**.
2. In the Clean Up Files section, click **Clean Up Files**. The switching platform rotates log files and identifies files that can be safely deleted.

   The J-Web interface displays the files that you can delete and the amount of space that will be freed on the file system.
3. Click one of the following options:
   - To delete the files and return to the Files page, click **OK**.
   - To cancel your entries and return to the list of files in the directory, click **Cancel**.

Downloading Files

You can use the J-Web interface to download a copy of an individual log, temporary, or crash file from the switching platform. When you download a file, it is not deleted from the file system.

To download files with the J-Web interface:

1. In the J-Web interface, select **Maintain** > **Files**.
2. In the Download and Delete Files section, Click one of the following options:
   - Log Files—Log files in the **/var/log** directory on the switch.
   - Temporary Files—Lists the temporary files in the **/var/tmp** directory on the switching platform.
   - Jailed Temporary Files (Install, Session, and so on)—Lists the files in the **/var/jail/tmp** directory on the switching platform.
   - Crash (Core) Files—Lists the core files in the **/var/crash** directory on the switching platform.

     The J-Web interface displays the files located in the directory.
3. Select the files that you want to download and click **Download**.
4. Choose a location for the saved file.

   The file is saved as a text file, with a **.txt** file extension.

Deleting Files

You can use the J-Web interface to delete an individual log, temporary, and crash file from the switching platform. When you delete the file, it is permanently removed from the file system.

CAUTION: If you are unsure whether to delete a file from the switching platform, we recommend using the Clean Up Files tool described in Cleaning Up Files. This tool determines which files can be safely deleted from the file system.

To delete files with the J-Web interface:

1. Select **Maintain** > **Files**.
2. In the Download and Delete Files section, Click one of the following options:
   - Log Files—Lists the log files in the **/var/log** directory on the switching platform.
   - Temporary Files—Lists the temporary files in the **/var/tmp** directory on the switching platform.
   - Jailed Temporary Files (Install, Session, etc)—Lists the files in the **/var/jail/tmp** directory on the switching platform.
   - Crash (Core) Files—Lists the core files in the **/var/crash** directory on the switching platform.

The J-Web interface displays the files in the directory.

3. Select the box next to each file you plan to delete.
4. Click **Delete**.

   The J-Web interface displays the files you can delete and the amount of space that will be freed on the file system.
5. Click one of the following buttons on the confirmation page:
   - To delete the files and return to the Files page, click **OK**.
   - To cancel your entries and return to the list of files in the directory, click **Cancel**.

RELATED DOCUMENTATION

J-Web User Interface for EX Series Switches Overview | 2

Managing Users (J-Web Procedure)

You can use the Users Configuration page for user information to add new users to an EX Series switch. For each account, you define a login name and password for the user and specify a login class for access privileges.

To configure users:

1. Select **Configure** > **System Properties** > **User Management**.

   The User Management page displays details of users, the authentication order, the RADIUS servers and TACACS servers present.
2. Click **Edit**.
3. Click any of the following options on the **Users** tab:
   - **Add**—Select this option to add a user. Enter details as described in Table 79 on page 215.
   - **Edit**—Select this option to edit an existing user's details. Enter details as described in Table 79 on page 215.
   - **Delete**—Select this option to delete a user.
4. Click an option on the **Authentication Methods and Order** tab:
   - Authentication Order—Drag and drop the authentication type from the Available Methods section to the Selected Methods. Click the up or down buttons to modify the authentication order.
   - RADIUS server—Click one of the following options:

- **Add**—Select this option to add an authentication server. Enter details as described in Table 80 on page 216.
- **Edit**—Select this option to modify the authentication server details. Enter details as described in Table 80 on page 216.
- **Delete**—Select this option to delete an authentication server from the list.

- TACACS server—Click one of the following options:
  - **Add**—Select this option to add an authentication server. Enter details as described in Table 80 on page 216.
  - **Edit**—Select this option to modify the authentication server details. Enter details as described in Table 80 on page 216.
  - **Delete**—Select this option to delete an authentication server from the list.

NOTE: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

Table 79: User Management Configuration Page Summary

Field	Function	Your Action
User Information		
Username (required)	Specifies the name that identifies the user.	Type the username. It must be unique within the switching platform. Do not include spaces, colons, or commas in the username.
User Id	Specifies the user identification.	Type the user's ID.
Full Name	Specifies the user's full name.	Type the user's full name. If the full name contains spaces, enclose it in quotation marks. Do not include colons or commas.

Table 79: User Management Configuration Page Summary *(Continued)*

Field	Function	Your Action
Login Class (required)	Defines the user's access privilege.	Select the user's login class from the list: • **operator** • **read-only** • **super-user/superuser** • **unauthorized** This list also includes any user-defined login classes.
Password	Specifies the login password for this user.	Type the login password for this user. The login password must meet these criteria: • The password must be at least 6 characters long. • It can include alphabetic, numeric, and special characters, but not control characters. • It must contain at least one change of case or character class.
Confirm Password	Verifies the login password for this user.	Retype the login password for this user.

Table 80: Add an Authentication Server

Field	Function	Your Action
IP Address	Specifies the IP address of the server.	Type the server's 32-bit IP address, in dotted decimal notation.
Password	Specifies the password of the server.	Type the password of the server.
Confirm Password	Verifies that the password of the server is entered correctly.	Retype the password of the server.

Table 80: Add an Authentication Server *(Continued)*

Field	Function	Your Action
Server Port	Specifies the port with which the server is associated.	Type the port number.
Source Address	Specifies the source address of the server.	Type the server's 32-bit IP address, in dotted decimal notation.
Retry Attempts	Specifies the number of login retries allowed after a login failure.	Type the number. **NOTE**: Only 1 retry is permitted for a TACACS server.
Time out	Specifies the time interval to wait before the connection to the server is closed.	Type the interval in seconds.

RELATED DOCUMENTATION

Configuring Management Access for the EX Series Switch (J-Web Procedure) | 73

Managing Licenses for the EX Series Switch (J-Web Procedure)

IN THIS SECTION

- Adding New Licenses | 218
- Deleting Licenses | 218
- Displaying License Keys | 218
- Downloading Licenses | 219

This topic applies only to the J-Web Application package.

To enable and use some Junos OS features on an EX Series switch, you must purchase, install, and manage separate software licenses. Each switch requires one license. For a Virtual Chassis deployment, two licenses are recommended for redundancy. After you have configured the features, you see a warning message if the switch does not have a license for the feature.

Before you begin managing licenses, be sure that you have:

- Obtained the needed licenses. For information about how to purchase software licenses, contact your Juniper Networks sales representative.
- Understand what makes up a license key. For more information, see *License Key Components for the EX Series Switch*.

This topic includes the following tasks:

Adding New Licenses

To add one or more new license keys on the switch, with the J-Web license manager:

1. In the J-Web interface, select **Maintain** > **Licenses**.
2. Under Installed Licenses, click **Add** to add a new license key or keys.
3. Do *one* of the following, using a blank line to separate multiple license keys:
   - In the License File URL box, type the full URL to the destination file containing the license key or keys to be added.
   - In the License Key Text box, paste the license key text, in plain-text format, for the license to be added.
4. Click **OK** to add the license key or keys.

A list of features that use the license key is displayed. The table also lists the ID, state, and version of the license key.

Deleting Licenses

To delete one or more license keys from a switch with the J-Web license manager:

1. In the J-Web interface, select **Maintain** > **Licenses**.
2. Select the check box of the license or licenses you want to delete.
3. Click **Delete**.

Displaying License Keys

To display the license keys installed on a switch with the J-Web license manager:

1. In the J-Web interface, select **Maintain** > **Licenses**.
2. Under Installed Licenses, click **Display Keys** to display all the license keys installed on the switch.

A screen displaying the license keys in text format appears. Multiple licenses are separated by a blank line.

Downloading Licenses

To download the license keys installed on the switch with the J-Web license manager:

1. In the J-Web interface, select **Maintain** > **Licenses**.
2. Under Installed Licenses, click **Download Keys** to download all the license keys installed on the switch to a single file.
3. Select **Save it to disk** and specify the file to which the license keys are to be written. You can also download the license file to your system.

Registering the EX Series Switch with the J-Web Interface

NOTE: This topic applies only to the J-Web Application package.

You can register your EX Series switch with the J-Web interface so that you can request technical assistance as and when required. To register an EX Series switch:

1. In the J-Web interface, select **Maintain** > **Customer Support** > **Product Registration**. For an EX8200 Virtual Chassis configuration, select the member from the list.

   Note the serial number that is displayed.
2. Click **Register**. Enter the serial number in the page that is displayed.

RELATED DOCUMENTATION

EX Series Switch Software Features Overview

Generating Support Information Reports for EX Series Switches Using the J-Web Interface

NOTE: This topic applies only to the J-Web Application package.

For requesting technical support for EX Series switches, you can either contact the Juniper Networks Technical Assistance Center (JTAC) or raise an online request on the Customer Support Center (CSC) portal at https://www.juniper.net/customers/support/ for quick and easy problem resolution. You can generate the support information report for your device before requesting technical support and include this information with your request for technical support. This information helps the technical assistance providers in identifying your system setup and diagnosing the problem.

To generate the support information report for your switch:

1. In the J-Web interface, select **Maintain** > **Customer Support** > **Support Information**. For a Virtual Chassis configuration, select a member from the list.

   The Support Information page displays the general information about the switch, such as software version, chassis information, and configuration.
2. To obtain the support information for your device, click **Generate Report** to obtain a local copy of the support information report.

With the support information generated, you can access the CSC portal to view a list of the support options available to you, or you can open a case online using CSC's Case Management tool.

JTAC policies—For understanding JTAC procedures and policies, use the JTAC User Guide located at https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf .

RELATED DOCUMENTATION

- EX Series Switch Software Features Overview

CHAPTER 15

Virtual Chassis Configuration

IN THIS CHAPTER

- Configuring a Virtual Chassis on an EX Series Switch (J-Web Procedure) | 221

Configuring a Virtual Chassis on an EX Series Switch (J-Web Procedure)

IN THIS SECTION

- Configuring an EX2200, EX2200-C, EX3300, EX4100, EX4100-F, EX4100-H, EX4200, EX4400, EX4500, or EX4550 Virtual Chassis (J-Web Procedure) | 221
- Enabling Virtual Chassis Mode on an EX8200 Switch (J-Web Procedure) | 225
- Configuring an EX8200 Virtual Chassis (J-Web Procedure) | 225

Configuring an EX2200, EX2200-C, EX3300, EX4100, EX4100-F, EX4100-H, EX4200, EX4400, EX4500, or EX4550 Virtual Chassis (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

To take advantage of the scalability features of EX2200, EX2200-C, EX3300, EX4100, EX4100-F, EX4200, EX4400, EX4500, and EX4550 switches, you can configure a Virtual Chassis. EX2200 and EX2200-C Virtual Chassis can include up to four member switches. EX3300 Virtual Chassis include up to six member switches. EX4100, EX4100-F, EX4100-H, EX4200, EX4400, EX4500, and EX4550 Virtual Chassis can include up to 10 member switches. You can interconnect the member switches by using dedicated Virtual Chassis ports (VCPs). You do not have to configure the interface for the dedicated VCPs. If you want to interconnect member switches that are located in different racks or wiring closets, interconnect them using 10-gigabit ports (SFP+ uplink module ports or SFP+ network ports for EX4500) configured as VCPs. EX4550 switches support 10-gigabit (SFP+ expansion module ports) and 40-gigabit

(QSFP+ uplink module ports or fixed ports) Ethernet interface. See *Setting an Uplink Port on an EX Series or QFX Series Switch as a Virtual Chassis Port*.

NOTE: In EX4300-48MP switches, you can use only the built-in QSFP+ ports as VCPs to connect the switch in a Virtual Chassis. You cannot connect the ports on the uplink module in EX4300-48MP switches to Virtual Chassis ports (VCPs).

Starting in Junos OS 23.1R1 Release, J-Web supports EX 4400-24X switches.

Starting in Junos OS 23.2R1 Release, J-Web supports EX4400-EM-1C uplink module for EX4400 and EX4400-24X switches.

Starting in Junos OS Release 24.4R1, J-Web supports EX4100-H-12MP, EX4400-48XP, and EX4400-48MXP switches.

To configure a Virtual Chassis by using the J-Web interface:

1. Select **Configure** > **Virtual Chassis**.

   NOTE: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. The properties that you can configure are displayed.

   The first section of the Virtual Chassis Configuration page displays the Virtual Chassis member configuration. The display includes a list of member switches, their member IDs, and the primary-role priority.

   The second section displays the operational status of the Virtual Chassis configuration, member details, and the dedicated and the configured VCPs.

3. Enter information into the page as described in Table 81 on page 224.
4. Click one of the following options:
   - **Add**—To add a member's configuration to the Virtual Chassis configuration, click **Add**.
   - **Edit**—To modify an existing member's configuration, click **Edit**.
   - **Delete**—To delete the configuration of a member, click **Delete**.
5. To configure uplink ports on EX2200, EX2200-C, and EX3300 switches and uplink module ports on EX4100, EX4100-F, EX4200, EX4400, and EX4500 switches as VCPs , select the member in the Virtual Chassis members list and select **Action** > **Set Uplink Port as VCP**. Select the port from the list.

On EX4550, EX4400-48XP, EX4400-48MXP, and EX4100-H switches, to configure a VCP, select the member in the Virtual Chassis members list and select **Action** > **Set Port as VCP**. Select the port from the list.

On EX4400-24X switches, to configure a VCP, do the following:

a. Select the member in the Virtual Chassis members list and select **Action**>**Set Mode**.

   Set Mode as VCP window opens.

b. Select mode as **HGOE**.

   NOTE: You must reboot to set the HGOE mode, and then proceed with the VCP configuration.

c. Select **Reboot**.

d. Click **OK**.

6. To remove the VCP configuration from the uplink ports on EX2200, EX2200-C, and EX3300 switches and uplink module ports on EX4100, and EX4100-F, EX4200, EX4400, and EX4500 switches , select the member in the Virtual Chassis members list and select **Action** > **Delete Uplink Port as VCP**.

   On EX4550, EX4400-48XP, EX4400-48MXP, and EX4100-H switches, to remove the VCP configuration from the port of a member, select the member in the Virtual Chassis members list and select **Action** > **Delete Port as VCP**.

   On EX4400-24X switches, to delete a VCP, do the following:

   a. Select the member in the Virtual Chassis members list and select **Action** > **Delete Mode**.

      Delete Mode as VCP window opens.

      NOTE: You must reboot to delete HGOE mode.

   b. Select **Reboot**.

   c. Click **OK**.

Table 82 on page 224 provides the field details of the Set or Delete Mode as VCP window on Virtual Chassis Configuration page.

Table 81: Virtual Chassis Configuration Fields

Field	Function	Your Action
Member Details		
Member ID	Specifies the identifier for the member switch.	Select an identifier (from **0** through **9**) from the list. **NOTE**: For EX2200 Virtual Chassis, you can select the member ID (from **0** through **3**) from the list.
Priority	Specifies the primary-role priority to be assigned to the member.	Select a number from **1** through **255**, (255 being the highest priority and **128**, the default).
Disable Management VLAN	If you want to reserve an individual member's management Ethernet port, you can remove that port from being part of the virtual management Ethernet (VME) interface.	Click to disable the management VLAN on the port.
Refresh	Refreshes the operational status of Virtual Chassis members.	Click to refresh the operational status.

Table 82: Set or Delete Mode as VCP Fields

Field	Action
Mode	Use HGOE mode to configure VCP on the switch.
All-members	Use All-members to set virtual chassis mode on all the virtual chassis members.
Reboot	Select Reboot to reboot system after changing mode.

Enabling Virtual Chassis Mode on an EX8200 Switch (J-Web Procedure)

Using the J-Web interface, you can enable Virtual Chassis mode on an EX8200 switch. To enable Virtual Chassis mode:

1. Select **Configure > Virtual Chassis**. The Virtual Chassis page displays the serial number of the member switch. You need the serial number while preprovisioning the Virtual Chassis.
2. Click **Enable Virtual Chassis**.

Configuring an EX8200 Virtual Chassis (J-Web Procedure)

IN THIS SECTION

- Preprovision the Virtual Chassis | **225**
- Configure Virtual Chassis Members | **226**
- Configure Virtual Chassis Ports | **226**

Using the J-Web interface, you can configure an EX8200 Virtual Chassis to include up to four EX8200 switches and one or two XRE200 External Routing Engines. You interconnect the member switches by connecting the management ports to the external Routing Engines, whose ports automatically function as Virtual Chassis ports (VCPs). A VCP is any port whose function is to send and receive Virtual Chassis Control Protocol (VCCP) traffic to create, monitor, and maintain the Virtual Chassis. VCPs also carry data traffic through the Virtual Chassis.

The EX8200 Virtual Chassis wizard helps to preprovision Virtual Chassis members and to configure Virtual Chassis ports.

To configure an EX8200 Virtual Chassis, select **Configure > Virtual Chassis**. The Virtual Chassis wizard is displayed. You can:

Preprovision the Virtual Chassis

If the Virtual Chassis has not been preprovisioned:

1. Select **Preprovision Virtual Chassis**. The prerequisites page is displayed.
2. Ensure that the following prerequisites are met:
   - The same version of Junos OS is running on all XRE200 Routing Engines and switches.
   - Virtual Chassis mode has been enabled on each EX8200 switch.
   - The XRE200 Routing Engines and switches have been cabled and connected.

Click **Next**. The Configure Virtual Chassis Members screen is displayed.

Configure Virtual Chassis Members

When you click **Configure Virtual Chassis Members** in the wizard, you can add a Virtual Chassis member, modify an existing Virtual Chassis member configuration, or delete the Virtual Chassis configuration for an existing member.

To add a Virtual Chassis member, click **Add**. For each member, specify:

- **Member ID**—The identifier for the member switch or the XRE200 External Routing Engine.
- **Serial Number**—The serial number of the member switch or the XRE200 External Routing Engine.
- **Management VLAN**—Click to enable or disable the management VLAN on the port.
- **Location**—A description of the location of the EX8200 member switch or external Routing Engine.
- **Role**—The role to be performed by each EX8200 member switch or each XRE200 External Routing Engine. EX8200 switches must be in the linecard role and XRE200 External Routing Engines must be in the Routing Engine role.

To edit an existing member configuration, click **Edit**.

NOTE: If you are editing an existing member configuration, you can modify only the Management VLAN option and the location of the Virtual Chassis member.

Click **Remove** to delete the Virtual Chassis configuration for an existing member.

Configure Virtual Chassis Ports

To configure Virtual Chassis ports that are needed between the switches for data traffic, select the **Configure Virtual Chassis Ports** option in the wizard.

NOTE: All XRE200 ports, the vcp-0/0 port, and any port on a Virtual Chassis Control Interface (VCCI) module are automatically VCPs. You need not configure these ports as VCPs.

1. Select the member from the list. The switch model, serial number, available ports, and configured ports are displayed. Select **All** to view details of available ports and configured ports of all the members.

NOTE: Only members with active EX8200-8XS line cards are listed. The J-Web interface does not support EX8200-2X4F40TE/PE line cards.

2. To convert network ports to Virtual Chassis ports or to convert Virtual Chassis ports to network ports, click the appropriate arrow.
3. Click **Next**. The Summary page displays the configuration changes. You can edit the configuration.

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
14.1X53-D10	For Junos OS Release 14.1X53-D10 and later, EX3300 Virtual Chassis include up to 10 member switches.

RELATED DOCUMENTATION

- *Configuring an EX4200, EX4500, or EX4550 Virtual Chassis (CLI Procedure)*
- *Setting an Uplink Port as a Virtual Chassis Port on an EX4500 or EX4550 Switch (CLI Procedure)*
- *Example: Configuring an EX4200 Virtual Chassis with a Primary and Backup in a Single Wiring Closet*
- *Example: Configuring an EX4200 Virtual Chassis Interconnected Across Multiple Wiring Closets*
- *Monitoring the Virtual Chassis Status and Statistics on EX Series Virtual Chassis*
- *Virtual Chassis Cabling Configuration Examples for EX4200 Switches*
- *Understanding EX Series Virtual Chassis*
- *Configuring an EX8200 Virtual Chassis (CLI Procedure)*
- *Example: Setting Up a Full Mesh EX8200 Virtual Chassis with Two EX8200 Switches and Redundant XRE200 External Routing Engines*
- *Adding or Replacing a Member Switch or an External Routing Engine in an EX8200 Virtual Chassis (CLI Procedure)*
- *Verifying the Member ID, Role, and Neighbor Member Connections of an EX8200 Virtual Chassis Member*

3

PART

Monitoring

Monitoring Tasks | 229

CHAPTER 16

Monitoring Tasks

IN THIS CHAPTER

- Check Active Alarms with the J-Web Interface | **230**
- Monitor System Log Messages | **231**
- Monitoring Chassis Information | **238**
- Monitoring System Properties | **241**
- Monitoring System Process Information | **245**
- Monitoring Switch Control Traffic | **246**
- Monitoring Interface Status and Traffic | **250**
- Monitoring PoE | **252**
- Monitoring Hosts Using the J-Web Ping Host Tool | **254**
- Monitoring Network Traffic Using Traceroute | **257**
- Monitoring DHCP Services | **259**
- Monitoring OSPF Routing Information | **264**
- Monitoring RIP Routing Information | **269**
- Monitoring BGP Routing Information | **271**
- Monitoring Routing Information | **275**
- Monitoring Ethernet Switching on EX Series Switches (J-Web) | **278**
- Monitoring IGMP Snooping | **281**
- Monitoring Spanning Tree Protocols on Switches | **282**
- Monitoring CoS Classifiers | **286**
- Monitoring CoS Drop Profiles | **288**
- Monitoring CoS Value Aliases | **290**
- Monitoring CoS Forwarding Classes | **291**
- Monitoring Interfaces That Have CoS Components | **294**
- Monitoring CoS Rewrite Rules | **296**
- Monitoring CoS Scheduler Maps | **298**
- Monitoring the Virtual Chassis Status and Statistics on EX Series Virtual Chassis | **301**

- Monitoring 802.1X Authentication | 303
- Monitoring Port Security | 304

Check Active Alarms with the J-Web Interface

IN THIS SECTION

- Purpose | 230
- Action | 230
- Meaning | 231

Purpose

NOTE: This topic applies only to the J-Web Application package.

Use the monitoring functionality to view alarm information for the EX Series switches including alarm type, alarm severity, and a brief description for each active alarm on the switching platform.

Action

To view the active alarms:

1. Select **Monitor** > **Events and Alarms** > **View Alarms** in the J-Web interface.
2. Select an alarm filter based on alarm type, severity, description, and date range.
3. Click **Go**.

   All the alarms matching the filter are displayed.

NOTE: When the switch is reset, the active alarms are displayed.

Meaning

Table 83 on page 231 lists the alarm output fields.

Table 83: Summary of Key Alarm Output Fields

Field	Values
Type	Category of the alarm: • Chassis—Indicates an alarm condition on the chassis (typically an environmental alarm such as one related to temperature). • System—Indicates an alarm condition in the system.
Severity	Alarm severity—either major (red) or minor (yellow or amber).
Description	Brief synopsis of the alarm.
Time	Date and time when the failure was detected.

RELATED DOCUMENTATION

Monitor System Log Messages

Dashboard for EX Series Switches

Understand Alarm Types and Severity Levels on EX Series Switches

Monitor System Log Messages

IN THIS SECTION

- Purpose | 232
- Action | 232
- Meaning | 235

Purpose

NOTE: This topic applies only to the J-Web Application package.

Use the monitoring functionality to filter and view system log messages for EX Series switches.

Action

To view events in the J-Web interface, select **Monitor** > **Events and Alarms** > **View Events**.

Apply a filter or a combination of filters to view messages. You can use filters to display relevant events. Table 84 on page 232 describes the different filters, their functions, and the associated actions.

To view events in the CLI, enter the following command:

```
show log
```

Table 84: Filtering System Log Messages

Field	Function	Your Action
System Log File	Specifies the name of a system log file for which you want to display the recorded events. Lists the names of all the system log files that you configure. By default, a log file, `messages`, is included in the `/var/log/` directory.	To specify events recorded in a particular file, select the system log filename from the list— for example, **messages**. Select **Include archived files** to include archived files in the search.
Process	Specifies the name of the process generating the events you want to display. To view all the processes running on your system, enter the CLI command `show system processes`. For more information about processes, see the *Junos OS Installation and Upgrade Guide*.	To specify events generated by a process, type the name of the process. For example, type `mgd` to list all messages generated by the management process.

Table 84: Filtering System Log Messages *(Continued)*

Field	Function	Your Action
Date From To	Specifies the time period in which the events you want displayed are generated. Displays a calendar that allows you to select the year, month, day, and time. It also allows you to select the local time. By default, the messages generated during the last one hour are displayed. End Time shows the current time and Start Time shows the time one hour before End Time.	To specify the time period: • Click the **Calendar** icon and select the year, month, and date— for example, **02/10/2007**. • Click the **Calendar** icon and select the year, month, and date— for example, **02/10/2007**. • Click to select the time in hours, minutes, and seconds.
Event ID	Specifies the event ID for which you want to display the messages. Allows you to type part of the ID and completes the remainder automatically. An event ID, also known as a system log message code, uniquely identifies a system log message. It begins with a prefix that indicates the generating software process or library.	To specify events with a specific ID, type the partial or complete ID— for example, **TFTPD_AF_ERR**.
Description	Specifies text from the description of events that you want to display. Allows you to use regular expressions to match text from the event description. **NOTE**: Regular expression matching is case-sensitive.	To specify events with a specific description, type a text string from the description with regular expression. For example, type **^Initial*** to display all messages with lines beginning with the term *Initial*.
Search	Applies the specified filter and displays the matching messages.	To apply the filter and display messages, click **Search**.
Reset	Resets all the fields in the Events Filter box.	To reset the field values that are listed in the Events Filter box, click **Reset**.

Table 84: Filtering System Log Messages *(Continued)*

Field	Function	Your Action
Generate Raw Report **NOTE**: • Starting in Junos OS Release 14.1X53, a Raw Report can be generated from the log messages being loaded in the Events Detail table. The Generate Raw Report button is enabled after the event log messages start loading in the Events Detail table. • After the log messages are completely loaded in the Events Detail table, Generate Raw Report changes to Generate Report.	Generates a list of event log messages in nontabular format.	To generate a raw report: 1. Click **Generate Raw Report**. The *Opening filteredEvents.html* window appears. 2. Select **Open with** to open the HTML file or select **Save File** to save the file. 3. Click **OK**.

Table 84: Filtering System Log Messages *(Continued)*

Field	Function	Your Action
Generate Report **NOTE**: Starting in Junos OS Release 14.1X53, a Formatted Report can be generated from event log messages being loaded in an Events Detail table. The Generate Report button appears only after event log messages are completely loaded in the Events Detail table. The Generate Raw Report button is displayed while event log messages are being loaded.	Generates a list of event log messages in tabular format, which shows system details, events filter criteria, and event details.	To generate a formatted report: 1. Click **Generate Report**. The *Opening Report.html* window appears. 2. Select **Open with** to open the HTML file or select **Save File** to save the file. 3. Click **OK**.

Meaning

Table 85 on page 236 describes the Event Summary fields.

NOTE: By default, the View Events page in the J-Web interface displays the most recent 25 events, with severity levels highlighted in different colors. After you specify the filters, Event Summary displays the events matching the specified filters. Click the **First**, **Next**, **Prev**, and **Last** links to navigate through messages.

Table 85: Viewing System Log Messages

Field	Function	Additional Information
Process	Displays the name and ID of the process that generated the system log message.	The information displayed in this field is different for messages generated on the local Routing Engine than for messages generated on another Routing Engine (on a system with two Routing Engines installed and operational). Messages from the other Routing Engine also include the identifiers **re0** and **re1** that identify the Routing Engine.
Severity	Severity level of a message is indicated by different colors. • **Unknown**—Gray—Indicates no severity level is specified. • **Debug/Info/Notice**—Green—Indicates conditions that are not errors but are of interest or might warrant special handling. • **Warning**—Yellow or Amber—Indicates conditions that warrant monitoring. • **Error**—Blue—Indicates standard error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels. • **Critical**—Pink—Indicates critical conditions, such as hard-drive errors. • **Alert**—Orange—Indicates conditions that require immediate correction, such as a corrupted system database. • **Emergency**—Red—Indicates system panic or other conditions that cause the switch to stop functioning.	A severity level indicates how seriously the triggering event affects switch functions. When you configure a location for logging a facility, you also specify a severity level for the facility. Only messages from the facility that are rated at that level or higher are logged to the specified file.

Table 85: Viewing System Log Messages *(Continued)*

Field	Function	Additional Information
Event ID	Displays a code that uniquely identifies the message. The prefix on each code identifies the message source, and the rest of the code indicates the specific event or error.	The event ID begins with a prefix that indicates the generating software process. Some processes on a switch do not use codes. This field might be blank in a message generated from such a process. An event can belong to one of the following type categories: • **Error**—Indicates an error or failure condition that might require corrective action. • **Event**—Indicates a condition or occurrence that does not generally require corrective action.
Event Description	Displays a more detailed explanation of the message.	
Time	Displays the time at which the message was logged.	

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
14.1X53	Starting in Junos OS Release 14.1X53, a Raw Report can be generated from the log messages being loaded in the Events Detail table.
14.1X53	Starting in Junos OS Release 14.1X53, a Formatted Report can be generated from event log messages being loaded in an Events Detail table.

RELATED DOCUMENTATION

Check Active Alarms with the J-Web Interface

Understand Alarm Types and Severity Levels on EX Series Switches

Monitoring Chassis Information

IN THIS SECTION

- Purpose | 238
- Action | 238
- Meaning | 238

Purpose

NOTE: This topic applies only to the J-Web Application package.

Use the monitoring functionality to view chassis properties such as general switch information, temperature and fan status, and resource information for the EX Series switch.

Action

To view chassis properties in the J-Web interface, select **Monitor** > **System View** > **Chassis Information**. For an EX8200 Virtual Chassis configuration, select the Virtual Chassis member from the list.

To view chassis properties in the CLI, enter the following commands:

- `show chassis environment`
- `show chassis fpc`
- `show chassis hardware`

Meaning

Table 86 on page 239 gives information about the key output fields for chassis information.

NOTE: For an EX2200, EX2200-C, EX3200, or EX4500 switch or an EX4200 or EX4550 standalone switch, the FPC slot number refers to the switch itself and is always 0. In a Virtual Chassis configuration, the FPC slot number refers to the member ID.

Table 86: Summary of the Key Output Fields for Chassis Information

Field	Values
Routing Engine Details	Select the **Master** tab to view details about the primary Routing Engine or select **Backup** to view details about the backup Routing Engine.
Name/Value	This table displays the following details of the primary Routing Engine: • Routing Engine module • Model • Version • Part number • Serial number • Memory utilization • Temperature • Start time • CPU load average for 1, 5, and 15 minutes
Power and Fan Tray Details	
Power	Select the **Power** tab to view details of the power supplies.
Name/Value	Displays the status and model number of each power supply.
Fan	Select the **Fan** tab to view details about the fans.
Name/Value	Displays the status of each fan in the corresponding FPC.

Table 86: Summary of the Key Output Fields for Chassis Information *(Continued)*

Field	Values
Chassis Component Details	
Select component	Select an FPC to view general, temperature, resource, and subcomponent details.
General	Select the **General** tab to view the general information about the chassis components.
Name/Value	Displays general information: • Version—Revision level. Supply the version number when reporting hardware problems to customer support. • Part number • Serial number—Supply the serial number when contacting customer support about the switch chassis. • Description—Brief text description.
Temperature	Select the **Temperature** tab to view the temperature details of the components in the selected FPC.
Name/Value	Displays the temperature details of the sensors present in the selected FPC.
Resource	Select the **Resource** tab to view the resource details of the selected FPC.

Table 86: Summary of the Key Output Fields for Chassis Information *(Continued)*

Field	Values

Name/Value	Displays resource details:
	• State:
	  • **Dead**—Held in reset because of errors.
	  • **Diag**—The FPC is running diagnostics.
	  • **Dormant**—Held in reset.
	  • **Empty**—No FPC is present.
	  • **Online**—The FPC is online and running.
	  • **Probed**—Probe is complete. The FPC is awaiting restart of the Packet Forwarding Engine.
	  • **Probe-wait**—The FPC is waiting for the probe operation to start.
	• **Total CPU DRAM**—Total DRAM, in megabytes, available to the FPC.
	• **Start time**—Date and time the switch was last rebooted.

RELATED DOCUMENTATION

Monitoring System Process Information | 245

Monitoring System Properties | 241

Dashboard for EX Series Switches

Monitoring System Properties

IN THIS SECTION

Purpose | 242

Action | 242
Meaning | 242

Purpose

NOTE: This topic applies only to the J-Web Application package.

Use the monitoring functionality to view system properties such as the name and IP address of the switch and resource usage.

Action

To monitor system properties in the J-Web interface, select **Monitor** > **System View** > **System Information**.

To monitor system properties in the CLI, enter the following commands:

- `show system uptime`
- `show system users`
- `show system storage`

Meaning

Table 87 on page 242 summarizes key output fields in the system properties display.

Table 87: Summary of Key System Properties Output Fields

Field	Values	Additional Information
General Information		
Serial Number	Serial number for the switch.	

Table 87: Summary of Key System Properties Output Fields *(Continued)*

Field	Values	Additional Information
Junos OS Version	Version of Junos OS active on the switch.	
Hostname	The name of switch.	
IP Address	The IP address of the switch.	
Loopback Address	The loopback address.	
Domain Name Server	The address of the domain name server.	
Time Zone	The time zone on the switch.	
Time		
Current Time	Current system time, in Coordinated Universal Time (UTC).	
System Booted Time	Date and time when the switch was last booted and how long it has been running.	
Protocol Started Time	Date and time when the switching protocols were last started and how long they have been running.	

Table 87: Summary of Key System Properties Output Fields *(Continued)*

Field	Values	Additional Information
Last Configured Time	Date and time when a configuration was last committed. This field also shows the name of the user who issued the last `commit` command, through either the J-Web interface or the CLI.	
Load Average	The CPU load average for 1, 5, and 15 minutes.	
Storage Media		
Internal Flash Memory	Memory usage details of internal flash.	
External Flash Memory	Usage details of external flash memory.	
Logged in Users Details		
User	Username of any user logged in to the switching platform.	
Terminal	Terminal through which the user is logged in.	
From	System from which the user has logged in. A hyphen indicates that the user is logged in through the console.	
Login Time	Time when the user logged in.	This is the **LOGIN@** field in `show system users` command output.
Idle Time	How long the user has been idle.	

RELATED DOCUMENTATION

Monitoring System Process Information | 245

Understanding J-Web User Interface Sessions | 14

Monitoring System Process Information

IN THIS SECTION

- Purpose | 245
- Action | 245
- Meaning | 245

Purpose

NOTE: This topic applies only to the J-Web Application package.

Use the monitoring functionality to view the processes running on the switch.

Action

To view the software processes running on the switch in the J-Web interface, select **Monitor** > **System View** > **Process Details**.

To view the software processes running on the switch in the CLI, enter the following command.

```
show system processes
```

Meaning

Table 88 on page 246 summarizes the output fields in the system process information display.

The display includes the total CPU load and total memory utilization.

Table 88: Summary of System Process Information Output Fields

Field	Values
PID	Identifier of the process.
Name	Owner of the process.
State	Current state of the process.
CPU Load	Percentage of the CPU that is being used by the process.
Memory Utilization	Amount of memory that is being used by the process.
Start Time	Time of day when the process started.

RELATED DOCUMENTATION

Monitoring System Properties | 241

show system uptime

Monitoring Switch Control Traffic

IN THIS SECTION

- Purpose | 247
- Action | 247
- Meaning | 247

Purpose

NOTE: This topic applies only to the J-Web Application package.

Use the packet capture feature when you need to quickly capture and analyze switch control traffic on a switch. The packet capture feature allows you to capture traffic destined for or originating from the Routing Engine.

Action

To use the packet capture feature in the J-Web interface, select **Troubleshoot** > **Packet Capture**.

To use the packet capture feature in the CLI, enter the following CLI command:

monitor traffic

Meaning

You can use the packet capture feature to compose expressions with various matching criteria to specify the packets that you want to capture. You can decode and view the captured packets in the J-Web interface as they are captured. The packet capture feature does not capture transient traffic.

Table 89: Packet Capture Field Summary

Field	Function	Your Action
Interface	Specifies the interface on which the packets are captured. If you select default, packets on the Ethernet management port 0, are captured.	From the list, select an interface—for example, **ge-0/0/0**.
Detail level	Specifies the extent of details to be displayed for the packet headers. • Brief—Displays the minimum packet header information. This is the default. • Detail—Displays packet header information in moderate detail. • Extensive—Displays the maximum packet header information.	From the list, select **Detail**.

Table 89: Packet Capture Field Summary *(Continued)*

Field	Function	Your Action
Packets	Specifies the number of packets to be captured. Values range from **1** to **1000**. Default is **10**. Packet capture stops capturing packets after this number is reached.	From the list, select the number of packets to be captured—for example, 10.
Addresses	Specifies the addresses to be matched for capturing the packets using a combination of the following parameters: • Direction—Matches the packet headers for IP address, hostname, or network address of the source, destination or both. • Type—Specifies if packet headers are matched for host address or network address. You can add multiple entries to refine the match criteria for addresses.	Select address-matching criteria. For example: 1. From the Direction list, select **source**. 2. From the Type list, select **host**. 3. In the Address box, type **10.1.40.48**. 4. Click **Add**.
Protocols	Matches the protocol for which packets are captured. You can choose to capture TCP, UDP, or ICMP packets or a combination of TCP, UDP, and ICMP packets.	From the list, select a protocol—for example, **tcp**.
Ports	Matches packet headers containing the specified source or destination TCP or UDP port number or port name.	Select a direction and a port. For example: • From the Type list, select **src**. • In the Port box, type **23**.
Advanced Options		
Absolute TCP Sequence	Specifies that absolute TCP sequence numbers are to be displayed for the packet headers.	To display absolute TCP sequence numbers in the packet headers, select this check box.

Table 89: Packet Capture Field Summary *(Continued)*

Field	Function	Your Action
Layer 2 Headers	Specifies that link-layer packet headers are to be displayed.	To include link-layer packet headers while capturing packets, select this check box.
Non-Promiscuous	Specifies not to place the interface in promiscuous mode, so that the interface reads only packets addressed to it. In promiscuous mode, the interface reads every packet that reaches it.	To read all packets that reach the interface, select this check box.
Display Hex	Specifies that packet headers, except link-layer headers, are to be displayed in hexadecimal format.	To display the packet headers in hexadecimal format, select this check box.
Display ASCII and Hex	Specifies that packet headers are to be displayed in hexadecimal and ASCII format.	To display the packet headers in ASCII and hexadecimal formats, select this check box.
Header Expression	Specifies the match condition for the packets to be captured. The match conditions you specify for Addresses, Protocols, and Ports are displayed in expression format in this field.	You can enter match conditions directly in this field in expression format or modify the expression composed from the match conditions you specified for Addresses, Protocols, and Ports. If you change the match conditions specified for Addresses, Protocols, and Ports again, packet capture overwrites your changes with the new match conditions.
Packet Size	Specifies the number of bytes to be displayed for each packet. If a packet header exceeds this size, the display is truncated for the packet header. The default value is 96 bytes.	Type the number of bytes you want to capture for each packet header—for example, **256**.
Don't Resolve Addresses	Specifies that IP addresses are not to be resolved into hostnames in the packet headers displayed.	To prevent packet capture from resolving IP addresses to hostnames, select this check box.

Table 89: Packet Capture Field Summary *(Continued)*

Field	Function	Your Action
No Timestamp	Suppresses the display of packet header timestamps.	To stop displaying timestamps in the captured packet headers, select this check box.
Write Packet Capture File	Writes the captured packets to a file in PCAP format in /var/tmp. The files are named with the prefix jweb-pcap and the extension .pcap. If you select this option, the decoded packet headers are not displayed on the packet capture page.	To decode and display the packet headers on the J-Web page, clear this check box.

RELATED DOCUMENTATION

Using the J-Web CLI Terminal | 62

Monitoring Interface Status and Traffic

IN THIS SECTION

- Purpose | 250
- Action | 251
- Meaning | 252

Purpose

NOTE: This topic applies only to the J-Web Application package.

Use the monitoring functionality to view interface status or to monitor interface bandwidth utilization and traffic statistics on the EX Series switches.

The J-Web interface monitors interface bandwidth utilization and plots real-time charts to display input and output rates in bytes per second. In addition, the Interface monitoring page displays input and output packet counters and error counters in the form of charts.

Alternatively, you can enter the `show` commands in the CLI to view interface status and traffic statistics.

NOTE: For logical interfaces on EX Series switches, the traffic statistics fields in **show interfaces** commands show only control traffic; the traffic statistics do not include data traffic.

NOTE: EX Series switches do not support the collection and reporting of IPv6 transit statistics. Therefore, the `IPv6 transit statistics` field in the `show interfaces` commands displays all values as `0`.

Action

To view general interface information in the J-Web interface such as available interfaces, select **Monitor** > **Interfaces**. Click any interface to view details about its status.

To set up interface monitoring for Virtual Chassis and EX8200 switches, select a member from the **Port for Member** list. Details such as the admin status and link status are displayed in the table. For an EX8200 Virtual Chassis setup, select the member, **FPC**, and the required interface.

NOTE: By default, the details of the first member in the **FPC** list is displayed. In an EX8200 Virtual Chassis setup, details of the first member and the first **FPC** is displayed.

You have the following options:

- **Start/Stop**—Starts or stops monitoring the selected interface.
- **Show Graph**—Displays input and output packet counters and error counters in the form of charts. Click the pop-up icon to view the graph in a separate window.
- **Details**—Displays interface information such as general details, traffic statistics, I/O errors, CoS counters, and Ethernet statistics.
- **Refresh Interval (sec)**—Displays the time interval you have set for page refresh.
- **Clear Statistics**—Clears the statistics for the interface selected from the table.

Using the CLI:

- To view interface status for all the interfaces, enter **show interfaces xe**.

- To view status and statistics for a specific interface, enter **show interfaces xe-*interface-name***.
- To view status and traffic statistics for all interfaces, enter either **show interfaces xe detail** or **show interfaces xe extensive**.

Meaning

In the J-Web interface the charts displayed are:

- Bar charts—Display the input and output error counters.
- Pie charts—Display the number of broadcast, unicast, and multicast packet counters.

For details about output from the CLI commands, see **show interfaces ge-** (Gigabit Ethernet) or **show interfaces xe-** (10-Gigabit Ethernet).

RELATED DOCUMENTATION

Configuring Gigabit Ethernet Interfaces (J-Web Procedure) | **139**

Configuring Gigabit Ethernet Interfaces (CLI Procedure)

Configuring Gigabit Ethernet Interfaces for EX Series Switches with ELS support

Monitoring PoE

IN THIS SECTION

Purpose | **252**

Action | **253**

Meaning | **253**

Purpose

NOTE: This topic applies only to the J-Web Application package.

Use the monitoring functionality to view real-time data of the power consumed by each PoE interface, and to enable and configure telemetry values. When telemetry is enabled, the software measures the power consumed by each interface and stores the data for future reference.

NOTE: If you are configuring a Virtual Chassis, the PoE monitoring option is displayed if any member of the Virtual Chassis supports PoE, even if the Virtual Chassis primary does not support PoE.

Action

To monitor PoE by using the J-Web interface, select **Monitor** > **Power over Ethernet**.

To monitor PoE power consumption with CLI commands in the CLI Terminal in the J-Web interface:

1. Select **Troubleshoot** > **CLI Terminal**.
2. Type any of the following CLI commands:
   - **show poe controller**
   - **show poe interface**
   - **show poe telemetries**

For detailed information about using these CLI commands to monitor PoE power consumption, see *Monitoring and Troubleshooting PoE*.

Meaning

In the J-Web interface the PoE Monitoring screen is divided into two parts. The top half of the screen displays real-time data of the power consumed by each PoE-capable interface and a list of ports that utilize maximum power.

Select a particular interface to view a graph of the power consumed by the selected interface.

The bottom half of the screen displays telemetry information for interfaces. The Telemetry Status field displays whether telemetry has been enabled on the interface. Click the **Show Graph** button to view a graph of the telemetries. The graph can be based on power or voltage. To modify telemetry values, click **Edit**. Specify Interval in minutes, Duration in hours, and select **Log Telemetries** to enable telemetry on the selected interface.

RELATED DOCUMENTATION

Monitoring and Troubleshooting PoE

Monitoring Hosts Using the J-Web Ping Host Tool

IN THIS SECTION

- Purpose | 254
- Action | 254
- Meaning | 255

Purpose

NOTE: This topic applies only to the J-Web Application package.

Use the J-Web ping host tool to verify that the host can be reached over the network. The output is useful for diagnosing host and network connectivity problems. The switch sends a series of ICMP echo (ping) requests to a specified host and receives ICMP echo responses.

Action

To use the J-Web ping host tool:

1. Select **Troubleshoot>Ping Host**.
2. Next to Advanced options, click the expand icon.
3. Enter information into the Ping Host page, as described in Table 90 on page 255.

   The Remote Host field is the only required field.
4. Click **Start**.

The results of the ping operation are displayed in the main pane . If no options are specified, each ping response is in the following format:

```
                    bytes bytes from ip-address: icmp_seq=number ttl=number
time=time
```

5. To stop the ping operation before it is complete, click **OK**.

Meaning

Table 90 on page 255 lists the fields.

Table 90: J-Web Ping Host Field Summary

Field	Function	Your Action
Remote Host	Identifies the host to ping.	Type the hostname or IP address of the host to ping.
Advanced Options		
Don't Resolve Addresses	Determines whether to display hostnames of the hops along the path.	• To suppress the display of the hop hostnames, select the check box. • To display the hop hostnames, clear the check box.
Interface	Specifies the interface on which the ping requests are sent.	Select the interface on which ping requests are sent from the list. If you select **any**, the ping requests are sent on all interfaces.
Count	Specifies the number of ping requests to send.	Select the number of ping requests to send from the list.
Don't Fragment	Specifies the Don't Fragment (DF) bit in the IP header of the ping request packet.	• To set the DF bit, select the check box. • To clear the DF bit, clear the check box.

Table 90: J-Web Ping Host Field Summary *(Continued)*

Field	Function	Your Action
Record Route	Sets the record route option in the IP header of the ping request packet. The path of the ping request packet is recorded within the packet and displayed in the main pane.	• To record and display the path of the packet, select the check box. • To suppress the recording and display of the path of the packet, clear the check box.
Type-of-Service	Specifies the type-of-service (TOS) value in the IP header of the ping request packet.	Select the decimal value of the TOS field from the list.
Routing Instance	Name of the routing instance for the ping attempt.	Select the routing instance name from the list.
Interval	Specifies the interval, in seconds, between transmissions of individual ping requests.	Select the interval from the list.
Packet Size	Specifies the size of the ping request packet.	Type the size, in bytes, of the packet. The size can be from 0 through 65468. The switch adds 8 bytes of ICMP header to the size.
Source Address	Specifies the source address of the ping request packet.	Type the source IP address.
Time-to-Live	Specifies the time-to-live (TTL) hop count for the ping request packet.	Select the TTL value from the list.
Bypass Routing	Determines whether ping requests are routed by means of the routing table. If the routing table is not used, ping requests are sent only to hosts on the interface specified in the Interface box. If the host is not on that interface, ping responses are not sent.	• To bypass the routing table and send the ping requests to hosts on the specified interface only, select the check box. • To route the ping requests using the routing table, clear the check box.

RELATED DOCUMENTATION

Monitoring Interface Status and Traffic | 250

Monitoring Network Traffic Using Traceroute

IN THIS SECTION

- Purpose | 257
- Action | 257
- Meaning | 258

Purpose

NOTE: This topic applies only to the J-Web Application package.

Use the Traceroute page in the J-Web interface to trace a route between the switch and a remote host. You can use a traceroute task to display a list of waypoints between the switch and a specified destination host. The output is useful for diagnosing a point of failure in the path from the switch platform to the destination host and addressing network traffic latency and throughput problems.

Action

To use the traceroute tool:

1. Select **Troubleshoot** > **Traceroute**.
2. Next to **Advanced options**, click the expand icon.
3. Enter information into the Traceroute page.

   The **Remote Host** field is the only required field.
4. Click **Start**.
5. To stop the traceroute operation before it is complete, click **OK** while the results of the traceroute operation are being displayed.

Meaning

The switch generates the list of waypoints by sending a series of ICMP traceroute packets in which the time-to-live (TTL) value in the messages sent to each successive waypoint is incremented by 1. (The TTL value of the first traceroute packet is set to 1.) In this manner, each waypoint along the path to the destination host replies with a Time Exceeded packet from which the source IP address can be obtained.

The results of the traceroute operation are displayed in the main pane. If no options are specified, each line of the traceroute display is in the following format:

hop-number host (ip-address) [as-number] time1 time2 time3

The switch sends a total of three traceroute packets to each waypoint along the path and displays the round-trip time for each traceroute operation. If the switch times out before receiving a **Time Exceeded** message, an asterisk (*) is displayed for that round-trip time.

Table 91: Traceroute field summary

Field	Function	Your Action
Remote Host	Identifies the destination host of the traceroute.	Type the hostname or IP address of the destination host.
Advanced Options		
Don't Resolve Addresses	Determines whether hostnames of the hops along the path are displayed, in addition to IP addresses.	To suppress the display of the hop hostnames, select the check box.
Gateway	Specifies the IP address of the gateway to route through.	Type the gateway IP address.
Source Address	Specifies the source address of the outgoing traceroute packets.	Type the source IP address.
Bypass Routing	Determines whether traceroute packets are routed by means of the routing table. If the routing table is not used, traceroute packets are sent only to hosts on the interface specified in the Interface box. If the host is not on that interface, traceroute responses are not sent.	To bypass the routing table and send the traceroute packets to hosts on the specified interface only, select the check box.

Table 91: Traceroute field summary *(Continued)*

Field	Function	Your Action
Interface	Specifies the interface on which the traceroute packets are sent.	From the list, select the interface on which traceroute packets are sent. If you select any, the traceroute requests are sent on all interfaces.
Time-to-live	Specifies the maximum time-to-live (TTL) hop count for the traceroute request packet.	From the list, select the TTL.
Type-of-Service	Specifies the type-of-service (TOS) value to include in the IP header of the traceroute request packet.	From the list, select the decimal value of the TOS field.
Resolve AS Numbers	Determines whether the autonomous system (AS) number of each intermediate hop between the router and the destination host is displayed.	To display the AS numbers, select the check box.

RELATED DOCUMENTATION

Connecting and Configuring an EX Series Switch (CLI Procedure)

Connecting and Configuring an EX Series Switch (J-Web Procedure)

Configuring Gigabit Ethernet Interfaces (J-Web Procedure) | **139**

Monitoring Interface Status and Traffic | **250**

Monitoring DHCP Services

IN THIS SECTION

- Purpose | **260**
- Action | **260**
- Meaning | **260**

Purpose

NOTE: This topic applies only to the J-Web Application package.

A switch or router can operate as a DHCP server. Use the monitoring functionality to view information about dynamic and static DHCP leases, conflicts, pools, and statistics.

Action

To monitor the DHCP server in the J-Web interface, select **Monitor** > **Services** > **DHCP**.

To monitor the DHCP server in the CLI, enter the following CLI commands:

- `show system services dhcp binding`
- `show system services dhcp conflict`
- `show system services dhcp pool`
- `show system services dhcp statistics`
- `show system services dhcp relay-statistics`
- `show system services dhcp global`
- `show system services dhcp client`
- `clear system services dhcp binding`
- `clear system services dhcp conflict`
- `clear system services dhcp statistics`
- `clear dhcp relay-statistics`

Meaning

Table 92 on page 260 summarizes the output fields in DHCP displays in the J-Web interface.

Table 92: Summary of DHCP Output Fields

Field	Values	Additional Information
Global tab		

Table 92: Summary of DHCP Output Fields *(Continued)*

Field	Values	Additional Information
Name	This column displays the following information: • Boot lease length • Domain Name • Name servers • Server identifier • Domain search • Gateway routers • WINS server • Boot file • Boot server • Default lease time • Minimum lease time • Maximum lease time	
Value	Displays the value for each of the parameters in the Name column.	
Bindings tab		
Allocated Address	List of IP addresses the DHCP server has assigned to clients.	
MAC Address	Corresponding media access control (MAC) address of the client.	
Binding Type	Type of binding assigned to the client: **dynamic** or **static**.	DHCP servers can assign a dynamic binding from a pool of IP addresses or a static binding to one or more specific IP addresses.

Table 92: Summary of DHCP Output Fields *(Continued)*

Field	Values	Additional Information
Lease Expires	Date and time the lease expires, or **never** for leases that do not expire.	
Pools tab		
Pool Name	Subnet on which the IP address pool is defined.	
Low Address	Lowest address in the IP address pool.	
High Address	Highest address in the IP address pool.	
Excluded Addresses	Addresses excluded from the address pool.	
Clients tab		
Interface Name	Name of the logical interface.	
Hardware Address	Vendor identification.	
Status	State of the client binding.	
Address Obtained	IP address obtained from the DHCP server.	
Update Server	Indicates whether server update is enabled.	

Table 92: Summary of DHCP Output Fields *(Continued)*

Field	Values	Additional Information
Lease Obtained	Date and time the lease was obtained.	
Lease Expires	Date and time the lease expires.	
Renew	Reacquires an IP address from the server for the interface. When you click this option, the command sends a discover message if the client state is INIT and a renew request message if the client state is BOUND. For all other states it performs no action.	
Release	Clears other resources received earlier from the server, and reinitializes the client state to INIT for the particular interface.	
Conflicts tab		
Detection Time	Date and time the client detected the conflict.	
Detection Method	How the conflict was detected.	Only client-detected conflicts are displayed.
Address	IP address where the conflict occurs.	The addresses in the conflicts list remain excluded until you use the `clear system services dhcp conflict` command to manually clear the list.
DHCP Statistics		
Relay Statistics tab		
Packet Counters	Displays the number of packet counters.	

Table 92: Summary of DHCP Output Fields *(Continued)*

Field	Values	Additional Information
Dropped Packet Counters	Graphically displays the number of dropped packet counters.	
Statistics tab		
Packets dropped	Total number of packets dropped and the number of packets dropped due to a particular condition.	
Messages received	Number of BOOTREQUEST, DHCPDECLINE, DHCPDISCOVER, DHCPINFORM, DHCPRELEASE, and DHCPREQUEST messages sent from DHCP clients and received by the DHCP server.	
Messages sent	Number of BOOTREPLY, DHCPACK, DHCPOFFER, DHCPNAK, and DHCPFORCERENEW messages sent from the DHCP server to DHCP clients.	

RELATED DOCUMENTATION

Configuring DHCP Services (J-Web Procedure) | 158

Monitoring OSPF Routing Information

IN THIS SECTION

- Purpose | 265
- Action | 265

Meaning | 265

Purpose

NOTE: This topic applies only to the J-Web Application package.

Use the monitoring functionality to monitor OSPF routing information on routing devices.

Action

To view OSPF routing information in the J-Web interface, select **Monitor** > **Routing** > **OSPF Information**.

To view OSPF routing information in the CLI, enter the following CLI commands:

- `show ospf neighbor`
- `show ospf interface`
- `show ospf statistics`

Meaning

Table 93 on page 265 summarizes key output fields in the OSPF routing display in the J-Web interface.

Table 93: Summary of Key OSPF Routing Output Fields

Field	Values	Additional Information
OSPF Interfaces		
Interface	Name of the interface running OSPF.	
State	State of the interface: **BDR**, **Down**, **DR**, **DRother**, **Loop**, **PtToPt**, or **Waiting**.	The **Down** state, indicating that the interface is not functioning, and **PtToPt** state, indicating that a point-to-point connection has been established, are the most common states.

Table 93: Summary of Key OSPF Routing Output Fields *(Continued)*

Field	Values	Additional Information
Area	Number of the area that the interface is in.	
DR ID	Address of the area's designated device.	
BDR ID	Address of the area's backup designated device.	
Neighbors	Number of neighbors on this interface.	
Adjacency Count	Number of devices in the area using the same area identifier.	
Stub Type	The areas into which OSPF does not flood AS external advertisements	
Passive Mode	In this mode the interface is present on the network but does not transmit or receive packets.	
Authentication Type	The authentication scheme for the backbone or area.	
Interface Address	The IP address of the interface.	
Address Mask	The subnet mask or address prefix.	
MTU	The maximum transmission unit size.	
Interface Cost	The path cost used to calculate the root path cost from any given LAN segment is determined by the total cost of each link in the path.	

Table 93: Summary of Key OSPF Routing Output Fields *(Continued)*

Field	Values	Additional Information
Hello Interval	How often the routing device sends hello packets out of the interface.	
Dead Interval	The interval during which the routing device receives no hello packets from the neighbor.	
Retransmit Interval	The interval for which the routing device waits to receive a link-state acknowledgment packet before retransmitting link-state advertisements to an interface's neighbors.	
OSPF Statistics		
Packets tab		
Sent	Displays the total number of packets sent.	
Received	Displays the total number of packets received.	
Details tab		
Flood Queue Depth	Number of entries in the extended queue.	
Total Retransmits	Number of retransmission entries enqueued.	
Total Database Summaries	Total number of database description packets.	
OSPF Neighbors		

Table 93: Summary of Key OSPF Routing Output Fields *(Continued)*

Field	Values	Additional Information
Address	Address of the neighbor.	
Interface	Interface through which the neighbor is reachable.	
State	State of the neighbor: **Attempt**, **Down**, **Exchange**, **ExStart**, **Full**, **Init**, **Loading**, or **2way**.	Generally, only the **Down** state, indicating a failed OSPF adjacency, and the **Full** state, indicating a functional adjacency, are maintained for more than a few seconds. The other states are transitional states that a neighbor is in only briefly while an OSPF adjacency is being established.
ID	ID of the neighbor.	
Priority	Priority of the neighbor to become the designated router.	
Activity Time	The activity time.	
Area	Area that the neighbor is in.	
Options	Option bits received in the hello packets from the neighbor.	
DR Address	Address of the designated router.	
BDR Address	Address of the backup designated router.	
Uptime	Length of time since the neighbor came up.	

Table 93: Summary of Key OSPF Routing Output Fields *(Continued)*

Field	Values	Additional Information
Adjacency	Length of time since the adjacency with the neighbor was established.	

RELATED DOCUMENTATION

Configuring an OSPF Network (J-Web Procedure) | 176

Supported Standards for IS-IS

Monitoring RIP Routing Information

IN THIS SECTION

- Purpose | 269
- Action | 269
- Meaning | 270

Purpose

NOTE: This topic applies only to the J-Web Application package.

Use the monitoring functionality to monitor RIP routing on routing devices.

Action

To view RIP routing information in the J-Web interface, select **Monitor** > **Routing** > **RIP Information**.

To view RIP routing information in the CLI, enter the following CLI commands:

- `show rip statistics`

- `show rip neighbor`

Meaning

Table 94 on page 270 summarizes key output fields in the RIP routing display in the J-Web interface.

Table 94: Summary of Key RIP Routing Output Fields

Field	Values	Additional Information
RIP Statistics		
Protocol Name	The RIP protocol name.	
Port number	The port on which RIP is enabled.	
Hold down time	The interval during which routes are neither advertised nor updated.	
Global routes learned	Number of RIP routes learned on the logical interface.	
Global routes held down	Number of RIP routes that are not advertised or updated during the hold-down interval.	
Global request dropped	Number of requests dropped.	
Global responses dropped	Number of responses dropped.	
RIP Neighbors		
Neighbor	Name of the RIP neighbor.	This value is the name of the interface on which RIP is enabled. Click the name to see the details for this neighbor.

Table 94: Summary of Key RIP Routing Output Fields *(Continued)*

Field	Values	Additional Information
State	State of the RIP connection: **Up** or **Dn** (Down).	
Source Address	Local source address.	This value is the configured address of the interface on which RIP is enabled.
Destination Address	Destination address.	This value is the configured address of the immediate RIP adjacency.
Send Mode	The mode of sending RIP messages.	
Receive Mode	The mode in which messages are received.	
In Metric	Value of the incoming metric configured for the RIP neighbor.	

Monitoring BGP Routing Information

IN THIS SECTION

- Purpose | 271
- Action | 272
- Meaning | 272

Purpose

NOTE: This topic applies only to the J-Web Application package.

Use the monitoring functionality to monitor BGP routing information on the routing device.

Action

To view BGP routing information in the J-Web interface, select **Monitor** > **Routing** > **BGP Information**.

To view BGP routing information in the CLI, enter the following commands:

- `show bgp summary`
- `show bgp neighbor`

Meaning

Table 95 on page 272 summarizes key output fields in the BGP routing display in the J-Web interface.

Table 95: Summary of Key BGP Routing Output Fields

Field	Values	Additional Information
BGP Peer Summary		
Total Groups	Number of BGP groups.	
Total Peers	Number of BGP peers.	
Down Peers	Number of unavailable BGP peers.	
Unconfigured Peers	Address of each BGP peer.	
RIB Summary tab		
RIB Name	Name of the RIB group.	
Total Prefixes	Total number of prefixes from the peer, both active and inactive, that are in the routing table.	

Table 95: Summary of Key BGP Routing Output Fields *(Continued)*

Field	Values	Additional Information
Active Prefixes	Number of prefixes received from the EBGP peers that are active in the routing table.	
Suppressed Prefixes	Number of routes received from EBGP peers currently inactive because of damping or other reasons.	
History Prefixes	History of the routes received or suppressed.	
Dumped Prefixes	Number of routes currently inactive because of damping or other reasons. These routes do not appear in the forwarding table and are not exported by routing protocols.	
Pending Prefixes	Number of pending routes.	
State	Status of the graceful restart process for this routing table: BGP restart is complete, BGP restart in progress, VPN restart in progress, or VPN restart is complete.	
BGP Neighbors		
Details	Click this button to view the selected BGP neighbor details.	
Peer Address	Address of the BGP neighbor.	
Autonomous System	AS number of the peer.	

Table 95: Summary of Key BGP Routing Output Fields *(Continued)*

Field	Values	Additional Information
Peer State	Current state of the BGP session: • **Active**—BGP is initiating a TCP connection in an attempt to connect to a peer. If the connection is successful, BGP sends an open message. • **Connect**—BGP is waiting for the TCP connection to become complete. • **Established**—The BGP session has been established, and the peers are exchanging BGP update messages. • **Idle**—This is the first stage of a connection. BGP is waiting for a Start event. • **OpenConfirm**—BGP has acknowledged receipt of an open message from the peer and is waiting to receive a keepalive or notification message. • **OpenSent**—BGP has sent an open message and is waiting to receive an open message from the peer.	Generally, the most common states are **Active**, which indicates a problem establishing the BGP connection, and **Established**, which indicates a successful session setup. The other states are transition states, and BGP sessions normally do not stay in those states for extended periods of time.
Elapsed Time	Elapsed time since the peering session was last reset.	
Description	Description of the BGP session.	

RELATED DOCUMENTATION

Configuring BGP Sessions (J-Web Procedure) | **168**

Supported Standards for IS-IS

Monitoring Routing Information

IN THIS SECTION

- Purpose | 275
- Action | 275
- Meaning | 275

Purpose

NOTE: This topic applies only to the J-Web Application package.

Use the monitoring functionality to view the **inet.0** routing table on the routing device.

Action

To view the routing tables in the J-Web interface, select **Monitor** > **Routing** > **Route Information**. Apply a filter or a combination of filters to view messages. You can use filters to display relevant events.

To view the routing table in the CLI, enter the following commands in the CLI interface:

- `show route terse`
- `show route detail`

Meaning

Table 96 on page 275 describes the different filters, their functions, and the associated actions.

Table 97 on page 276 summarizes key output fields in the routing information display.

Table 96: Filtering Route Messages

Field	Function	Your Action
Destination Address	Specifies the destination address of the route.	Enter the destination address.

Table 96: Filtering Route Messages *(Continued)*

Field	Function	Your Action
Protocol	Specifies the protocol from which the route was learned.	Enter the protocol name.
Next hop address	Specifies the network layer address of the directly reachable neighboring system (if applicable) and the interface used to reach it.	Enter the next hop address.
Receive protocol	Specifies the dynamic routing protocol using which the routing information was received through a particular neighbor.	Enter the routing protocol.
Best route	Specifies only the best route available.	Select the view details of the best route.
Inactive routes	Specifies the inactive routes.	Select the view details of inactive routes.
Exact route	Specifies the exact route.	Select the view details of the exact route.
Hidden routes	Specifies the hidden routes.	Select the view details of hidden routes.
Search	Applies the specified filter and displays the matching messages.	To apply the filter and display messages, click **Search**.

Table 97: Summary of Key Routing Information Output Fields

Field	Values	Additional Information
Static Route Addresses	The list of static route addresses.	

Table 97: Summary of Key Routing Information Output Fields *(Continued)*

Field	Values	Additional Information
Protocol	Protocol from which the route was learned: **Static**, **Direct**, **Local**, or the name of a particular protocol.	
Preference	The preference is the individual preference value for the route.	The route preference is used as one of the route selection criteria.
Next-Hop	Network layer address of the directly reachable neighboring system (if applicable) and the interface used to reach it.	If a next hop is listed as **Discard**, all traffic with that destination address is discarded rather than routed. This value generally means that the route is a static route for which the **discard** attribute has been set. If a next hop is listed as **Reject**, all traffic with that destination address is rejected. This value generally means that the address is unreachable. For example, if the address is a configured interface address and the interface is unavailable, traffic bound for that address is rejected. If a next hop is listed as **Local**, the destination is an address on the host (either the loopback address or Ethernet management port 0 address, for example).
Age	How long the route has been active.	
State	Flags for this route.	There are many possible flags.

Table 97: Summary of Key Routing Information Output Fields *(Continued)*

Field	Values	Additional Information
AS Path	AS path through which the route was learned. The letters of the AS path indicate the path origin: • **I**—IGP. • **E**—EGP. • **?**—Incomplete. Typically, the AS path was aggregated.	

RELATED DOCUMENTATION

- Configuring Static Routing (J-Web Procedure) | **188**
- Configuring Static Routing (CLI Procedure)
- Supported Standards for IS-IS

Monitoring Ethernet Switching on EX Series Switches (J-Web)

IN THIS SECTION

- Purpose | **278**
- Action | **279**
- Meaning | **279**

Purpose

NOTE: This topic applies only to the J-Web Application package.

Use the monitoring feature to view details that the EX Series switch maintains in its Ethernet switching table. These are details about the nodes on the LAN, such as VLAN name, VLAN ID, member interfaces, MAC addresses, and so on.

Action

To display Ethernet switching details in the J-Web interface, select **Monitor** > **Switching** > **Ethernet Switching**.

To view Ethernet switching details in the CLI, enter the following commands:

- `show ethernet-switching table`
- `show vlans`
- `show ethernet-switching interfaces`

Meaning

Table 98 on page 279 summarizes the Ethernet switching output fields.

Table 98: Ethernet Switching Output Fields

Field	Value
Ethernet Switching Table Information or MAC Table Summary	
MAC Table Count	The number of entries added to the Ethernet switching table.
MAC Table Learned	The number of dynamically learned MAC addresses in the Ethernet switching table.
Ethernet Switching Table Information or MAC Table Information	
VLAN	The VLAN name.
MAC Address	The MAC address associated with the VLAN. If a VLAN range has been configured for a VLAN, the output displays the MAC addresses for the entire series of VLANs that were created with that name.

Table 98: Ethernet Switching Output Fields *(Continued)*

Field	Value
Type	The type of MAC address. Values are: • **static**—The MAC address is manually created. • **learn**—The MAC address is learned dynamically from a packet's source MAC address. • **flood**—The MAC address is unknown and flooded to all members.
Age	The time remaining before the entry ages out and is removed from the Ethernet switching table.
Interfaces	The associated interfaces.
MAC Learning Log or Interface Information	
VLAN-Name	The VLAN name.
MAC Address	The learned MAC address associated with the VLAN ID.
MAC Limit	Maximum number of MAC addresses.
Time	Time at which the MAC address was added or deleted from the MAC learning log.
State	Operating state of the interface. Values are Up or Down.

RELATED DOCUMENTATION

Configuring MAC Table Aging on Switches

Understanding Bridging and VLANs on Switches

Monitoring IGMP Snooping

IN THIS SECTION

- Purpose | 281
- Action | 281
- Meaning | 281

Purpose

NOTE: This topic applies only to the J-Web Application package.

Use the monitoring feature to view status and information about IGMP snooping configuration on your EX Series switch.

Action

To display IGMP snooping details in the J-Web interface, select **Monitor** > **Switching** > **IGMP Snooping**.

To display IGMP snooping details in the CLI, enter the following commands:

- `show igmp-snooping route`
- `show igmp-snooping statistics`
- `show igmp-snooping vlans`

Meaning

Table 99 on page 281 summarizes the IGMP snooping details displayed.

Table 99: Summary of IGMP Snooping Output Fields

Field	Values
IGMP Snooping Monitor	

Table 99: Summary of IGMP Snooping Output Fields *(Continued)*

Field	Values
VLAN	The VLAN for which IGMP snooping is enabled.
Interfaces	Indicates the interfaces configured as switching interfaces that are associated with the multicast router.
Groups	Indicates the number of the multicast groups learned by the VLAN.
MRouters	Specifies the multicast router.
Receivers	Specifies the multicast receiver.
IGMP Route Information	
VLAN	The VLAN for which IGMP snooping is enabled.
Group	Indicates the multicast groups learned by the VLAN.
Next-Hop	Specifies the next hop assigned by the switch after performing the route lookup.

RELATED DOCUMENTATION

Example: Configuring IGMP Snooping on EX Series Switches

Monitoring Spanning Tree Protocols on Switches

IN THIS SECTION

Purpose | 283

Action | 283
Meaning | 283

Purpose

NOTE: This topic applies only to the J-Web Application package.

Use the monitoring feature to view status and information about the spanning-tree protocol parameters on your EX Series switch.

Action

To display spanning-tree protocol parameter details in the J-Web interface, select **Monitor** > **Switching** > **STP**.

To display spanning-tree protocol parameter details in the CLI, enter the following commands:

- `show spanning-tree interface`
- `show spanning-tree bridge`

Meaning

Table 100 on page 283 summarizes the spanning-tree protocol parameters.

Table 100: Summary of Spanning Tree Protocols Output Fields

Field	Values
Bridge Parameters	
Context ID	An internally generated identifier.
Enabled Protocol	Spanning-tree protocol type enabled.

Table 100: Summary of Spanning Tree Protocols Output Fields *(Continued)*

Field	Values
Root ID	Bridge ID of the elected spanning-tree root bridge. The bridge ID consists of a configurable bridge priority and the MAC address of the bridge.
Root cost	Calculated cost to reach the root bridge from the bridge where the command is entered.
Root port	Interface that is the current elected root port for this bridge.
Bridge ID	Locally configured bridge ID.
Hello time	The time for which the bridge interface remains in the listening or learning state.
Forward delay	The time for which the bridge interface remains in the listening or learning state before transitioning to the forwarding state.
Extended System ID	The system ID.
Inter Instance ID	An internally generated instance identifier.
Maximum age	Maximum age of received bridge protocol data units (BPDUs).
Number of topology changes	Total number of spanning-tree protocol topology changes detected since the switch last booted.
Spanning Tree Interface Details	
Interface Name	Interface configured to participate in the spanning-tree protocol instance.
Port ID	Logical interface identifier configured to participate in the spanning-tree protocol instance.

Table 100: Summary of Spanning Tree Protocols Output Fields *(Continued)*

Field	Values
Designated Port ID	Port ID of the designated port for the LAN segment to which the interface is attached.
Designated Bridge ID	ID of the designated bridge to which the interface is attached.
Port Cost	Configured cost for the interface.
Port State	Spanning-tree protocol port state: • Forwarding (FWD) • Blocking (BLK) • Listening • Learning • Disabled
Role	MSTP or RSTP port role, Designated (DESG), backup (BKUP), alternate (ALT), or root.
Spanning Tree Statistics of Interface	
Interface	Interface for which statistics is being displayed.
BPDUs Sent	Total number of BPDUs sent.
BPDUs Received	Total number of BPDUs received.
Next BPDU Transmission	Number of seconds until the next BPDU is scheduled to be sent.

Monitoring CoS Classifiers

IN THIS SECTION

- Purpose | 286
- Action | 286
- Meaning | 286

Purpose

NOTE: This topic applies only to the J-Web Application package.

Use the monitoring functionality to display the mapping of incoming CoS values to the forwarding class and loss priority for each classifier.

Action

To monitor CoS classifiers in the J-Web interface, select **Monitor** > **Class of Service** > **Classifiers**.

To monitor CoS classifiers in the CLI, enter the following CLI command:

```
show class-of-service classifier
```

Meaning

Table 101 on page 286 summarizes key output fields for CoS classifiers.

Table 101: Summary of Key CoS Classifier Output Fields

Field	Values	Additional Information
Classifier Name	Name of a classifier.	To display classifier assignments, click the plus sign (+).

Table 101: Summary of Key CoS Classifier Output Fields *(Continued)*

Field	Values	Additional Information
CoS Value Type	The classifiers are displayed by type: • **dscp**—All classifiers of the DSCP type. • **ieee-802.1**—All classifiers of the IEEE 802.1 type. • **inet-precedence**—All classifiers of the IP precedence type.	
Index	Internal index of the classifier.	
Incoming CoS Value	CoS value of the incoming packets, in bits. These values are used for classification.	
Assign to Forwarding Class	Forwarding class that the classifier assigns to an incoming packet. This class affects the forwarding and scheduling policies that are applied to the packet as it transits the switch.	
Assign to Loss Priority	Loss priority value that the classifier assigns to the incoming packet based on its CoS value.	

RELATED DOCUMENTATION

- *Defining CoS Classifiers (CLI Procedure)*
- *Defining CoS Classifiers (J-Web Procedure)*
- *Example: Configuring CoS on EX Series Switches*

Monitoring CoS Drop Profiles

IN THIS SECTION

- Purpose | 288
- Action | 288
- Meaning | 288

Purpose

NOTE: This topic applies only to the J-Web Application package.

Use the monitoring functionality to view data point information for each CoS random early detection (RED) drop profile.

Action

To monitor CoS RED drop profiles in the J-Web interface, select **Monitor** > **Class of Service** > **RED Drop Profiles**.

To monitor CoS RED drop profiles in the CLI, enter the following CLI command:

```
show class-of-service drop-profile
```

Meaning

Table 102 on page 289 summarizes the key output fields for CoS RED drop profiles.

Table 102: Summary of the Key Output Fields for CoS Red Drop Profiles

Field	Values	Additional Information
RED Drop Profile Name	Name of the RED drop profile. A drop profile consists of pairs of values between 0 and 100, one for queue buffer fill level and the other for drop probability, that determine the relationship between a buffer's fullness and the likelihood it will drop packets.	To display profile values, click the plus sign (+).
Graph RED Profile	Links to a graph of a RED curve that the system uses to determine the drop probability based on queue buffer fullness.	The x axis represents the queue buffer fill level, and the y axis represents the drop probability.
Type	Type of a specific drop profile: • **interpolated**—The two coordinates (x and y) of the graph are interpolated to produce a smooth profile. • **segmented**—The two coordinates (x and y) of the graph are represented by line fragments to produce a segmented profile.	
Index	Internal index of this drop profile.	
Fill Level	Percentage fullness of a buffer queue. This value is the x coordinate of the RED drop profile graph.	
Drop Probability	Drop probability of a packet corresponding to a specific queue buffer fill level. This value is the y coordinate of the RED drop profile graph.	

RELATED DOCUMENTATION

Defining CoS Drop Profiles (J-Web Procedure)

Example: Configuring CoS on EX Series Switches

Monitoring CoS Value Aliases

IN THIS SECTION

- Purpose | 290
- Action | 290
- Meaning | 290

Purpose

NOTE: This topic applies only to the J-Web Application package.

Use the monitoring functionality to display information about the CoS value aliases that the system is currently using to represent DSCP, IEEE 802.1p, and IPv4 precedence bits.

Action

To monitor CoS value aliases in the J-Web interface, select **Monitor** > **Class of Service** > **CoS Value Aliases**.

To monitor CoS value aliases in the CLI, enter the following command:

```
show class-of-service code-point-aliases
```

Meaning

Table 103 on page 291 summarizes key output fields for CoS value aliases.

Table 103: Summary of Key CoS Value Alias Output Fields

Field	Values	Additional Information
CoS Value Type	Type of the CoS value: • **dscp**—Examines Layer 3 packet headers for IP packet classification. • **ieee-802.1**—Examines Layer 2 packet headers for packet classification. • **inet-precedence**—Examines Layer 3 packet headers for IP packet classification.	To display aliases and bit patterns, click the plus sign (+).
CoS Value Alias	Name given to a set of bits—for example, **af11** is a name for **001010** bits.	
CoS Value	Set of bits associated with an alias.	

RELATED DOCUMENTATION

- *Defining CoS Code-Point Aliases (CLI Procedure)*
- *Defining CoS Code-Point Aliases (J-Web Procedure)*
- *Example: Configuring CoS on EX Series Switches*

Monitoring CoS Forwarding Classes

IN THIS SECTION

- Purpose | 292
- Action | 292

- Meaning | 292

Purpose

NOTE: This topic applies only to the J-Web Application package.

View the current assignment of CoS forwarding classes to queues on the switch.

Action

To monitor CoS forwarding classes in the J-Web interface, select **Monitor** > **Class of Service** > **Forwarding Classes**.

To monitor CoS forwarding classes in the CLI, enter the following CLI command:

```
show class-of-service forwarding-class
```

Meaning

Table 104 on page 293 summarizes key output fields for CoS forwarding classes.

Table 104: Summary of Key CoS Forwarding Class Output Fields

Field	Values
Forwarding Class	Names of forwarding classes assigned to queue numbers. The following are the default forwarding classes: • **best-effort**—Provides no special CoS handling of packets. Loss priority is typically not carried in a CoS value. • **expedited-forwarding**—Provides low loss, low delay, low jitter, assured bandwidth, and end-to-end service. • **assured-forwarding**—Provides high assurance for packets within the specified service profile. Excess packets are dropped. • **network-control**—Packets can be delayed but not dropped. EX4300 switches have the following additional default forwarding classes: • **mcast-be**—Provides no special CoS handling of packets. • **mcast-ef**—Provides low loss, low delay, low jitter, assured bandwidth, and end-to-end service. • **mcast-af**—Provides high assurance for packets within the specified service profile. Excess packets are dropped. • **mcast-nc**—Provides multicast network-control traffic.
Queue	Queue number corresponding to the forwarding class name. The default forwarding classes are assigned as follows: • **best-effort**—0 • **expedited-forwarding**—5 • **assured-forwarding**—1 • **network-control**—7 • **mcast-be**—2 • **mcast-ef**—4 • **mcast-af**—6

RELATED DOCUMENTATION

Defining CoS Forwarding Classes (CLI Procedure)

Defining CoS Forwarding Classes (J-Web Procedure)

Example: Configuring CoS on EX Series Switches

Monitoring Interfaces That Have CoS Components

IN THIS SECTION

- Purpose | 294
- Action | 294
- Meaning | 294

Purpose

NOTE: This topic applies only to the J-Web Application package.

Use the monitoring functionality to display details about the physical and logical interfaces and the CoS components assigned to them.

Action

To monitor interfaces that have CoS components in the J-Web interface, select **Monitor** > **Class of Service** > **Interface Association**.

To monitor interfaces that have CoS components in the CLI, enter the following command:

```
show class-of-service interface interface
```

Meaning

Table 105 on page 295 summarizes key output fields for CoS interfaces.

Table 105: Summary of Key CoS Interfaces Output Fields

Field	Values	Additional Information
Interface	Name of a physical interface to which CoS components are assigned.	To display names of logical interfaces configured on this physical interface, click the plus sign (+).
Scheduler Map	Name of the scheduler map associated with this interface.	
Queues Supported	Number of queues you can configure on the interface.	
Queues in Use	Number of queues currently configured.	
Logical Interface	Name of a logical interface on the physical interface to which CoS components are assigned.	
Object	Category of an object—for example, **classifier**, **scheduler-map**, or **rewrite**.	
Name	Name that you have given to an object —for example, **ba-classifier**.	
Type	Type of an object—for example, **dscp** for a classifier.	
Index	Index of this interface or the internal index of a specific object.	

RELATED DOCUMENTATION

Assigning CoS Components to Interfaces (CLI Procedure)

Assigning CoS Components to Interfaces (J-Web Procedure)

Example: Configuring CoS on EX Series Switches

Monitoring CoS Rewrite Rules

IN THIS SECTION

- Purpose | 296
- Action | 296
- Meaning | 296

Purpose

NOTE: This topic applies only to the J-Web Application package.

Use the monitoring functionality to display information about CoS value rewrite rules, which are based on the forwarding class and loss priority.

Action

To monitor CoS rewrite rules in the J-Web interface, select **Monitor** > **Class of Service** > **Rewrite Rules**.

To monitor CoS rewrite rules in the CLI, enter the following command:

```
show class-of-service rewrite-rules
```

Meaning

Table 106 on page 296 summarizes key output fields for CoS rewrite rules.

Table 106: Summary of Key CoS Rewrite Rules Output Fields

Field	Values	Additional Information
Rewrite Rule Name	Names of rewrite rules.	

Table 106: Summary of Key CoS Rewrite Rules Output Fields *(Continued)*

Field	Values	Additional Information
CoS Value Type	Rewrite rule type: • **dscp**—For IPv4 DiffServ traffic. • **exp**—For MPLS traffic. • **ieee-802.1**—For Layer 2 traffic. • **inet-precedence**—For IPv4 traffic.	To display forwarding classes, loss priorities, and rewritten CoS values, click the plus sign (+).
Index	Internal index for this particular rewrite rule.	
Forwarding Class	Forwarding class that is used to determine CoS values for rewriting in combination with loss priority.	Rewrite rules are applied to CoS values in outgoing packets based on forwarding class and loss priority setting.
Loss Priority	Loss priority that is used to determine CoS values for rewriting in combination with forwarding class.	
Rewrite CoS Value To	Value that the CoS value is rewritten to.	

RELATED DOCUMENTATION

- *Defining CoS Rewrite Rules (CLI Procedure)*
- *Defining CoS Rewrite Rules (J-Web Procedure)*
- *Example: Configuring CoS on EX Series Switches*

Monitoring CoS Scheduler Maps

IN THIS SECTION

- Purpose | 298
- Action | 298
- Meaning | 298

Purpose

NOTE: This topic applies only to the J-Web Application package.

Use the monitoring functionality to display assignments of CoS forwarding classes to schedulers.

Action

To monitor CoS scheduler maps in the J-Web interface, select **Monitor** > **Class of Service** > **Scheduler Maps**.

To monitor CoS scheduler maps in the CLI, enter the following CLI command:

```
show class-of-service scheduler-map
```

Meaning

Table 107 on page 298 summarizes key output fields for CoS scheduler maps.

Table 107: Summary of Key CoS Scheduler Maps Output Fields

Field	Values	Additional Information
Scheduler Map	Name of a scheduler map.	For details, click the plus sign (+).
Index	Index of a specific object—scheduler maps, schedulers, or drop profiles.	

Table 107: Summary of Key CoS Scheduler Maps Output Fields *(Continued)*

Field	Values	Additional Information
Scheduler Name	Name of a scheduler.	
Forwarding Class	Forwarding classes this scheduler is assigned to.	
Transmit Rate	Configured transmit rate of the scheduler in bits per second (bps). The rate value can be either of the following: • A percentage—The scheduler receives the specified percentage of the total interface bandwidth. • **remainder**—The scheduler receives the remaining bandwidth of the interface after bandwidth allocation to other schedulers.	
Buffer Size	Delay buffer size in the queue or the amount of transmit delay (in milliseconds). The buffer size can be either of the following: • A percentage—The buffer is a percentage of the total buffer allocation. • **remainder**—The buffer is sized according to what remains after other scheduler buffer allocations.	
Priority	Scheduling priority of a queue: • **strict-high**—Packets in this queue are transmitted first. • **low**—Packets in this queue are transmitted last.	

Table 107: Summary of Key CoS Scheduler Maps Output Fields *(Continued)*

Field	Values	Additional Information
Excess rate	The percentage of excess bandwidth traffic to share.	
Drop Profiles	Name and index of a drop profile that is assigned to a specific loss priority and protocol pair.	
Loss Priority	Packet loss priority corresponding to a drop profile.	
Protocol	Transport protocol corresponding to a drop profile.	
Drop Profile Name	Name of the drop profile.	
Index	Index of a specific object—scheduler maps, schedulers, or drop profiles.	

RELATED DOCUMENTATION

- *Defining CoS Schedulers and Scheduler Maps (CLI Procedure)*
- *Defining CoS Schedulers (J-Web Procedure)*
- *Example: Configuring CoS on EX Series Switches*

Monitoring the Virtual Chassis Status and Statistics on EX Series Virtual Chassis

IN THIS SECTION

- Purpose | 301
- Action | 301
- Meaning | 302

Purpose

NOTE: This topic applies only to the J-Web Application package.

You can use the J-Web monitoring functionality to view information about the switches that are members of a Virtual Chassis and their ports. J-Web monitoring is supported on EX2200, EX3300, EX4200, EX4400, EX4500, EX4550, and EX8200 switches in a Virtual Chassis.

Use the monitoring functionality to view the following information about the switches and the ports on EX2200, EX3300, EX4200, EX4400, EX4500, EX4550, and EX8200 switches that are members of a Virtual Chassis:

- Member details and how members are connected with each other
- Traffic statistics for Virtual Chassis ports (VCPs) of the selected members
- Details of the VCP packet counters

Action

To view Virtual Chassis monitoring details in the J-Web interface for a Virtual Chassis, select **Monitor > Virtual Chassis**.

To view member details for all members in the CLI, enter the following command:

```
user@switch> show virtual-chassis
```

To view VCP traffic statistics for a specific member in the CLI, enter the following command:

```
user@switch> show virtual-chassis vc-port statistics member member-id
```

To view the path a packet takes when going from a source interface to a destination interface in a Virtual Chassis configuration using the CLI, enter the following command:

```
user@switch> show virtual-chassis vc-path
```

Meaning

In the J-Web interface, the top half of the screen displays details of the Virtual Chassis configuration, such as:

- Member
- Role
- Status
- Interface
- Type
- Speed
- Neighboring Member ID
- Link Status
- Error count

NOTE: If the member switch in the Virtual Chassis is not provisioned, the member ID will be displayed as **-**.

Click the **Stop** button to stop fetching values from the switch, and click the **Start** button to start plotting data again from the point where it was stopped.

To view a graph of the statistics for the selected VCP of the member, click **Show Graph**.

Refresh Interval (sec)—Displays the time interval you have set for page refresh.

Click **Clear Statistics** to clear the monitoring statistics for the selected member switch. You can specify the interval at which the member details and statistics must be refreshed.

The bottom half of the screen displays a chart of the Virtual Chassis statistics and the port packet counters.

For details about the output from CLI commands, see the **show virtual-chassis** and **show virtual-chassis vc-port statistics** command summaries.

RELATED DOCUMENTATION

Configuring a Virtual Chassis on an EX Series Switch (J-Web Procedure)

Verifying the Member ID, Role, and Neighbor Member Connections of a Virtual Chassis Member

Monitoring 802.1X Authentication

IN THIS SECTION

- Purpose | 303
- Action | 303
- Meaning | 304

Purpose

NOTE: This topic applies only to the J-Web Application package.

Use the monitoring feature to display details of authenticated users and users that failed authentication.

Action

To display authentication details in the J-Web interface, select **Monitoring** > **Security** > **802.1X**.

To display authentication details in the CLI, enter the following commands:

- `show dot1x interface detail | display xml`
- `show dot1x interface detail <interface> | display xml`
- `show dot1x auth-failed-users`

Meaning

The details displayed include:

- A list of authenticated users.
- The number of connected users.
- A list of users that failed authentication.

You can also specify an interface for which the details must be displayed.

RELATED DOCUMENTATION

Configuring 802.1X Authentication (J-Web Procedure)

Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch

Monitoring Port Security

IN THIS SECTION

- Purpose | 304
- Action | 305
- Meaning | 305

Purpose

NOTE: This topic applies only to the J-Web Application package.

Use the monitoring functionality to view these port security details:

- DHCP snooping database for a VLAN or all VLANs
- ARP inspection details for all interfaces

Action

To monitor port security in the J-Web interface, select **Monitor** > **Security** > **Port Security**.

To monitor and manipulate the DHCP snooping database and ARP inspection statistics in the CLI, enter the following commands:

- `show dhcp snooping binding`
- `clear dhcp snooping binding`—In addition to clearing the whole database, you can clear database entries for specified VLANs or MAC addresses.
- `show arp inspection statistics`
- `clear arp inspection statistics`

Meaning

The J-Web Port Security Monitoring page comprises two sections:

- DHCP Snooping Details—Displays the DHCP snooping database for all the VLANs for which DHCP snooping is enabled. To view the DHCP snooping database for a specific VLAN, select the specific VLAN from the list.
- ARP Inspection Details—Displays the ARP inspection details for all interfaces. The information includes details of the number of packets that passed ARP inspection and the number of packets that failed the inspection. The pie chart graphically represents these statistics when you select an interface. To view ARP inspection statistics for a specific interface, select the interface from the list.

You can use the following options on the page to clear DHCP snooping and ARP inspection details:

- Clear All—Clears the DHCP snooping database, either for all VLANs if the option **ALL** has been selected in the Select VLANs list or for the specific VLAN that has been selected in that list.
- Clear—Deletes a specific IP address from the DHCP snooping database.

To clear ARP inspection details on the page, click **Clear All** in the ARP inspection details section.

Use the CLI commands to show and clear DHCP snooping database and ARP inspection statistics details.

RELATED DOCUMENTATION

Configuring Port Security (non-ELS)

Configuring Port Security (J-Web Procedure) | **104**

Example: Configuring Port Security (non-ELS)

4

PART

Administration

Software, Files, Licenses, Logs | 308

CHAPTER 17

Software, Files, Licenses, Logs

IN THIS CHAPTER

- Uploading a Configuration File (J-Web Procedure) | 308
- Managing Configuration Files Through the Configuration History (J-Web Procedure) | 309
- Setting or Deleting the Rescue Configuration (J-Web Procedure) | 313
- Updating J-Web Interface on EX Series Switches (J-Web Procedure) | 314
- Upgrading Junos OS on EX Series Switches (J-Web Procedure) | 316
- Managing Licenses for the EX Series Switch (J-Web Procedure) | 317
- Rebooting or Halting the EX Series Switch (J-Web Procedure) | 319
- Managing Log, Temporary, and Crash Files on the Switch (J-Web Procedure) | 320
- Registering the EX Series Switch with the J-Web Interface | 322
- Generating Support Information Reports for EX Series Switches Using the J-Web Interface | 323

Uploading a Configuration File (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

You can create a configuration file on your local system, copy the file to the EX Series switch and then load the file into the CLI. After you have loaded the configuration file, you can commit it to activate the configuration on the switch. You can also edit the configuration interactively using the CLI and commit it at a later time.

To upload a configuration file from your local system:

1. Select **Maintain** > **Config Management** > **Upload**.

   The work area displays the File to Upload box.
2. Specify the name of the file to upload using one of the following methods:
   - Type the absolute path and filename in the File to Upload box.

- Click **Browse** to navigate to the file.

3. Click **Upload and Commit** to upload and commit the configuration.

   The switch checks the configuration for the correct syntax before committing it.

RELATED DOCUMENTATION

- Uploading a Configuration File (CLI Procedure)
- Understanding J-Web Configuration Tools | 50
- *Understanding Configuration Files*

Managing Configuration Files Through the Configuration History (J-Web Procedure)

IN THIS SECTION

- Displaying Configuration History | 309
- Displaying Users Editing the Configuration | 311
- Comparing Configuration Files with the J-Web Interface | 312
- Downloading a Configuration File with the J-Web Interface | 312
- Loading a Previous Configuration File with the J-Web Interface | 312

NOTE: This topic applies only to the J-Web Application package.

Use the Configuration History function to manage configuration files.

Displaying Configuration History

To manage configuration files with the J-Web interface, select **Maintain** > **Config Management** > **History**. The main pane displays History — Database Information page.

Table 77 on page 207 summarizes the contents of the display.

The configuration history display allows you to:

- View a configuration.
- Compare two configurations.
- Download a configuration file to your local system.
- Roll back the configuration to any of the previous versions stored on the switch.

Table 108: J-Web Configuration History Summary

Field	Description
Number	Version of the configuration file.
Date/Time	Date and time the configuration was committed.
User	Name of the user who committed the configuration.
Client	Method by which the configuration was committed: • **cli**—A user entered a Junos OS CLI command. • **junoscript**—A Junos XML protocol client performed the operation. Commit operations performed by users through the J-Web interface are identified in this way. • **snmp**—An SNMP **set** request started the operation. • **other**—Another method was used to commit the configuration.
Comment	Comment.
Log Message	Method used to edit the configuration: • Imported via paste— Configuration was edited and loaded with the **Configure** > **CLI Tools** > **Edit Configuration Text** option. • Imported upload [*filename*]—Configuration was uploaded with the **Configure** > **CLI Tools** > **Point Click Editor** option. • Modified via J–Web Configure — Configuration was modified with the J-Web Configure menu. • Rolled back via *user-interface*— Configuration was rolled back to a previous version through the user interface specified by *user-interface*, which can be Web Interface or CLI.

Table 108: J-Web Configuration History Summary *(Continued)*

Field	Description
Action	Action to perform with the configuration file. The action can be **Download** or **Rollback**.

Displaying Users Editing the Configuration

To display a list of users editing the switching platform configuration, select **Config Management** > **History**. The list is displayed as Database Information in the main pane. Table 78 on page 208 summarizes the Database Information display.

Table 109: J-Web Configuration Database Information Summary

Field	Description
User Name	Name of user editing the configuration.
Start Time	Time of day the user logged in to the switch.
Idle Time	Elapsed time since the user issued a configuration command from the CLI.
Terminal	Terminal on which the user is logged in.
PID	Process identifier assigned to the user by the switching platform.
Edit Flags	Designates a private or exclusive edit.
Edit Path	Level of the configuration hierarchy that the user is editing.

SEE ALSO

Understanding Configuration Files

Understanding J-Web Configuration Tools | 50

Comparing Configuration Files with the J-Web Interface

To compare any two of the past 50 committed configuration files:

1. Select **Config Management** > **History**. A list of the current and the previous 49 configurations is displayed as Configuration History in the main pane.
2. Select the check boxes to the left of the two configuration versions you want to compare.
3. Click **Compare**.

   The main pane displays the differences between the two configuration files at each hierarchy level as follows:

   - Lines that have changed are highlighted side by side in green.
   - Lines that exist only in the more recent configuration file are displayed in red on the left.
   - Lines that exist only in the older configuration file are displayed in blue on the right.

Downloading a Configuration File with the J-Web Interface

To download a configuration file from the switch to your local system:

1. Select **Config Management** > **History**. A list of current and previous 49 configurations is displayed as Configuration History in the main pane.
2. In the Action column, click **Download** for the version of the configuration you want to download.
3. Select the options your Web browser provides that allow you to save the configuration file to a target directory on your local system.

   The file is saved as an ASCII file.

Loading a Previous Configuration File with the J-Web Interface

To load (roll back) and commit a previous configuration file stored on the switching platform:

1. Select **Config Management** > **History**. A list of current and previous 49 configurations is displayed as Configuration History in the main pane.
2. In the Action column, click **Rollback** for the version of the configuration you want to load.

   The main pane displays the results of the rollback operation.

NOTE: When you click **Rollback**, the switch loads and commits the selected configuration. This behavior is different from the switch's behavior that occurs after you enter the **rollback** configuration mode command from the CLI. In the latter case, the configuration is loaded but not committed.

RELATED DOCUMENTATION

Understanding Configuration Files

Understanding J-Web Configuration Tools | 50

Setting or Deleting the Rescue Configuration (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

A rescue configuration is a well-known configuration that recovers a switch from a configuration that denies management access. You set a current committed configuration to be the rescue configuration through the J-Web interface or CLI.

If someone inadvertently commits a configuration that denies management access to an EX Series switch and the console port is not accessible, you can overwrite the invalid configuration and replace it with the rescue configuration by using the LCD panel on the switch. The rescue configuration is a previously committed, valid configuration. We recommend that the rescue configuration include the IP address (accessible from the network) for the management port.

To view, set, or delete the rescue configuration using the J-Web interface, select **Maintain** > **Config Management** > **Rescue**. On the Rescue page, you can perform the following tasks:

- View the current rescue configuration—Click **View rescue configuration**.
- Set the current running configuration as the rescue configuration—Click **Set rescue configuration**.
- Delete the current rescue configuration—Click **Delete rescue configuration**.

RELATED DOCUMENTATION

Rescue Configuration

Configuration Files Terms

Updating J-Web Interface on EX Series Switches (J-Web Procedure)

IN THIS SECTION

- Installing J-Web Application Package by Using Auto Update | 314
- Installing J-Web Application Package by Using Manual Update | 315

You can update the J-Web software packages on a single fixed-configuration switch or for all members of a Virtual Chassis.

You can use the J-Web interface to install the latest Application package that is associated with the installed Junos OS, from a server by using FTP or HTTPS, or by uploading the file to the switch.

There are two ways in which you can use the J-Web interface to download and install the J-Web Application package:

- Auto update
- Manual update

Installing J-Web Application Package by Using Auto Update

To *automatically* check for and install the latest version of the J-Web Application package:

1. Click **Update Now** in the Update Available window that appears when you log in to the J-Web interface.

   NOTE:

   - For the Update Available window to appear when you log in, your switch or computer should be connected to the Internet.
   - The Update Available window appears only if there is a latest update available on the Juniper Networks server.
   - For the Update Available window to appear when you log in, the **Check for updates automatically on every login** in the *Update Preference* section in the **Maintain > Update J-Web** side pane must be selected.

- If you choose *Update Later*, you can update to the latest J-Web Application package by clicking the orange icon next to *Update Available* on the top pane of the J-Web interface or through **Maintain > Update J-Web**.

2. If the switch is connected to the Internet, the Update J-Web window appears. Enter the authentication details to download from the Juniper Networks download server. The J-Web Application package downloads and installs on the switch.

   If the switch is not connected to the Internet and your computer is connected to the Internet, download the latest version of the J-Web Application package to your computer and install it on your switch. Click **Download Application Package** in the Update J-Web window, enter authentication details to download from the Juniper Networks download server, and download the file to your computer. Select the file and click **Update**.

NOTE: You can also download the file to your computer and update it on the switch later by clicking *Select Application Package* in the Maintain > Update J-Web side pane, and selecting where the package is located.

SEE ALSO

Upgrading Junos OS on EX Series Switches (J-Web Procedure) | 204

Installing J-Web Application Package by Using Manual Update

To *manually* check for and install the latest J-Web Application package:

1. Go to **Maintain > Update J-Web** in the side pane, and click **Check for updates**.

   If the latest update is available on the Juniper Networks server, the Update Available window appears.

2. Click **Update Now** in the Update Available window.
3. If the switch is connected to the Internet, the Update J-Web window appears. Enter the authentication details to download from the Juniper Networks download server, and click **Update**. The J-Web Application package downloads and installs on the switch.

   If the switch is not connected to the Internet and your computer is connected to the Internet, download the latest version of the J-Web Application package to your local computer and install it on your switch. Click **Download Application Package** in the Update J-Web window, enter authentication details to download from the Juniper Networks download server, and download the file to your local system. Select the file, and click **Update**.

NOTE: You can also download the file to your computer and update it on the switch later by clicking *Select Application Package* in the Maintain > Update J-Web side pane, and selecting where the downloaded package is located.

SEE ALSO

Upgrading Junos OS on EX Series Switches (J-Web Procedure) | **204**

Upgrading Junos OS on EX Series Switches (J-Web Procedure)

IN THIS SECTION

- Installing Junos OS Upgrades by Uploading File from Local Computer | **316**

You can upgrade the Junos OS package on a single fixed-configuration switch or for all members of a Virtual Chassis.

You can use the J-Web interface to download and install Junos OS upgrades by copying the file to the EX Series switch.

Installing Junos OS Upgrades by Uploading File from Local Computer

To install software upgrades by uploading files:

1. Download the software package.
2. In the J-Web interface, select **Maintain > Update Junos**.
3. In the *Update Junos* section, select **Local File**. The *Upload Package* section appears below the Update Junos section.
4. In the Upload Package section, enter information into the fields described in Table 76 on page 205.
5. Click **Upload and Install Package**. The software is activated after the switching platform completes the installation procedure.

Table 110: Upload Package Summary

Field	Function	Your Action
File to Upload (required)	Specifies the location of the software package.	Type the location of the software package, or click **Browse** to navigate to the location.
Reboot If Required	Specifies that the switching platform is automatically rebooted when the upgrade is complete.	Select the check box if you want the switching platform to reboot automatically when the upgrade is complete.

SEE ALSO

Updating J-Web Interface on EX Series Switches (J-Web Procedure) | 202

Managing Licenses for the EX Series Switch (J-Web Procedure)

IN THIS SECTION

- Adding New Licenses | 318
- Deleting Licenses | 318
- Displaying License Keys | 318
- Downloading Licenses | 318

This topic applies only to the J-Web Application package.

To enable and use some Junos OS features on an EX Series switch, you must purchase, install, and manage separate software licenses. Each switch requires one license. For a Virtual Chassis deployment, two licenses are recommended for redundancy. After you have configured the features, you see a warning message if the switch does not have a license for the feature.

Before you begin managing licenses, be sure that you have:

- Obtained the needed licenses. For information about how to purchase software licenses, contact your Juniper Networks sales representative.

- Understand what makes up a license key. For more information, see *License Key Components for the EX Series Switch*.

This topic includes the following tasks:

Adding New Licenses

To add one or more new license keys on the switch, with the J-Web license manager:

1. In the J-Web interface, select **Maintain** > **Licenses**.
2. Under Installed Licenses, click **Add** to add a new license key or keys.
3. Do *one* of the following, using a blank line to separate multiple license keys:
   - In the License File URL box, type the full URL to the destination file containing the license key or keys to be added.
   - In the License Key Text box, paste the license key text, in plain-text format, for the license to be added.
4. Click **OK** to add the license key or keys.

A list of features that use the license key is displayed. The table also lists the ID, state, and version of the license key.

Deleting Licenses

To delete one or more license keys from a switch with the J-Web license manager:

1. In the J-Web interface, select **Maintain** > **Licenses**.
2. Select the check box of the license or licenses you want to delete.
3. Click **Delete**.

Displaying License Keys

To display the license keys installed on a switch with the J-Web license manager:

1. In the J-Web interface, select **Maintain** > **Licenses**.
2. Under Installed Licenses, click **Display Keys** to display all the license keys installed on the switch.

A screen displaying the license keys in text format appears. Multiple licenses are separated by a blank line.

Downloading Licenses

To download the license keys installed on the switch with the J-Web license manager:

1. In the J-Web interface, select **Maintain** > **Licenses**.

2. Under Installed Licenses, click **Download Keys** to download all the license keys installed on the switch to a single file.
3. Select **Save it to disk** and specify the file to which the license keys are to be written. You can also download the license file to your system.

Rebooting or Halting the EX Series Switch (J-Web Procedure)

You can use the J-Web interface to schedule a reboot or to halt the switching platform.

To reboot or halt the switching platform by using the J-Web interface:

1. In the J-Web interface, select **Maintain** > **Reboot**.
2. Select one:
   - **Reboot Immediately**—Reboots the switching platform immediately.
   - **Reboot in *number of* minutes**—Reboots the switch in the number of minutes from now that you specify.
   - **Reboot when the system time is *hour:minute*** —Reboots the switch at the absolute time that you specify, on the current day. You must select a 2-digit hour in 24-hour format and a 2-digit minute.
   - **Halt Immediately**— Stops the switching platform software immediately. After the switching platform software has stopped, you can access the switching platform through the console port only.
3. (Optional) In the Message box, type a message to be displayed to any users on the switching platform before the reboot occurs.
4. Click **Schedule**. The J-Web interface requests confirmation to perform the reboot or halt.
5. Click **OK** to confirm the operation.
   - If the reboot is scheduled to occur immediately, the switch reboots. You cannot access the J-Web interface until the switch has restarted and the boot sequence is complete. After the reboot is complete, refresh the browser window to display the J-Web interface login page.
   - If the reboot is scheduled to occur in the future, the Reboot page displays the time until reboot. You have the option to cancel the request by clicking **Cancel Reboot** on the J-Web interface Reboot page.
   - If the switch is halted, all software processes stop and you can access the switching platform through the console port only. Reboot the switch by pressing any key on the keyboard.

RELATED DOCUMENTATION

Starting the J-Web Interface | 58

Managing Log, Temporary, and Crash Files on the Switch (J-Web Procedure)

IN THIS SECTION

- Cleaning Up Files | 320
- Downloading Files | 321
- Deleting Files | 321

NOTE: This topic applies only to the J-Web Application package.

You can use the J-Web interface to rotate log files and delete unnecessary log, temporary, and crash files on the switch.

Cleaning Up Files

If you are running low on storage space, use the file cleanup procedure to quickly identify files to delete.

The file cleanup procedure performs the following tasks:

- Rotates log files—Archives the current log files, and creates fresh log files.
- Deletes log files in **/var/log**—Deletes files that are not currently being written to.
- Deletes temporary files in **/var/tmp**—Deletes files that have not been accessed within two days.
- Deletes all crash files in **/var/crash**—Deletes core files that the switch has written during an error.

To rotate log files and delete unnecessary files with the J-Web interface:

1. Select **Maintain** > **Files**.
2. In the Clean Up Files section, click **Clean Up Files**. The switching platform rotates log files and identifies files that can be safely deleted.

The J-Web interface displays the files that you can delete and the amount of space that will be freed on the file system.

3. Click one of the following options:
   - To delete the files and return to the Files page, click **OK**.
   - To cancel your entries and return to the list of files in the directory, click **Cancel**.

Downloading Files

You can use the J-Web interface to download a copy of an individual log, temporary, or crash file from the switching platform. When you download a file, it is not deleted from the file system.

To download files with the J-Web interface:

1. In the J-Web interface, select **Maintain** > **Files**.
2. In the Download and Delete Files section, Click one of the following options:
   - Log Files—Log files in the **/var/log** directory on the switch.
   - Temporary Files—Lists the temporary files in the **/var/tmp** directory on the switching platform.
   - Jailed Temporary Files (Install, Session, and so on)—Lists the files in the **/var/jail/tmp** directory on the switching platform.
   - Crash (Core) Files—Lists the core files in the **/var/crash** directory on the switching platform.

     The J-Web interface displays the files located in the directory.
3. Select the files that you want to download and click **Download**.
4. Choose a location for the saved file.

   The file is saved as a text file, with a **.txt** file extension.

Deleting Files

You can use the J-Web interface to delete an individual log, temporary, and crash file from the switching platform. When you delete the file, it is permanently removed from the file system.

CAUTION: If you are unsure whether to delete a file from the switching platform, we recommend using the Clean Up Files tool described in Cleaning Up Files. This tool determines which files can be safely deleted from the file system.

To delete files with the J-Web interface:

1. Select **Maintain** > **Files**.
2. In the Download and Delete Files section, Click one of the following options:
   - Log Files—Lists the log files in the **/var/log** directory on the switching platform.

- Temporary Files—Lists the temporary files in the **/var/tmp** directory on the switching platform.
- Jailed Temporary Files (Install, Session, etc)—Lists the files in the **/var/jail/tmp** directory on the switching platform.
- Crash (Core) Files—Lists the core files in the **/var/crash** directory on the switching platform.

  The J-Web interface displays the files in the directory.

3. Select the box next to each file you plan to delete.
4. Click **Delete**.

   The J-Web interface displays the files you can delete and the amount of space that will be freed on the file system.
5. Click one of the following buttons on the confirmation page:
   - To delete the files and return to the Files page, click **OK**.
   - To cancel your entries and return to the list of files in the directory, click **Cancel**.

RELATED DOCUMENTATION

J-Web User Interface for EX Series Switches Overview | 2

Registering the EX Series Switch with the J-Web Interface

NOTE: This topic applies only to the J-Web Application package.

You can register your EX Series switch with the J-Web interface so that you can request technical assistance as and when required. To register an EX Series switch:

1. In the J-Web interface, select **Maintain** > **Customer Support** > **Product Registration**. For an EX8200 Virtual Chassis configuration, select the member from the list.

   Note the serial number that is displayed.
2. Click **Register**. Enter the serial number in the page that is displayed.

RELATED DOCUMENTATION

EX Series Switch Software Features Overview

Generating Support Information Reports for EX Series Switches Using the J-Web Interface

NOTE: This topic applies only to the J-Web Application package.

For requesting technical support for EX Series switches, you can either contact the Juniper Networks Technical Assistance Center (JTAC) or raise an online request on the Customer Support Center (CSC) portal at https://www.juniper.net/customers/support/ for quick and easy problem resolution. You can generate the support information report for your device before requesting technical support and include this information with your request for technical support. This information helps the technical assistance providers in identifying your system setup and diagnosing the problem.

To generate the support information report for your switch:

1. In the J-Web interface, select **Maintain** > **Customer Support** > **Support Information**. For a Virtual Chassis configuration, select a member from the list.

   The Support Information page displays the general information about the switch, such as software version, chassis information, and configuration.
2. To obtain the support information for your device, click **Generate Report** to obtain a local copy of the support information report.

With the support information generated, you can access the CSC portal to view a list of the support options available to you, or you can open a case online using CSC's Case Management tool.

JTAC policies—For understanding JTAC procedures and policies, use the JTAC User Guide located at https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf .

RELATED DOCUMENTATION

EX Series Switch Software Features Overview

5

PART

Troubleshooting

Troubleshooting Task | 325

FAQ | 327

CHAPTER 18

Troubleshooting Task

IN THIS CHAPTER

- Troubleshooting Interface Configuration and Cable Faults | 325

Troubleshooting Interface Configuration and Cable Faults

IN THIS SECTION

- Interface Configuration or Connectivity Is Not Working | 325

NOTE: This topic applies only to the J-Web Application package.

Troubleshooting interface configuration and connectivity on the EX Series switch:

Interface Configuration or Connectivity Is Not Working

IN THIS SECTION

- Problem | 326
- Solution | 326

Problem

Description

NOTE: This topic applies only to the J-Web Application package.

You encounter errors when you attempt to configure an interface on the switch, or the interface is exhibiting connectivity problems.

Solution

Use the port troubleshooter feature in the J-Web interface to identify and rectify port configuration and connectivity related problems.

To use the J-Web interface port troubleshooter:

1. Select the option **Troubleshoot** from the main menu.
2. Click **Troubleshoot Port**. The Port Troubleshooting wizard is displayed. Click **Next**.
3. Select the ports to troubleshoot.
4. Select the test cases to be executed on the selected port. Click **Next**.

   When the selected test cases are executed, the final result and the recommended action is displayed.

If there is a cable fault, the port troubleshooter displays details and the recommended action. For example, the cable must be replaced.

If the port configuration needs to be modified, the port troubleshooter displays details and the recommended action.

RELATED DOCUMENTATION

Monitoring Interface Status and Traffic | 250

Configuring Gigabit Ethernet Interfaces (J-Web Procedure) | 139

Configuring Gigabit Ethernet Interfaces (CLI Procedure)

Configuring Gigabit Ethernet Interfaces for EX Series Switches with ELS support

Connecting and Configuring an EX Series Switch (CLI Procedure)

Connecting and Configuring an EX Series Switch (J-Web Procedure)

CHAPTER 19

FAQ

IN THIS CHAPTER

- J-Web Application Package for EX Series—Frequently Asked Questions | **327**

J-Web Application Package for EX Series—Frequently Asked Questions

IN THIS SECTION

- Does the J-Web Application package 15.1A1 support all the features supported in the previous release, that is, J-Web Application package 14.1X53-A1? | **328**
- What has changed in the distribution or packaging of J-Web for the EX Series switches? | **328**
- What are the benefits of the new J-Web distribution? | **328**
- Will the SRX Series platforms support the new J-Web distribution model? | **329**
- Which EX Series switches does the new J-Web distribution model support? | **329**
- What is included in the J-Web Platform package? | **346**
- What is included in the J-Web Application package? | **346**
- Do I need to install the J-Web Platform package? | **346**
- How do I upgrade the J-Web Platform package? | **346**
- How do I know whether an Application package is installed on my switch? | **347**
- How do I upgrade my J-Web Application package? | **347**
- Do I need to reboot the switch as part an Application package installation? | **347**
- What is the release compatibility between Junos OS, J-Web Platform packages, and J-Web Application packages? | **348**
- Can I install Application package version 15.1X53-A1 on top of Junos OS Release 14.1X53-D10? | **352**
- Can I install an Application package on top of Junos OS releases prior to Release 14.1X53? | **352**
- Are there switch-specific Application package images available for EX Series switches? | **352**

Do I need Internet connectivity from the switch for the auto update feature to work? | 352

Can I uninstall J-Web packages? | 352

This FAQ addresses questions regarding J-Web distribution model for EX Series switches and upgrading the J-Web Application package. The J-Web distribution model is introduced on EX Series switches at Junos OS Release 14.1X53-D10.

This FAQ covers the following questions:

Does the J-Web Application package 15.1A1 support all the features supported in the previous release, that is, J-Web Application package 14.1X53-A1?

Yes. The J-Web Application package 15.1A1 supports all the features supported in the previous release.

What has changed in the distribution or packaging of J-Web for the EX Series switches?

In Junos OS Releases earlier than Release 14.1X53-D10, J-Web was available as a single package as part of the Junos OS. For Junos OS Release 14.1X53-D10 and later, J-Web is available in two packages:

- Platform package—Installed as part of Junos OS by default; provides only minimal or basic features of J-Web (which includes, EZ Setup, Interface configuration, management access, user management, static routing, and image management).
- Application package—Separately installable package; provides complete features of J-Web (which include configuring, monitoring, maintaining, and troubleshooting).

NOTE: These distribution or packaging changes are specific to J-Web for EX Series switches.

What are the benefits of the new J-Web distribution?

The new distribution decouples J-Web release from the Junos OS release cycle and provides the following benefits:

- New features for J-Web are available as part of the Application package and delivered independent of Junos OS releases.

- Application package installation and upgrades do not mandate upgrade of Junos OS and the need to reboot the switch.

Will the SRX Series platforms support the new J-Web distribution model?

No. As of now, only EX Series switches will support this J-Web distribution model from Junos OS Release 14.1X53-D10.

Which EX Series switches does the new J-Web distribution model support?

Table 111 on page 329 shows the Junos OS release, the associated J-Web Application package release, and the switches supported in that release.

Table 111: EX Series Switches supported by J-Web Interface

Junos OS Release	Associated J-Web Application Package Release	Switches Supported by the J-Web Interface	For More Information
14.1X53-D10 through 14.1X53-D46	Application package 14.1X53-A2	EX2200, EX3200, EX3300, EX4200, EX4300, EX4500, EX4550, EX4600, and EX6200	Release Notes for 14.1X53-A2 J-Web Application Package
14.1X53-D47 and later	Application package 14.1X53-A3	EX2200, EX3200, EX3300, EX4200, EX4300, EX4500, EX4550, EX4600, and EX6200	Release Notes for 14.1X53-A3 J-Web Application Package
15.1R1	Application package 15.1A1	EX2200, EX3300, EX4200, EX4500, EX4550, and EX6210	Release Notes for 15.1A1 J-Web Application Package
15.1R3	Application package 15.1A2	EX2200, EX3300, EX4200, EX4300, EX4500, EX4550, and EX6200	Release Notes for 15.1A2 J-Web Application Package

Table 111: EX Series Switches supported by J-Web Interface *(Continued)*

Junos OS Release	Associated J-Web Application Package Release	Switches Supported by the J-Web Interface	For More Information
15.1X53-D50	Application package 15.1X53-A1	EX2300, EX2300-C, and EX3400	Release Notes for 15.1X53-A1 J-Web Application Package
15.1R4-S5	Application package 15.1A3	EX2200, EX3200, EX3300, EX4200, EX4300, EX4500, EX4550, and EX6200	Release Notes for 15.1A3 J-Web Application Package
16.1R1	Application package 16.1A1	EX4300 and EX4600	Release Notes for 16.1A1 J-Web Application Package
17.1R1	Application package 17.1A1	EX4300 and EX4600 **NOTE**: You cannot connect to and perform initial configuration of EX4600 switch by using the EZSetup procedure from the J-Web interface; you must use EZSetup from the switch console.	Release Notes for 17.1A1 J-Web Application Package

Table 111: EX Series Switches supported by J-Web Interface *(Continued)*

Junos OS Release	Associated J-Web Application Package Release	Switches Supported by the J-Web Interface	For More Information
17.2R1	Application package 17.2A1	EX4300 and EX4600 **NOTE**: You cannot connect to and perform initial configuration of EX4600 switch by using the EZSetup procedure from the J-Web interface; you must use EZSetup from the switch console.	Release Notes for 17.2A1 J-Web Application Package
17.3R1	Application package 17.3A1	EX4300 and EX4600 **NOTE**: You cannot connect to and perform initial configuration of EX4600 switch by using the EZSetup procedure from the J-Web interface; you must use EZSetup from the switch console.	Release Notes for 17.3A1 J-Web Application Package
15.1X53-D57	Application package 15.1X53-A2	EX2300, EX2300-C, and EX3400	Release Notes for 15.1X53-A2 J-Web Application Package

Table 111: EX Series Switches supported by J-Web Interface *(Continued)*

Junos OS Release	Associated J-Web Application Package Release	Switches Supported by the J-Web Interface	For More Information
17.4R1	Application package 17.4A1	EX4300 and EX4600 **NOTE**: You cannot connect to and perform initial configuration of EX4600 switch by using the EZSetup procedure from the J-Web interface; you must use EZSetup from the switch console.	Release Notes for 17.4A1 J-Web Application Package
18.1R1	Application package 18.1A1	EX2300, EX2300-C, EX3400, EX4300 and EX4600 **NOTE**: You cannot connect to and perform initial configuration of EX4600 switch by using the EZSetup procedure from the J-Web interface; you must use EZSetup from the switch console.	Release Notes for 18.1A1 J-Web Application Package

Table 111: EX Series Switches supported by J-Web Interface *(Continued)*

Junos OS Release	Associated J-Web Application Package Release	Switches Supported by the J-Web Interface	For More Information
18.1R2	Application package 18.1A2	EX2300, EX2300-C, EX3400, EX4300 and EX4600 **NOTE**: You cannot connect to and perform initial configuration of EX4600 switch by using the EZSetup procedure from the J-Web interface; you must use EZSetup from the switch console.	Release Notes for 18.1A2 J-Web Application Package
15.1X53-D59	Application package 15.1X53-A3	EX2300, EX2300-C, and EX3400	Release Notes for 15.1X53-A2 J-Web Application Package
18.2R1	Application package 18.2A1	EX2300, EX2300-C, EX3400, EX4300, and EX4600 **NOTE**: You cannot connect to and perform initial configuration of EX4600 switch by using the EZSetup procedure from the J-Web interface; you must use EZSetup from the switch console.	Release Notes for 18.2A1 J-Web Application Package

Table 111: EX Series Switches supported by J-Web Interface *(Continued)*

Junos OS Release	Associated J-Web Application Package Release	Switches Supported by the J-Web Interface	For More Information
18.2R1 and later and all service releases of 18.2R1 and later	Application Package 18.2A2	EX2300, EX2300-C, EX3400, EX4300, and EX4600 **NOTE**: You cannot connect to and perform initial configuration of EX4600 switch by using the EZSetup procedure from the J-Web interface; you must use EZSetup from the switch console.	Release Notes for 18.2A2 J-Web Application Package
15.1R2 and later and all service releases of 15.1R2 and later	Application package 15.1A4	EX2200, EX3200, EX3300, EX4200, EX4300, EX4500, EX4550, and EX6200	Release Notes for 15.1A4 J-Web Application Package
18.3R1	Application package 18.3A1	EX2300, EX2300-C, EX3400, EX4300, and EX4600 **NOTE**: You cannot connect to and perform initial configuration of EX4600 switch by using the EZSetup procedure from the J-Web interface; you must use EZSetup from the switch console.	Release Notes for 18.3A1 J-Web Application Package

Table 111: EX Series Switches supported by J-Web Interface *(Continued)*

Junos OS Release	Associated J-Web Application Package Release	Switches Supported by the J-Web Interface	For More Information
18.4R1	Application package 18.4A1	EX2300, EX2300-C, EX2300-MP, EX3400, EX4300, EX4300-MP, and EX4600 **NOTE**: You cannot connect to and perform initial configuration of EX4600 switch by using the EZSetup procedure from the J-Web interface; you must use EZSetup from the switch console.	Release Notes for 18.4A1 J-Web Application Package
18.4R1 and later and all service releases of 18.4R1 and later	Application Package 18.4A2	EX2300, EX2300-C, EX2300-MP, EX3400, EX4300, EX4300-MP, and EX4600 **NOTE**: You cannot connect to and perform initial configuration of EX4600 switch by using the EZSetup procedure from the J-Web interface; you must use EZSetup from the switch console.	Release Notes for 18.4A2 J-Web Application Package

Table 111: EX Series Switches supported by J-Web Interface *(Continued)*

Junos OS Release	Associated J-Web Application Package Release	Switches Supported by the J-Web Interface	For More Information
19.1R1	Application package 19.1A1	EX2300, EX2300-C, EX2300-MP, EX3400, EX4300, EX4300-MP, and EX4600 **NOTE**: You cannot connect to and perform initial configuration of EX4600 switch by using the EZSetup procedure from the J-Web interface; you must use EZSetup from the switch console.	Release Notes for 19.1A1 J-Web Application Package
19.2R1	Application package 19.2A1	EX2300, EX2300-C, EX2300-MP, EX3400, EX4300, EX4300-MP, EX4600, and EX4650 **NOTE**: You cannot connect to and perform initial configuration of EX4600 and EX4650 switches by using the EZSetup procedure from the J-Web interface; you must use EZSetup from the switch console.	Release Notes for 19.2A1 J-Web Application Package

Table 111: EX Series Switches supported by J-Web Interface *(Continued)*

Junos OS Release	Associated J-Web Application Package Release	Switches Supported by the J-Web Interface	For More Information
19.3R1	Application package 19.3A1	EX2300, EX2300-C, EX2300-MP, EX3400, EX4300, EX4300-MP, EX4600, and EX4650 **NOTE**: You cannot connect to and perform initial configuration of EX4600 and EX4650 switches by using the EZSetup procedure from the J-Web interface; you must use EZSetup from the switch console.	Release Notes for 19.3A1 J-Web Application Package
19.3R1 and later and all service releases of 19.3R1 and later	Application package 19.3A2	EX2300, EX2300-C, EX2300-MP, EX3400, EX4300, EX4300-MP, EX4600, and EX4650 **NOTE**: You cannot connect to and perform initial configuration of EX4600 and EX4650 switches by using the EZSetup procedure from the J-Web interface; you must use EZSetup from the switch console.	Release Notes for 19.3A2 J-Web Application Package

Table 111: EX Series Switches supported by J-Web Interface *(Continued)*

Junos OS Release	Associated J-Web Application Package Release	Switches Supported by the J-Web Interface	For More Information
19.4R1	Application package 19.4A1	EX2300, EX2300-C, EX2300-MP, EX3400, EX4300, EX4300-MP, EX4600, and EX4650 **NOTE**: You cannot connect to and perform initial configuration of EX4600 and EX4650 switches by using the EZSetup procedure from the J-Web interface; you must use EZSetup from the switch console.	Release Notes for 19.4A1 J-Web Application Package
19.4R1 and later and all service releases of 19.4R1 and later	Application package 19.4A2	EX2300, EX2300-C, EX2300-MP, EX3400, EX4300, EX4300-MP, EX4600, and EX4650 **NOTE**: You cannot connect to and perform initial configuration of EX4600 and EX4650 switches by using the EZSetup procedure from the J-Web interface; you must use EZSetup from the switch console.	Release Notes for 19.4A2 J-Web Application Package

Table 111: EX Series Switches supported by J-Web Interface *(Continued)*

Junos OS Release	Associated J-Web Application Package Release	Switches Supported by the J-Web Interface	For More Information
20.1R1	Application package 20.1A1	EX2300, EX2300-C, EX2300-MP, EX3400, EX4300, EX4300-MP, EX4600, and EX4650 **NOTE**: You cannot connect to and perform initial configuration of EX4600 and EX4650 switches by using the EZSetup procedure from the J-Web interface; you must use EZSetup from the switch console.	Release Notes for 20.1A1 J-Web Application Package
20.1R1	Application package 20.1A2	EX2300, EX2300-C, EX2300-MP, EX3400, EX4300, EX4300-MP, EX4600, and EX4650 **NOTE**: You cannot connect to and perform initial configuration of EX4600 and EX4650 switches by using the EZSetup procedure from the J-Web interface; you must use EZSetup from the switch console.	Release Notes for 20.1A2 J-Web Application Package

Table 111: EX Series Switches supported by J-Web Interface *(Continued)*

Junos OS Release	Associated J-Web Application Package Release	Switches Supported by the J-Web Interface	For More Information
20.2R1	Application package 20.2A1	EX2300, EX2300-C, EX2300-MP, EX3400, EX4300, EX4300-MP, EX4600, and EX4650 **NOTE**: You cannot connect to and perform initial configuration of EX4600 and EX4650 switches by using the EZSetup procedure from the J-Web interface; you must use EZSetup from the switch console.	Release Notes for 20.2A1 J-Web Application Package
20.3R1	Application package 20.3A1	EX2300, EX2300-C, EX2300-MP, EX3400, EX4300, EX4300-MP, EX4600, and EX4650 **NOTE**: You cannot connect to and perform initial configuration of EX4600 and EX4650 switches by using the EZSetup procedure from the J-Web interface; you must use EZSetup from the switch console.	Release Notes for 20.3A1 J-Web Application Package

Table 111: EX Series Switches supported by J-Web Interface *(Continued)*

Junos OS Release	Associated J-Web Application Package Release	Switches Supported by the J-Web Interface	For More Information
20.4R1	Application package 20.4A1	EX2300, EX2300-C, EX2300-MP, EX3400, EX4300, EX4300-MP, EX4600, and EX4650 **NOTE**: You cannot connect to and perform initial configuration of EX4600 and EX4650 switches by using the EZSetup procedure from the J-Web interface; you must use EZSetup from the switch console.	Release Notes for 20.4A1 J-Web Application Package
21.1R1	Application package 21.1A1	EX2300, EX2300-C, EX2300-MP, EX3400, EX4300, EX4300-MP, EX4600, and EX4650 **NOTE**: You cannot connect to and perform initial configuration of EX4600 and EX4650 switches by using the EZSetup procedure from the J-Web interface; you must use EZSetup from the switch console.	Release Notes for 21.1A1 J-Web Application Package

Table 111: EX Series Switches supported by J-Web Interface *(Continued)*

Junos OS Release	Associated J-Web Application Package Release	Switches Supported by the J-Web Interface	For More Information
21.2R1	Application package 21.2A1	EX2300, EX2300-C, EX2300-MP, EX3400, EX4300, EX4300-MP, EX4600, and EX4650 **NOTE**: You cannot connect to and perform initial configuration of EX4600 and EX4650 switches by using the EZSetup procedure from the J-Web interface; you must use EZSetup from the switch console.	Release Notes for 21.2A1 J-Web Application Package
21.3R1	Application package 21.3A1	EX2300, EX2300-C, EX2300-MP, EX3400, EX4300, EX4300-MP, EX4600, and EX4650 **NOTE**: You cannot connect to and perform initial configuration of EX4600 and EX4650 switches by using the EZSetup procedure from the J-Web interface; you must use EZSetup from the switch console.	Release Notes for 21.3A1 J-Web Application Package

Table 111: EX Series Switches supported by J-Web Interface *(Continued)*

Junos OS Release	Associated J-Web Application Package Release	Switches Supported by the J-Web Interface	For More Information
21.4R1	Application package 21.4A1	EX2300, EX2300-C, EX2300-MP, EX3400, EX4300, EX4300-MP, EX4600, and EX4650 **NOTE**: You cannot connect to and perform initial configuration of EX4600 and EX4650 switches by using the EZSetup procedure from the J-Web interface; you must use EZSetup from the switch console.	Release Notes for 21.4A1 J-Web Application Package
21.4R1	Application package 21.4A2	EX2300, EX2300-C, EX2300-MP, EX3400, EX4300, EX4300-MP, EX4600, and EX4650 **NOTE**: You cannot connect to and perform initial configuration of EX4600 and EX4650 switches by using the EZSetup procedure from the J-Web interface; you must use EZSetup from the switch console.	Release Notes for 21.4A2 J-Web Application Package
22.1R1	Application package 22.1A1	EX2300, EX2300-C, EX2300-MP, and EX3400	Release Notes for 22.1A1 J-Web Application Package

Table 111: EX Series Switches supported by J-Web Interface *(Continued)*

Junos OS Release	Associated J-Web Application Package Release	Switches Supported by the J-Web Interface	For More Information
22.2R1	Application package 22.2A1	EX2300, EX2300-C, EX2300-MP, and EX3400	Release Notes for 22.2A1 J-Web Application Package
22.2R1	Application package 22.2A2	EX2300, EX2300-C, EX2300-MP, and EX3400	Release Notes for 22.2A2 J-Web Application Package
22.3R1	Application package 22.3A1	EX2300, EX2300-C, EX2300-MP, EX3400, and EX4400	Release Notes for 22.3A1 J-Web Application Package
22.3R1 You must upgrade from Junos OS Release 22.3R1 to 22.3R3-S3 or later to install Application Package 22.3A2.	Application package 22.3A2	EX2300, EX2300-C, EX2300-MP, EX3400, and EX4400	Release Notes for 22.3A2 J-Web Application Package
22.4R1	Application package 22.4A1	EX2300, EX2300-C, EX2300-MP, EX3400, EX4100, EX4100-F, and EX4400	Release Notes for 22.4A1 J-Web Application Package
22.4R1 You must upgrade from Junos OS Release 22.4R1 to 22.4R3-S2 or later to install Application Package 22.4A2.	Application package 22.4A2	EX2300, EX2300-C, EX2300-MP, EX3400, EX4100, EX4100-F, and EX4400	Release Notes for 22.4A2 J-Web Application Package

Table 111: EX Series Switches supported by J-Web Interface *(Continued)*

Junos OS Release	Associated J-Web Application Package Release	Switches Supported by the J-Web Interface	For More Information
23.1R1	Application package 23.1A1	EX2300, EX2300-C, EX2300-MP, EX3400, EX4100, EX4100-F, EX4400, and EX4400-24X	Release Notes for 23.1A1 J-Web Application Package
23.2R1	Application package 23.2A1	EX2300, EX2300-C, EX2300-MP, EX3400, EX4100, EX4100-F, EX4400, and EX4400-24X	Release Notes for 23.2A1 J-Web Application Package
23.2R1	Application package 23.2A2	EX2300, EX2300-C, EX2300-MP, EX3400, EX4100, EX4100-F, EX4400, and EX4400-24X	Release Notes for 23.2A2 J-Web Application Package
23.4R1	Application package 23.4A1	EX2300, EX2300-C, EX2300-MP, EX3400, EX4100, EX4100-F, EX4400, and EX4400-24X	Release Notes for 23.4A1 J-Web Application Package
24.2R1	Application package 24.2A1	EX2300, EX2300-C, EX2300-MP, EX3400, EX4100, EX4100-F, EX4400, and EX4400-24X	Release Notes for 24.2A1 J-Web Application Package

Table 111: EX Series Switches supported by J-Web Interface *(Continued)*

Junos OS Release	Associated J-Web Application Package Release	Switches Supported by the J-Web Interface	For More Information
24.4R1	Application package 24.4A1	EX2300, EX2300-C, EX2300-MP, EX3400, EX4100, EX4100-H-12MP, EX4100-F, EX4400, EX4400-24X, EX4400-48XP, and EX4400-48MXP.	Release Notes for 24.4A1 J-Web Application Package

What is included in the J-Web Platform package?

The J-Web Platform package is bundled and shipped along with the Junos OS Release 14.1X53-D10 or later image according to the Junos OS release cycle schedule. The Platform package includes support for basic configuration and maintenance of the applicable fixed chassis EX Series switches, namely, EZSetup, interface configuration, management access, user management, static routing, image management, and so on.

What is included in the J-Web Application package?

The J-Web Application package provides all the features and functionalities of the J-Web interface that enable you to configure, monitor, maintain, and troubleshoot your switch.

The Application packages have their own release cycles which are independent of the Junos OS release cycle. The Application package is not installed by default on your switch; you download and install it over the Platform package on your switch.

Do I need to install the J-Web Platform package?

No. The J-Web Platform package is included in the Junos OS from Release 14.1X53-D10. It is installed on your switch as part of the Junos OS installation.

How do I upgrade the J-Web Platform package?

The J-Web Platform package is included in the Junos OS from Release 14.1X53-D10 and is installed on your switch as part of the Junos OS installation. If you upgrade to a later version of Junos OS, you automatically get the Platform package associated with that Junos OS.

NOTE: If you have the Application package installed on your switch, and you upgrade Junos OS on your switch, then the Application package is removed and the Platform package that is associated with Junos OS is installed on your switch. You must install the associated J-Web Application package over the Platform package.

How do I know whether an Application package is installed on my switch?

You can view details of the J-Web packages installed on your switch in the About window in the J-Web interface or in the output of the show version command in the Junos OS CLI.

How do I upgrade my J-Web Application package?

The new J-Web packaging supports two new features: the auto update feature and the manual update feature.

- Every time you log in to the J-Web interface, the auto update feature checks the Juniper Networks server for the availability of the latest version of Application package. If the latest version is available, you are prompted for installation.
- You also have the option of checking for the availability of the latest Application package at the Juniper Networks' download website and installing an available update on your switch by using the J-Web interface or CLI.

NOTE: Using CLI, the application packages are available for both Occam and non-Occam. For example:

- **jweb-ex-app-19.1A1_app.50-signed.tgz** for non-Occam.
- **jweb-ex-app-x86-32-19.1A1_bsdx-app.51.tgz** for Occam. Where, x86 represents the Occam software.

Do I need to reboot the switch as part an Application package installation?

No. There is no need to reboot the switch after the installation. The J-Web Application package is hot pluggable and installs on top of the current Junos OS image.

What is the release compatibility between Junos OS, J-Web Platform packages, and J-Web Application packages?

The Application packages of J-Web henceforth have their own release cycles (A1, A2, A3, and so on), which are independent of the Junos OS release cycle. An Application package is compatible only with the corresponding major release of Junos OS.

Table 112 on page 348 illustrates the release compatibility.

Table 112: J-Web Release Compatibility Matrix

Junos OS Release	Associated J-Web Application Package Release
14.1X53-D10 through 14.1X53-D46	Application package 14.1X53-A2
14.1X53-D47 and later	Application package 14.1X53-A3
15.1R1	Application package 15.1A1
15.1R2, 15.1R3, 15.1R4-S5, and so on.	Application package 15.1A3 **NOTE**: Application package 15.1A3 cannot be installed on Junos OS Release 15.1R1.
15.1X53-D50	Application package 15.1X53-A1. **NOTE**: Application package 15.1X53-A1 cannot be installed on Junos OS Release 15.1R3.
16.1R1	16.1A1
17.1R1	17.1A1
17.2R1	17.2A1
17.3R1	17.3A1
15.1X53-D57	Application package 15.1X53-A2

Table 112: J-Web Release Compatibility Matrix *(Continued)*

Junos OS Release	Associated J-Web Application Package Release
17.4R1	17.4A1
18.1R1	18.1A1
18.1R2	18.1A2
15.1X53-D59	Application package 15.1X53-A3
18.2R1	18.2A1
18.2R1 and later and all service releases of 18.2R1 and later	18.2A2
18.3R1	18.3A1
18.4R1	18.4A1
18.4R1 and later and all service releases of 18.4R1 and later	18.4A2
19.1R1	19.1A1
19.2R1	19.2A1
19.3R1	19.3A1
19.3R1 and later and all service releases of 19.3R1 and later	19.3A2
19.4R1	19.4A1

Table 112: J-Web Release Compatibility Matrix *(Continued)*

Junos OS Release	Associated J-Web Application Package Release
19.4R1 and later and all service releases of 19.4R1 and later	19.4A2
20.1R1	20.1A1
20.2R1	20.2A1
20.3R1	20.3A1
20.4R1	20.4A1
21.1R1	21.1A1
21.2R1	21.2A1
21.3R1	21.3A1
21.4R1	21.4A1
21.4R1	21.4A2
22.1R1	22.1A1
22.2R1	22.2A1
22.2R1	22.2A2
22.3R1	22.3A1

Table 112: J-Web Release Compatibility Matrix *(Continued)*

Junos OS Release	Associated J-Web Application Package Release
22.3R1 You must upgrade from Junos OS Release 22.3R1 to 22.3R3-S3 or later to install Application Package 22.3A2.	22.3A2
22.4R1	22.4A1
22.4R1 You must upgrade from Junos OS Release 22.4R1 to 22.4R3-S2 or later to install Application Package 22.4A2.	22.4A2
23.1R1	23.1A1
23.2R1	23.2A1
23.2R1	23.2A2
23.4R1	23.4A1
24.2R1	24.2A1
24.4R1	24.4A1

Any available later version of the Application package for a Junos OS release supersedes the earlier version. Thus, if Application package version 17.3A2 is available for 17.3R1, it will supersede version 17.3A1. We recommend that you install the latest available version of the Application package.

Can I install Application package version 15.1X53-A1 on top of Junos OS Release 14.1X53-D10?

No. Releases 14.1X53 and 15.1X53 are two distinct major releases of Junos OS. You can install Application package 14.1X53-A<*x*> where *x* is the latest available version (14.1X53-A2) of the Application package, on top of Junos OS Release 14.1X53-D10.

Similarly, an Application package for Junos OS Release 14.1X53-D<x> is not compatible with Junos OS Release 15.1X53-D<*x*>.

Can I install an Application package on top of Junos OS releases prior to Release 14.1X53?

No. The feature that separates J-Web for EX Series switches into Platform and Application packages is introduced in Junos OS Release 14.1X53.

Are there switch-specific Application package images available for EX Series switches?

No. There is a single Application package image that is compatible with all EX Series switches that is supported by J-Web, for the given release.

Any exceptions or limitations are documented in the release notes for the corresponding Application package.

Do I need Internet connectivity from the switch for the auto update feature to work?

Yes. Internet connectivity is required for the auto update feature to work. However, the Internet connectivity can be either from the switch or from the computer.

Can I uninstall J-Web packages?

You can uninstall an Application package by using the CLI command. After the Application package is uninstalled, the Platform package features will still be available for use.

We recommended that you do not uninstall the Platform package. If you uninstall the Platform package, you must reinstall Junos OS on your switch for the J-Web interface to be restored.

NOTE: You cannot uninstall the J-Web package from EX2300 or EX3400 switch.