JUNIPER NETWORKS | Engineering Simplicity

J-Web Platform Package for EX Series Ethernet Switches

J-Web Platform Package User Guide for EX Series Switches

Published
2025-12-18

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

J-Web Platform Package for EX Series Ethernet Switches J-Web Platform Package User Guide for EX Series Switches

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

Use this guide to configure, monitor, and troubleshoot your EX Series switch using the J-Web Application package. The J-Web Platform package basic features of J-Web and is installed as part of Junos OS.

PART 1

Overview

CHAPTER 1

J-Web Overview

IN THIS CHAPTER

J-Web User Interface for EX Series Switches Overview

IN THIS SECTION

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.
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
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

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

Junos OS Release	Associated J-Web Application Package Release
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—Platform Package

IN THIS SECTION

With the J-Web Platform package, you can:

- Configure Ethernet interfaces.
- Configure static routing.

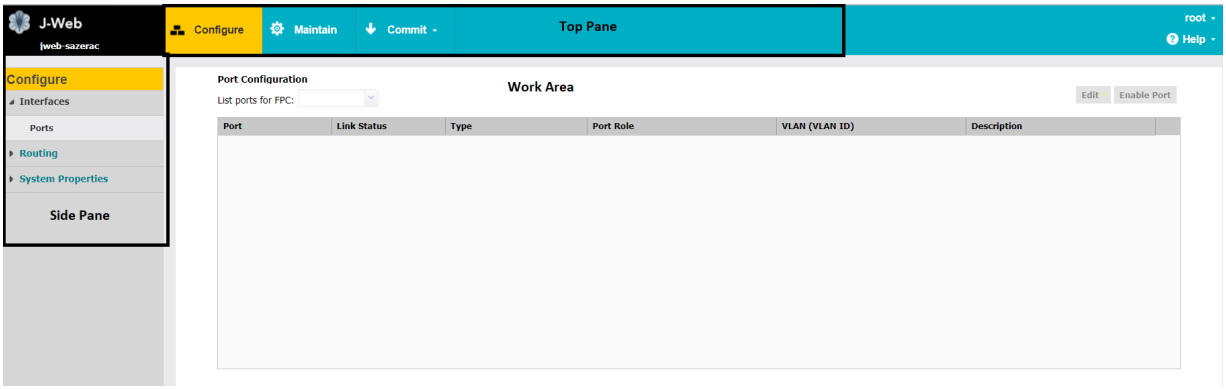
- Configure system properties, such as:
  - User management and authentication management.
  - Management access, such as, HTTPS, HTTP, Telnet, or SSH.
- Manage software upgrades or schedule a reboot.

J-Web Platform Package—First Look

Each page of the J-Web interface is divided into panes (see Figure 1 on page 7).

- Top pane—It is located at the top of the page. It displays the J-Web logo and hostname, tasks– Configure, Monitor, and Maintain, 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 or Maintain– 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 Platform interface.

Table 2: J-Web Platform Package Interface Elements

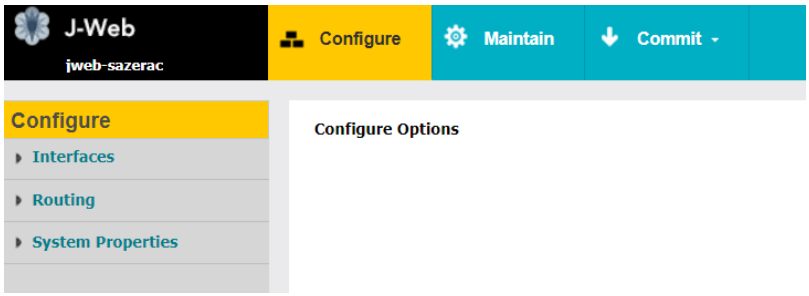
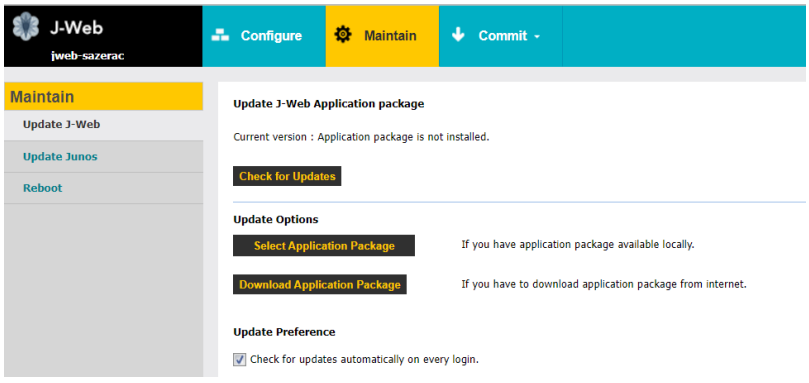
Element	Description
Top Pane	
J-Web *Hostname*	The J-Web logo and hostname of the switch.
Taskbar—Configure	Configure—Configure the switch, and view the configuration history. **Figure 2: Example of the Configure Tab** 
Taskbar—Maintain	Maintain—Update J-Web interface, upgrade Junos OS, and reboot the switch. **Figure 3: Example of the Maintain Tab** 

Table 2: J-Web Platform 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 **Logout**. Logout ends your current session with the switch and returns you to the login page.

Table 2: J-Web Platform 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. • About—Displays information about the J-Web interface, such as the version number.
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)*
- EX Series Switch Software Features Overview
- *Connecting and Configuring an EX Series Switch (J-Web Procedure)*
- CLI User Interface Overview

CHAPTER 2

Understanding the J-Web User Interface

IN THIS CHAPTER

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

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

2

PART

Configuring a Switch Using J-Web Interface

CHAPTER 3

Starting J-Web

IN THIS CHAPTER

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

Dashboard for EX Series Switches

CHAPTER 4

Configuring System Basics

IN THIS CHAPTER

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, EX4100-H-24MP, EX4100-H-24F, EX4400-48XP, and EX4400-48MXP switches.

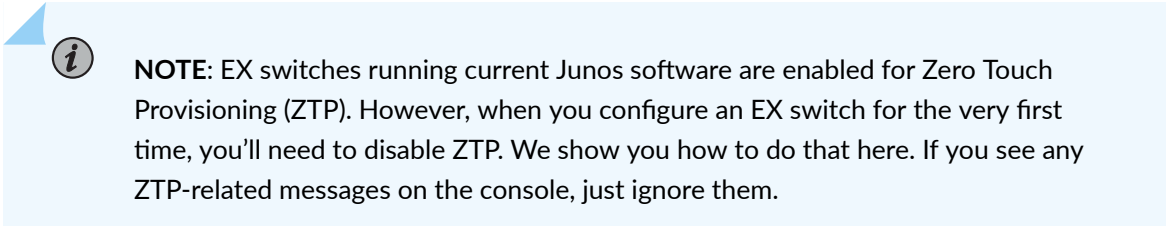
Have these values handy before you begin customizing settings for the switch:

- 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 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 3 on page 19.
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 3: Secure Management Access Configuration Summary

Field	Function	Your Action
Management Access tab		
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		

Table 3: Secure Management Access Configuration Summary *(Continued)*

Field	Function	Your Action
Services	Specifies services to be enabled: telnet and SSH.	Select to enable the required services.
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 3: 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*
- *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*

CHAPTER 5

Configuring Interfaces

IN THIS CHAPTER

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)* 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)*. 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 4 on page 25 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 4: 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 4: 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 4: 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 5 on page 31 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 4: 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 5 on page 31 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 4: 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 4: 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 4: 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 5: 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 5: 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*
- *Interfaces Overview for Switches*
- *Junos OS CoS for EX Series Switches Overview*
- *Understanding Interface Naming Conventions*

CHAPTER 6

Configuring Layer 3 Protocols

IN THIS CHAPTER

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 6 on page 33.
   - **Edit**—To modify an existing route. Enter information into the routing page as described in Table 6 on page 33.
   - **Delete**—To delete an existing route.

Table 6: Static Routing Configuration Summary

Field	Function	Your Action
Default Route		

Table 6: 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*
- Supported Standards for IS-IS

PART 3

Administering a Switch Using J-Web Interface

CHAPTER 7

Managing Users

IN THIS CHAPTER

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 7 on page 38.
   - **Edit**—Select this option to edit an existing user's details. Enter details as described in Table 7 on page 38.
   - **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 8 on page 39.

- **Edit**—Select this option to modify the authentication server details. Enter details as described in Table 8 on page 39.
- **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 8 on page 39.
  - **Edit**—Select this option to modify the authentication server details. Enter details as described in Table 8 on page 39.
  - **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 7: 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 7: 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 8: 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 8: 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)

CHAPTER 8

Managing Configurations and Files

IN THIS CHAPTER

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 9 on page 42 for details on the actions.
3. Configure the commit options by selecting **Preference**. See Table 10 on page 43 for details on preference options.

Table 9: 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.

Table 9: Commit Options *(Continued)*

Menu Item	Function	Your Action
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 10 on page 43 for details on preference options.

Table 10: 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

EX Series Switch Software Features Overview

CHAPTER 9

Managing Software and Licenses

IN THIS CHAPTER

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

IN THIS SECTION

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, by uploading the file to the switch.

Installing J-Web Application Package by Using Manual Update

To *manually* check for and install the latest J-Web Application package:

1. When you log in to J-Web, the Update Available window appears if the latest update is available on the Juniper Networks server. Additionally, you can navigate to **Maintain** > **Update J-Web** in the left-side pane and click on **Check for updates** to manually check for updates.
2. Click the support site link available in the Update Available window to download the latest Junos OS web management application package.
3. Navigate to **Maintain > Update J-Web** in the left-side pane once you download the latest application package, and click **Select Application Package**.

The Update J-Web window appears.

4. Click **Browse** to choose the downloaded application package file, and then click **Install Package**.

> **NOTE**: You must save all your changes before installing the latest J-Web Application package.

SEE ALSO

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

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

IN THIS SECTION

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 11 on page 46.
5. Click **Upload and Install Package**. The software is activated after the switching platform completes the installation procedure.

Table 11: 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)*

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