




J-Web for EX Series Switches Online Help—Platform Package



Modified: 2017-03-04
Part Number: , Revision

Revision History

September 2014—For J-Web Platform package release 14.1X53-D10

March 2016—For J-Web Platform package release 15.1R3

June 2016—For J-Web Platform package release 15.1X53-D50

July 2016—For J-Web Platform package release 16.1R1

Dec 2016—Modified this document for unification wrt Freedom Project

Table of Contents

Part 1	J-Web for EX Series Switches Online Help—Platform Package	
Chapter 1	J-Web Overview	3
	J-Web User Interface for EX Series Switches Overview	3
	J-Web Packages	3
	Release Compatibility	4
	Software Requirements	5
	J-Web Interface—Platform Package	6
	J-Web Platform Package—First Look	6
	Understanding J-Web User Interface Sessions	8
	Using the Commit Options to Commit Configuration Changes (J-Web Procedure)	9
Chapter 2	Configuring the Switch by Using the J-Web Interface	11
	Starting the J-Web Interface	11
	System Basics Configuration	12
	Connecting and Configuring an EX Series Switch (J-Web Procedure)	12
	Configuring Management Access for the EX Series Switch (J-Web Procedure)	16
	Generating SSL Certificates to Be Used for Secure Web Access	19
	Rebooting or Halting the EX Series Switch (J-Web Procedure)	20
	Interfaces Configuration	21
	Configuring Gigabit Ethernet Interfaces (J-Web Procedure)	21
	Configuring Static Routing (J-Web Procedure)	27
	Software Installation and Upgrades	29
	Updating J-Web Interface on EX Series Switches (J-Web Procedure)	29
	Installing J-Web Application Package by Using Auto Update	29
	Installing J-Web Application Package by Using Manual Update	30
	Upgrading Junos OS on EX Series Switches (J-Web Procedure)	30
	Installing Junos OS Upgrades from a Remote Server	31
	Installing Junos OS Upgrades by Uploading File from Local Computer	31
	Managing Users (J-Web Procedure)	32
Chapter 3	Maintaining the Switch Using J-Web Interface	35

PART 1

J-Web for EX Series Switches Online Help—Platform Package

- J-Web Overview on page 3
- Configuring the Switch by Using the J-Web Interface on page 11
- Maintaining the Switch Using J-Web Interface on page 35

CHAPTER 1

J-Web Overview

- J-Web User Interface for EX Series Switches Overview on page 3
- J-Web Interface—Platform Package on page 6
- Understanding J-Web User Interface Sessions on page 8
- Using the Commit Options to Commit Configuration Changes (J-Web Procedure) on page 9

J-Web User Interface for EX Series Switches Overview

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.

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.

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

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

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

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.

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 version 24 through 30, and Google Chrome version 27 through 36.



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



NOTE: Other browser versions might not work on the switch. The browser and the network must support receiving and processing HTTP 1.1 GZIP compressed data.

- Language support—English-version browsers

Release History Table

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

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.

- **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.

The layout of the panes enables you to quickly navigate through the interface.

[Table 2 on page 6](#) summarizes the elements of the J-Web Platform interface.

Table 2: J-Web Platform Package Interface Elements

Element	Description
Top Pane	
J-Web	The J-Web logo and hostname of the switch.
Hostname	
Taskbar	Menu that displays the main options. Click the tab to access an option. <ul style="list-style-type: none"> • Configure—Configure the switch, and view the configuration history. • Maintain—Update J-Web interface, upgrade Junos OS, and reboot the switch.

Table 2: J-Web Platform Package Interface Elements (*continued*)

Element	Description
Commit Options	<p>A set of options using which you can configure committing multiple changes with a single commit.</p> <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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. <p>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).</p>
Update Available	<p>This icon message appears only if there is a J-Web Application package update available on the Juniper Networks server.</p> <p>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.</p>
<i>username</i>	<p>The username you used to log in to the switch.</p> <p>The down arrow option displays Logout. Logout ends your current session with the switch and returns you to the login page.</p>
Help	<p>Displays links to help topics and information about the J-Web interface.</p> <ul style="list-style-type: none"> Help Contents—Provides context-sensitive help. About—Displays information about the J-Web interface, such as the version number.
Work Area	
Configuration hierarchy	<p>(Applies to the Junos OS CLI configuration editor only) Displays the hierarchy of committed statements in the switch configuration.</p> <ul style="list-style-type: none"> 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 \(J-Web Procedure\) on page 9](#)
 - [EX Series Switch Software Features Overview](#)
 - [Connecting and Configuring an EX Series Switch \(J-Web Procedure\) on page 12](#)
 - [CLI User Interface Overview](#)

Understanding J-Web User Interface Sessions

You establish a J-Web session with the switch through an HTTP-enabled or 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” on page 19](#).

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 on page 3](#)
 - [Configuring Management Access for the EX Series Switch \(J-Web Procedure\) on page 16](#)

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 3 on page 10](#) for details on the actions.
3. Configure the commit options by selecting **Preference**. See [Table 4 on page 10](#) for details on preference options.

Table 3: Commit Options

Menu Item	Function	Your Action
Commit	Commits the candidate configuration of the current user session, along with changes from other user sessions.	<ol style="list-style-type: none"> 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.	<ol style="list-style-type: none"> 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.	<ol style="list-style-type: none"> 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.	<ol style="list-style-type: none"> 1. Select Commit Options > Preference. The Commit Preference page is displayed. 2. Configure the commit options by selecting your preference. See Table 4 on page 10 for details on preference options.

Table 4: 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	<p>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.</p> <p>Once you select this option, you need to select Commit Options > Commit to commit your changes.</p>

Related Documentation

- [J-Web User Interface for EX Series Switches Overview on page 3](#)
- [EX Series Switch Software Features Overview](#)

CHAPTER 2

Configuring the Switch by Using the J-Web Interface

J-Web uses the Configuration tab to display the configuration pages that enable you to configure various Junos OS features by using J-Web.



NOTE: If you are using the J-Web Platform package, the *Update Available* window appears. This window is enabled by the auto update feature of J-Web. See [“Installing J-Web Application Package by Using Auto Update”](#) on page 29 to know more.

The following topics describe the configuration pages supported on J-Web for EX Series switches:

- [Starting the J-Web Interface](#) on page 11
- [System Basics Configuration](#) on page 12
- [Interfaces Configuration](#) on page 21
- [Configuring Static Routing \(J-Web Procedure\)](#) on page 27
- [Software Installation and Upgrades](#) on page 29
- [Managing Users \(J-Web Procedure\)](#) on page 32

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 HTTP-enabled or HTTPS-enabled Web browser.
To use HTTPS, you must have installed a certificate on the switch and enabled HTTPS.
2. After **http://** or **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 on page 3](#)
- [Dashboard for EX Series Switches](#)

System Basics Configuration

- [Connecting and Configuring an EX Series Switch \(J-Web Procedure\) on page 12](#)
- [Configuring Management Access for the EX Series Switch \(J-Web Procedure\) on page 16](#)
- [Generating SSL Certificates to Be Used for Secure Web Access on page 19](#)
- [Rebooting or Halting the EX Series Switch \(J-Web Procedure\) on page 20](#)

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

There are two ways to connect and configure an EX Series switch: one method is through the console by using the CLI and the other is by using the J-Web interface.



NOTE: You cannot connect to and perform initial configuration of EX2200-24T-4G-DC and EX4600 switches using EZSetup procedure from the J-Web interface. For EX2200-24T-4G-DC switches, you must use EZSetup from the switch console, and for EX4600 switches, you must use the CLI procedure through the switch console.

This topic describes the J-Web procedure.



NOTE: Before you begin the configuration, enable a DHCP client on the management PC that you will connect to the switch so that the PC can obtain an IP address dynamically.



NOTE: Read the following steps before you begin the configuration. You must complete the initial configuration by using EZSetup within 10 minutes. The switch exits EZSetup after 10 minutes and reverts to the factory default configuration, and the PC loses connectivity to the switch.

- EX2200 and EX2200-C switch—The LEDs on the network ports on the front panel blink when the switch is in the initial setup mode.
 - EX3200, EX3300, EX4200, EX4300, EX4500, EX4550, EX6200, or EX8200 switch—The LCD panel displays a count-down timer when the switch is in initial setup mode.
-

To connect and configure the switch by using the J-Web interface:

1. Transition the switch into initial setup mode:
 - EX2200 and EX2200-C switch—Press the mode button located on the lower right corner of the front panel for 10 seconds.
 - EX3200, EX3300, EX4200, EX4300, EX4500, EX4550, EX6200, or EX8200 switch—Use the **Menu** and **Enter** buttons located to the right of the LCD panel (see [Figure 1 on page 14](#) or [Figure 2 on page 14](#)):

Figure 1: LCD Panel in an EX3200, EX4200, EX4500, EX4550, or EX8200 Switch

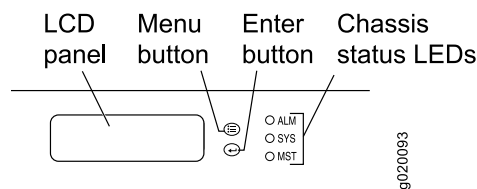
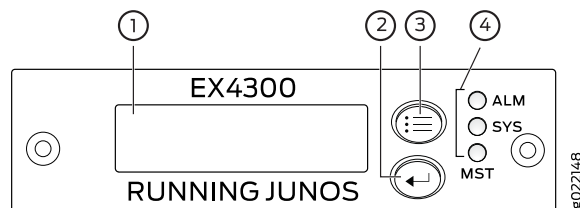


Figure 2: LCD Panel in an EX4300 Switch



1—LCD panel	3—LCD panel Menu button
2—LCD panel Enter button	4—Chassis status LEDs

1. Press the **Menu** button until you see **MAINTENANCE MENU**. Then press the **Enter** button.
 2. Press **Menu** until you see **ENTER EZSetup**. Then press **Enter**.

If EZSetup does not appear as an option in the menu, select **Factory Default** to return the switch to the factory default configuration. EZSetup is displayed in the menu of standalone switches only when a switch is set to the factory default configuration.
 3. Press **Enter** to confirm setup and continue with EZSetup.
2. 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.
 - EX3300, EX4500, or EX4550 switch—Connect the cable to the port labeled **MGMT** on the front panel (LCD panel side) of the switch.
 - EX4300 switch—Connect the cable to the port labeled **MGMT** 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.

These ports are configured as the DHCP server with the default IP address, 192.168.1.1. The switch can assign an IP address to the management PC in the IP address range 192.168.1.2 through 192.168.1.253.

3. From the PC, open a Web browser, type **http://192.168.1.1** in the address field, and press **Enter**.
4. On the J-Web login page, type **root** as the username, leave the password field blank, and click **Login**.
5. On the Introduction page, click **Next**.
6. On the Basic Settings page, modify the hostname, the root password, and date and time settings:
 - Enter the hostname. This is optional.
 - Enter a password and reenter the password.
 - Specify the time zone.
 - Synchronize the date and time settings of the switch with the management PC or set them manually by selecting the appropriate option button. This is optional.

Click **Next**.

7. Use the Management Options page to select the management scenario:



NOTE: On EX4500, EX6210, and EX8200 switches, only the out-of-band management option is available.

- **In-band Management—Use VLAN 'default' for management.**

Select this option to configure all data interfaces as members of the default VLAN. Click **Next**. Specify the management IP address and the default gateway for the default VLAN.

- **In-band Management—Create new VLAN for management.**

Select this option to create a management VLAN. Click **Next**. Specify the VLAN name, VLAN ID, member interfaces, management IP address, and default gateway for the new VLAN.

- **Out-of-band Management—Configure management port.**

Select this option to configure only the management interface. Click **Next**. Specify the IP address and default gateway for the management interface.

8. Click **Next**.

9. On the Manage Access page, you can select options to enable Telnet, SSH, and SNMP services. For SNMP, you can configure the read community, location, and contact.
10. Click **Next**. The Summary screen displays the configured settings.
11. Click **Finish**. The configuration is committed as the active switch configuration.



NOTE: After the configuration is committed, the connectivity between the PC and the switch might be lost. To renew the connection, release and renew the IP address by executing the appropriate commands on the management PC or by removing and reinserting the Ethernet cable.

12. (For EX4500 switches only) In the CLI, enter the **request chassis pic-mode intraconnect** operational mode command to set the PIC mode to intraconnect.

You can now log in by using the CLI or the J-Web interface to continue configuring the switch.

If you use the J-Web interface to continue configuring the switch, the Web session is redirected to the new management IP address. If the connection cannot be made, the J-Web interface displays instructions for starting a J-Web session.

Related Documentation

- [Connecting and Configuring an EX Series Switch \(CLI Procedure\)](#)
- [Installing and Connecting an EX2200 Switch](#)
- [Installing and Connecting an EX3200 Switch](#)
- [Installing and Connecting an EX3300 Switch](#)
- [Installing and Connecting an EX4200 Switch](#)
- [Installing and Connecting an EX4300 Switch](#)
- [Installing and Connecting an EX4500 Switch](#)
- [Installing and Connecting an EX4550 Switch](#)
- [Installing and Connecting an EX4600 Switch](#)
- [Installing and Connecting an EX6210 Switch](#)
- [Installing and Connecting an EX8208 Switch](#)
- [Installing and Connecting an EX8216 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 communicate with the switch, the J-Web interface uses HTTP. HTTP enables easy Web access, but uses no encryption. The data that is transmitted between the Web browser and the switch by means of HTTP is vulnerable to interception and attack. To enable secure Web access the switch supports HTTPS. You can enable HTTP or 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 HTTP and 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 5 on page 17](#).
2. To verify that Web access is enabled correctly, connect to the switch using the appropriate method:
 - For HTTP access—In your Web browser, type **http://URL** or **http://IP address**.
 - 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 5: 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.	<p>To specify an IPv4 address:</p> <ol style="list-style-type: none"> 1. Select the check box IPv4 address. 2. Type an IP address—for example: 10.10.10.10. NOTE: In J-Web Application package Release 14.1X53-A2, EX4600 switches display two management ports, em0 and em1. In Type the IP address and subnet mask for any of the two management ports. 3. Enter the subnet mask or address prefix. For example, 24 bits represents 255.255.255.0. 4. Click OK. <p>To specify an IPv6 address:</p> <ol style="list-style-type: none"> 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.

Table 5: Secure Management Access Configuration Summary (*continued*)

Field	Function	Your Action
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.
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 HTTP	Enables HTTP access on interfaces.	To enable HTTP access, select the Enable HTTP access check box. Select and clear interfaces by clicking the direction arrows: <ul style="list-style-type: none"> To enable HTTP access on an interface, add the interface to the HTTP Interfaces list. You can either select either all interfaces or specific interfaces.
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: <ul style="list-style-type: none"> 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. <p>NOTE: Specify the certificate to be used for HTTPS access.</p>
Certificates tab		

Table 5: Secure Management Access Configuration Summary (*continued*)

Certificates	<p>Displays digital certificates required for SSL access to the switch.</p> <p>Allows you to add and delete SSL certificates.</p>	<p>To add a certificate:</p> <ol style="list-style-type: none"> 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. <p>To edit a certificate, select it and click Edit.</p> <p>To delete a certificate, select it and click Delete.</p>
--------------	---	---

Release History Table

Release	Description
14.1X53-A2	In J-Web Application package Release 14.1X53-A2, EX4600 switches display two management ports, em0 and em1.

Related Documentation

- [Security Features for EX Series Switches Overview](#)
- [Understanding J-Web User Interface Sessions on page 8](#)
- [Enabling HTTPS and XNM-SSL Services on Switches Using Self-Signed Certificates \(CLI Procedure\)](#)

Generating SSL Certificates to Be Used for Secure Web Access

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
```

Related Documentation

- [Configuring Management Access for the EX Series Switch \(J-Web Procedure\) on page 16](#)
- [Security Features for EX Series Switches Overview](#)

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 on page 11](#)

Interfaces Configuration

- [Configuring Gigabit Ethernet Interfaces \(J-Web Procedure\) on page 21](#)

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 9 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 <http://www.juniper.net/techpubs/>.

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 6 on page 23](#) 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 6: Port Edit Options

Field	Function	Your Action
Port Role Options		
Port Role	<p>Specifies a profile (role) to assign to the interface.</p> <p>NOTE: After a port role is configured on the interface, you cannot specify VLAN options or IP options.</p> <p>NOTE: Port roles are not supported by the et interfaces (40-Gigabit Ethernet interfaces) on EX4300 and EX4550 switches.</p> <p>NOTE: Only the following port roles can be applied on EX8200 switch interfaces:</p> <ul style="list-style-type: none"> • Default • Layer 2 uplink • Routed uplink 	
Default	<p>Applies the default role.</p> <p>The interface family is set to ethernet-switching, port mode is set to access, and RSTP is enabled.</p> <p>To enable security configuration, select the Enable Security Configuration check box. The forwarding-options dhcp-security-arp-inspection will be configured.</p>	<ol style="list-style-type: none"> 1. Click Details to view CLI commands for this role. 2. Click OK.
Desktop	<p>Applies the desktop role.</p> <p>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.</p> <p>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.</p>	<ol style="list-style-type: none"> 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 6: Port Edit Options (*continued*)

Field	Function	Your Action
Desktop and Phone	<p>Applies the desktop and phone role.</p> <p>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 7 on page 26 for more CoS information.</p> <p>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.</p>	<ol style="list-style-type: none"> 1. Select an existing VLAN configuration or type the name of a new VLAN configuration to be associated with the interface. <p>You can also select an existing VoIP VLAN configuration or a new VoIP VLAN configuration to be associated with the interface.</p> <p>NOTE: VoIP is not supported on EX8200 switches.</p> <ol style="list-style-type: none"> 2. Click Details to view CLI commands for this role. 3. Click OK.
Wireless Access Point	<p>Applies the wireless access point role.</p> <p>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.</p>	<ol style="list-style-type: none"> 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.
Routed Uplink	<p>Applies the routed uplink role.</p> <p>The interface family is set to inet, and recommended CoS parameters are set for schedulers and classifiers. See Table 7 on page 26 for more CoS information.</p>	<p>To specify an IPv4 address:</p> <ol style="list-style-type: none"> 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. <p>To specify an IPv6 address:</p> <ol style="list-style-type: none"> 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. <p>NOTE: IPv6 is not supported on EX2200 VC switches.</p>
Layer 2 Uplink	<p>Applies the Layer 2 uplink role.</p> <p>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.</p>	<ol style="list-style-type: none"> 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.

Table 6: Port Edit Options (*continued*)

Field	Function	Your Action
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		
Port Mode	Specifies the mode of operation for the interface: trunk or access.	<p>If you select Trunk, you can:</p> <ol style="list-style-type: none"> 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. <p>If you select Access, you can:</p> <ol style="list-style-type: none"> 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. <p>NOTE: VoIP is not supported on EX8200 switches.</p> <ol style="list-style-type: none"> 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.	<p>Select one of the following values: 10 Mbps, 100 Mbps, 1000 Mbps, or Auto-Negotiation.</p> <p>NOTE: EX4300 switches support Auto-Negotiation 10M-100M apart from the values mentioned above.</p>
Duplex	Specifies the link mode.	<p>Select one: automatic, half, or full.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • For link-mode setting on EX4300, see <i>Configuring Gigabit Ethernet Interfaces (CLI Procedure)</i>.
Description	<p>Describes the link.</p> <p>NOTE: If the interface is part of a link aggregation group (LAG), only the Description option is enabled. Other Port Edit options are unavailable.</p>	Enter a brief description for the link.

Table 6: Port Edit Options (*continued*)

Field	Function	Your Action
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. <i>NOTE:</i> If the IPv4 Address check box is cleared, the interface still belongs to the inet family.	<ol style="list-style-type: none"> 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.
IPv6 Address	Specifies an IPv6 address for the interface. <i>NOTE:</i> If the IPv6 Address check box is cleared, the interface still belongs to the inet family.	<ol style="list-style-type: none"> 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. <p><i>NOTE:</i> IPv6 address is not supported on EX2200 and EX4500 switches.</p>

Table 7: Recommended CoS Settings for Port Roles

CoS Parameter	Recommended Settings
Forwarding Classes	<p>There are four forwarding classes:</p> <ul style="list-style-type: none"> • 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.

Table 7: Recommended CoS Settings for Port Roles (*continued*)

CoS Parameter	Recommended Settings
Schedulers	<p>The schedulers and their settings are:</p> <ul style="list-style-type: none"> • 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.
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 \(CLI Procedure\)](#)
- [Monitoring Interface Status and Traffic](#)
- [EX Series Switches Interfaces Overview](#)
- [Junos OS CoS for EX Series Switches Overview](#)
- [Understanding Interface Naming Conventions on EX Series Switches](#)

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 8 on page 28](#).
- **Edit**—To modify an existing route. Enter information into the routing page as described in [Table 8 on page 28](#).
- **Delete**—To delete an existing route.

Table 8: Static Routing Configuration Summary

Field	Function	Your Action
Default Route		
Default Route	<p>Specifies the default gateway for the switch.</p> <p>NOTE: IPv6 is not supported on EX2200 and EX4500 switches.</p>	<p>To specify an IPv4 address:</p> <ol style="list-style-type: none"> 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. <p>To specify an IPv6 address:</p> <ol style="list-style-type: none"> 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	<p>Specifies the next-hop address or addresses to be used when routing traffic to the static route.</p>	<p>To add an address:</p> <ol style="list-style-type: none"> 1. Click Add. 2. In the IP address dialog, enter the IP address. <p>NOTE: If a route has multiple next-hop addresses, traffic is routed across each address in round-robin fashion.</p> <ol style="list-style-type: none"> 3. Click OK. <p>To delete a next-hop address, select it from the list and click Delete.</p>

- Related Documentation**
- *Configuring Static Routing (CLI Procedure)*
 - *Monitoring Routing Information*
 - *Layer 3 Protocols Supported on EX Series Switches*

Software Installation and Upgrades

- [Updating J-Web Interface on EX Series Switches \(J-Web Procedure\) on page 29](#)
- [Upgrading Junos OS on EX Series Switches \(J-Web Procedure\) on page 30](#)

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

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 HTTP, 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 on page 29](#)
- [Installing J-Web Application Package by Using Manual Update on page 30](#)

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.

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.

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

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 from a remote server by using FTP or HTTP, or by copying the file to the EX Series switch.

- [Installing Junos OS Upgrades from a Remote Server on page 31](#)
- [Installing Junos OS Upgrades by Uploading File from Local Computer on page 31](#)

Installing Junos OS Upgrades from a Remote Server

To install Junos OS upgrade from a remote server by using FTP or HTTP:

1. Download the software package as described in *Downloading Software Packages from Juniper Networks*.
2. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. In the J-Web interface, select **Maintain > Update Junos**.
4. In the *Update Junos* section, select **Remote Server**. The *Install Package* section appears below the Update Junos section.
5. In the Install Package section, enter information into the fields described in [Table 9 on page 31](#).
6. Click **Fetch and Install Package**. The software is activated after the switch has rebooted.

Table 9: Install Remote Summary

Field	Function	Your Action
Package Location (required)	Specifies the FTP or HTTP server, file path, and software package name.	Type the full address of the software package location on the FTP or HTTP server—one of the following: <code>ftp://hostname/pathname/package-name</code> <code>http://hostname/pathname/package-name</code>
User	Specifies the username, if the server requires one.	Type the username.
Password	Specifies the password, if the server requires one.	Type the password.
Reboot If Required	<p>NOTE: Reboot is disabled if you enter a J-Web Application package name in the Package Location text box. To enable Reboot, enter a Junos package name in the Package Location text box.</p> <p>If this box is checked, the switching platform will automatically reboot when the upgrade is complete.</p>	Check the box if you want the switching platform to reboot automatically when the upgrade is complete.

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 10 on page 32](#).
5. Click **Upload and Install Package**. The software is activated after the switching platform completes the installation procedure.

Table 10: 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.

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 11 on page 33](#).
 - **Edit**—Select this option to edit an existing user's details. Enter details as described in [Table 11 on page 33](#).
 - **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 12 on page 34](#).
 - **Edit**—Select this option to modify the authentication server details. Enter details as described in [Table 12 on page 34](#).
 - **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 12 on page 34](#).
 - **Edit**—Select this option to modify the authentication server details. Enter details as described in [Table 12 on page 34](#).
 - **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 11: 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.
Login Class (required)	Defines the user's access privilege.	Select the user's login class from the list: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 12: 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.
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 \(J-Web Procedure\) on page 16](#)

CHAPTER 3

Maintaining the Switch Using J-Web Interface

Using the Maintaining tab in the J-Web Platform package, you can update to J-Web Application package, upgrade Junos OS, or reboot your switch. The following topics describe the maintaining pages supported on J-Web for EX Series switches:

- [Updating J-Web Interface on EX Series Switches \(J-Web Procedure\) on page 29](#)
- [Upgrading Junos OS on EX Series Switches \(J-Web Procedure\) on page 30](#)
- [Rebooting or Halting the EX Series Switch \(J-Web Procedure\) on page 20](#)

