



J-Web User Interface Guide for JUNOS® Software for EX-series Switches

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Part Number: , Revision B1

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOSe is a trademark of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

JUNOS® Software for EX-series J-Web User Interface Guide for JUNOS® Software for EX-series Switches
Copyright © 2008, Juniper Networks, Inc.
All rights reserved. Printed in USA.

Writing: Vinita Kurup
Editing: Cindy Martin
Illustration: Faith Bradford Brown
Cover Design:

Revision History
15 March 2008—Revision 9.0 R1
28 April 2008—Revision 9.1 R1
12 August 2008—Revision 9.2 R1

The information in this document is current as of the date listed in the revision history.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. The JUNOS software has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

SOFTWARE LICENSE

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions.

Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details.

For complete product documentation, please see the Juniper Networks Web site at www.juniper.net/techpubs.

End User License Agreement

READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. **The Parties.** The parties to this Agreement are Juniper Networks, Inc. and its subsidiaries (collectively "Juniper"), and the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").
2. **The Software.** In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, and updates and releases of such software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller. "Embedded Software" means Software which Juniper has embedded in the Juniper equipment.
3. **License Grant.** Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:
 - a. Customer shall use the Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.
 - b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius software on multiple computers requires multiple licenses, regardless of whether such computers are physically contained on a single chassis.
 - c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.
 - d. For any trial copy of the Software, Customer's right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.
 - e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer's enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. **Use Prohibitions.** Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use the Embedded Software on non-Juniper equipment; (j) use the Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.
5. **Audit.** Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.
6. **Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. **Ownership.** Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.
8. **Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.
9. **Termination.** Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.
10. **Taxes.** All license fees for the Software are exclusive of taxes, withholdings, duties, or levies (collectively "Taxes"). Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software.
11. **Export.** Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.
12. **Commercial Computer Software.** The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT III) as applicable.
13. **Interface Information.** To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.
14. **Third Party Software.** Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at <http://www.gnu.org/licenses/gpl.html>, and a copy of the LGPL at <http://www.gnu.org/licenses/lgpl.html>.
15. **Miscellaneous.** This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattaché, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

Table of Contents

	About This Topic Collection	ix
	How To Use This Guide	ix
	List of EX-series Guides for JUNOS 9.2	ix
	Downloading Software	x
	Documentation Symbols Key	x
	Notice Icons	x
	Text and Syntax Conventions	x
	Documentation Feedback	xi
	Getting Support	xii
Part 1	J-Web User Interface	
Chapter 1	J-Web User Interface Overview	3
	J-Web User Interface for EX-series Switches Overview	3
	Understanding J-Web Configuration Tools	5
	Using the CLI Viewer in the J-Web Interface to View Configuration Text	6
	Using the Point and Click CLI Tool in the J-Web Interface to Edit Configuration Text	6
	Text	6
	Using the CLI Editor in the J-Web Interface to Edit Configuration Text	8
Chapter 2	Installing and Starting J-Web Software	9
	Starting the J-Web Interface	9
	Understanding How to Use the J-Web Interface to View System Information	10
Chapter 3	Managing J-Web Software	11
	Configuring System Identity for the EX-Series Switch (J-Web Procedure)	11
	Configuring Management Access for the EX-series Switch (J-Web Procedure)	12
	Managing Users (J-Web Procedure)	14
	Configuring Date and Time for the EX-series Switch (J-Web Procedure)	16
	Understanding J-Web User Interface Sessions	17
	Generating SSL Certificates to Be Used for Secure Web Access	17
	Rebooting or Halting the EX-series Switch (J-Web Procedure)	18

Part 2

Index

Index23

List of Tables

- Table 1: J-Web Interface4
- Table 2: Switching Platform Configuration Interfaces5
- Table 3: J-Web Edit Point & Click Configuration Links7
- Table 4: J-Web Edit Point & Click Configuration Icons7
- Table 5: J-Web Edit Point & Click Configuration Buttons8
- Table 6: Set Up Configuration Summary11
- Table 7: Secure Management Access Configuration Summary12
- Table 8: User Management > Add a User Configuration Page Summary15
- Table 9: Add an Authentication Server16
- Table 10: Date and Time Settings16

About This Topic Collection

- How To Use This Guide on page ix
- List of EX-series Guides for JUNOS 9.2 on page ix
- Downloading Software on page x
- Documentation Symbols Key on page x
- Documentation Feedback on page xi
- Getting Support on page xii

How To Use This Guide

Complete documentation for EX-series product family is provided on web pages at http://www.juniper.net/techpubs/en_US/release-independent/information-products/pathway-pages/exseries/product/index.html. We have selected content from these web pages and created a number of EX-series guides that collect related topics into a book-like format so that the information is easy to print and easy to download to your local computer.

This guide, *J-Web User Interface Guide for JUNOS Software for EX-series Switches*, collects together information about the J-Web user interface in JUNOS Software for EX-series Release 9.2. For release-specific information, see the release notes at http://www.juniper.net/techpubs/en_US/junos9.2/information-products/pathway-pages/exseries/software/index.html.

List of EX-series Guides for JUNOS 9.2

Title	Description
<i>Complete Hardware Guide for EX 3200 and EX 4200 Switches</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance
<i>Complete Software Guide for JUNOS® Software for EX-series, Release 9.2</i>	Software feature descriptions, configuration examples and tasks, and reference pages for configuration statements and operational commands
<i>J-Web User Interface Guide for JUNOS for EX-series Software</i>	How to use the J-Web graphical user interface (GUI) with JUNOS for EX-series software
<i>JUNOS® Software for EX-series Release Notes, Release 9.2</i>	Summary of hardware and software features and known problems with the software and hardware

Downloading Software

You can download the JUNOS for EX-series software from the Download Software area at <http://www.juniper.net/customers/support/>. To download the software, you must have a Juniper Networks user account. For information about obtaining an account, see <http://www.juniper.net/entitlement/setupAccountInfo.do>.

Documentation Symbols Key

Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the <code>configure</code> command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> ■ Introduces important new terms. ■ Identifies book names. ■ Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> ■ A policy <i>term</i> is a named structure that defines match conditions and actions. ■ <i>JUNOS System Basics Configuration Guide</i> ■ RFC 1997, <i>BGP Communities Attribute</i>

<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Plain text like this	Represents names of configuration statements, commands, files, and directories; IP addresses; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> ■ To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. ■ The console port is labeled CONSOLE.
< > (angle brackets)	Enclose optional keywords or variables.	stub <default-metric <i>metric</i> >;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Enclose a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identify a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> ■ In the Logical Interfaces box, select All Interfaces. ■ To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web selections.	In the configuration editor hierarchy, select Protocols > Ospf .

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. Send email to techpubs-comments@juniper.net with the following:

- Document URL or title
- Page number if applicable
- Software version
- Your name and company

Getting Support

For technical support, open a support case with the Case Manager link at <http://www.juniper.net/support/> or call 1-888-314-JTAC (from the United States, Canada, or Mexico) or 1-408-745-9500 (from elsewhere).

Part 1

J-Web User Interface

- J-Web User Interface Overview on page 3
- Installing and Starting J-Web Software on page 9
- Managing J-Web Software on page 11

Chapter 1

J-Web User Interface Overview

- J-Web User Interface for EX-series Switches Overview on page 3
- Understanding J-Web Configuration Tools on page 5
- Using the CLI Viewer in the J-Web Interface to View Configuration Text on page 6
- Using the Point and Click CLI Tool in the J-Web Interface to Edit Configuration Text on page 6
- Using the CLI Editor in the J-Web Interface to Edit Configuration Text on page 8

J-Web User Interface for EX-series Switches Overview

You can use two interfaces to monitor, configure, troubleshoot, and manage an EX-series switch: the J-Web graphical user interface and the JUNOS command-line interface (CLI). Both of these user interfaces are shipped with the switch. This topic describes the J-Web interface. You can navigate the J-Web interface, scroll pages, and expand and collapse elements as you do in a typical Web browser interface. For information about the CLI user interface, see CLI User Interface Overview.

Use Internet Explorer version 6.0 and higher, or Firefox version 2.0 and higher, to access the J-Web interface.



NOTE: The browser and the network must support receiving and processing HTTP 1.1 GZIP compressed data.

Each page of the J-Web interface is divided into panes.

- Top pane—Displays system identity information and links.
- Main pane—Location where you monitor, configure, diagnose (troubleshoot), and manage (maintain) the switch by entering information in text boxes, making selections, and clicking buttons.
- Side pane—Displays suboptions of the Monitor, Configure, Troubleshoot, or Maintain task currently displayed in the main pane. Click a suboption to access it in the main pane.

The layout of the panes allows you to quickly navigate through the interface. Table 1 on page 4 summarizes the elements of the J-Web interface.

The J-Web interface provides CLI tools that allow you to perform all of the tasks that you can perform from the JUNOS command-line interface (CLI), including a CLI Viewer to view the current configuration, a CLI Editor for viewing and modifying the configuration, and a Point & Click CLI editor that allows you to click through all of the available CLI statements.

Table 1: J-Web Interface

J-Web Interface Element	Description
Top Pane	
hostname	Hostname of the switch.
Logged in as: username	Username you used to log in to the switch.
Help	Link to context-sensitive help information.
About	Displays information about the J-Web interface, such as the version number.
Logout	Ends your current login session with the switch and returns you to the login page.
Taskbar	<p>Menu of J-Web main options. Click the tab to access the option.</p> <ul style="list-style-type: none"> ■ Dashboard—Displays a high-level, graphical view of the chassis and status of the switch. It displays system health information, alarms, and system status. ■ Configure—Configure the switch, and view configuration history. ■ Monitor—View information about configuration and hardware on the switch. ■ Maintain—Manage files and licenses, upgrade software, and reboot the switch. ■ Troubleshoot—Run diagnostic tools to troubleshoot network issues.
Main Pane	
Help (?) icon	Displays useful information—such as the definition, format, and valid range of an option—when you move the cursor over the question mark.
Red asterisk (*)	Indicates a required field.
Icon legend	<p>(Applies to the Point & Click CLI editor only) Explains icons that appear in the user interface to provide information about configuration statements:</p> <ul style="list-style-type: none"> ■ C—Comment. Move your cursor over the icon to view a comment about the configuration statement. ■ I—Inactive. The configuration statement does not affect the switch. ■ M—Modified. The configuration statement has been added or modified. ■ *—Mandatory. The configuration statement must have a value.
Task Pane	
Configuration hierarchy	<p>(Applies to the JUNOS 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 plus signs (+) to expand individual items. ■ Click minus signs (-) to hide individual items.

- Related Topics**
- EX-series Switch Software Features Overview
 - EX-series Switch Hardware Overview
 - EX-series Switch Software Features Overview
 - Connecting and Configuring the EX-series Switch (J-Web Procedure)
 - CLI User Interface Overview

Understanding J-Web Configuration Tools

The J-Web graphical user interface (GUI) allows you to monitor, configure, troubleshoot, and manage the switching platform by means of a Web browser with Hypertext Transfer Protocol (HTTP) or HTTP over Secure Sockets Layer (HTTPS) enabled. The J-Web interface provides access to all the configuration statements supported by the switch, so you can fully configure the switch without using the CLI.

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

- Configure menu
- Point & Click CLI Editor
- CLI Editor

Table 2 on page 5 gives a comparison of the three methods of configuration.

Table 2: Switching Platform Configuration Interfaces

Tool	Description	Function	Use
Configure menu	<p>Web browser pages for setting up the switch quickly and easily without configuring each statement individually.</p> <p>For example, use the Virtual Chassis Configuration page to configure the virtual chassis parameters on the switch.</p>	<p>Configure basic switch platform services:</p> <ul style="list-style-type: none"> ■ Interfaces ■ Switching ■ Virtual Chassis ■ Security ■ Services ■ System Properties ■ Routing 	Use for basic configuration.
Point & Click CLI editor	<p>Web browser pages divided into panes in which you can do any of the following:</p> <ul style="list-style-type: none"> ■ Expand the entire configuration hierarchy and click a configuration statement to view or edit. The main pane displays all the options for the statement, with a text box for each option. ■ Paste a complete configuration hierarchy into a scrollable text box, or edit individual lines. ■ Upload or download a complete configuration. ■ Roll back to a previous configuration. ■ Create or delete a rescue configuration. 	<p>Configure all switching platform services:</p> <ul style="list-style-type: none"> ■ System parameters ■ User Accounting and Access ■ Interfaces ■ VLAN properties ■ Virtual Chassis properties ■ Secure Access ■ Services ■ Routing protocols 	Use for complete configuration if you are not familiar with the JUNOS CLI or prefer a graphical interface.

Table 2: Switching Platform Configuration Interfaces (continued)

CLI editor	Interface in which you do any of the following: <ul style="list-style-type: none"> ■ Type commands on a line and press Enter to create a hierarchy of configuration statements. ■ Create an ASCII text file that contains the statement hierarchy. ■ Upload a complete configuration, or roll back to a previous configuration. ■ Create or delete a rescue configuration. 	Configure all switching platform services: <ul style="list-style-type: none"> ■ System parameters ■ User Accounting and Access ■ Interfaces ■ VLAN properties ■ Virtual Chassis properties ■ Secure Access ■ Services ■ Routing protocols 	Use for complete configuration if you know the JUNOS CLI or prefer a command interface.
------------	---	---	---

- Related Topics**
- Understanding J-Web User Interface Sessions on page 17
 - J-Web User Interface for EX-series Switches Overview on page 3
 - Connecting and Configuring the EX-series Switch (J-Web Procedure)
 - Configuration Files Terms

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

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

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

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

- Related Topics**
- Understanding J-Web Configuration Tools on page 5

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

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

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

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

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

To include, edit, or delete statements in the candidate configuration, click one of the links described in Table 3 on page 7. Then specify configuration information by typing in a field, selecting a value from a list, or clicking a check box (toggle).

Table 3: J-Web Edit Point & Click Configuration Links

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

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

The main pane includes icons that display information about statements and identifiers when you place your cursor over them. Table 4 on page 7 describes these icons.

Table 4: J-Web Edit Point & Click Configuration Icons

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

After typing or selecting your configuration edits, click a button in the main pane (described in Table 5 on page 8) to apply your changes or cancel them, refresh the display, or discard parts of the candidate configuration. An updated configuration does not take effect until you commit it.

Table 5: J-Web Edit Point & Click Configuration Buttons

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

- Related Topics**
- CLI User Interface Overview
 - Understanding J-Web Configuration Tools on page 5

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

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

To edit the entire configuration in text format:



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

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

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

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

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

- Related Topics**
- CLI User Interface Overview
 - Understanding J-Web Configuration Tools on page 5

Chapter 2

Installing and Starting J-Web Software

- Starting the J-Web Interface on page 9
- Understanding How to Use the J-Web Interface to View System Information on page 10

Starting the J-Web Interface

You can use the J-Web graphical 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 **Log In**.

To correct or change the username or password you typed, click **Reset**, type the new entry or entries, and click **Log In**.



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

The Chassis Dashboard information page appears.

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

- Related Topics**
- J-Web User Interface for EX-series Switches Overview on page 3
 - Understanding How to Use the J-Web Interface to View System Information on page 10

Understanding How to Use the J-Web Interface to View System Information

When you log into the J-Web interface, the first page that is displayed is the Dashboard and Chassis Information page. This page displays:

- Chassis view—A high-level, graphical view of the chassis. It indicates the state of the interfaces. When the administrative and operational status of the interface is up, it is displayed in green. If the administrative status is down, the interface is displayed in grey. And, if the administrative status is up and operational status is down, the interface is displayed in amber. The image is a replica of the switch. If you are connected to a virtual chassis, the image includes all the member switches of the virtual chassis.

The chassis view also displays a count of alarms generated in the system; major alarms are displayed in red, and minor alarms in orange.

- Dashboard view—The dashboard comprises:
 - System Information table—Displays the system name, device model, inventory details (number of FPCs, and the number of member devices if the device is operating in virtual chassis mode), JUNOS image, boot image, device uptime, and the last configured time. In a virtual chassis setup when you click on a member switch, details of the selected member are displayed.
 - Health Status table—Displays details of the memory utilized on the routing engine, temperature, CPU load, and fan status. A fan running at normal speed is displayed in green. If the fan is running at maximum speed or not running at all, it is displayed in red. For a virtual chassis the status of the fans for the selected member is displayed. If a fan in any of the member's is not running at normal speed, a status of **Not Ok** is displayed.
 - Capacity Utilization—Displays the total number of active ports versus the total number of ports, the total number of MAC-Table entries versus the maximum number of MAC-Table entries permitted, and the total number of configured VLANs versus the maximum number of VLANs that are supported.
 - Alarm table—This table displays information about the last five alarms raised in the system. For example, if there are 5 major alarms details of these 5 major alarms are displayed. If there are 4 major and 3 minor alarms, details of the 4 major and one minor alarm is displayed.

- Related Topics**
- J-Web User Interface for EX-series Switches Overview on page 3
 - Checking Active Alarms with the J-Web Interface

Chapter 3

Managing J-Web Software

- Configuring System Identity for the EX-Series Switch (J-Web Procedure) on page 11
- Configuring Management Access for the EX-series Switch (J-Web Procedure) on page 12
- Managing Users (J-Web Procedure) on page 14
- Configuring Date and Time for the EX-series Switch (J-Web Procedure) on page 16
- Understanding J-Web User Interface Sessions on page 17
- Generating SSL Certificates to Be Used for Secure Web Access on page 17
- Rebooting or Halting the EX-series Switch (J-Web Procedure) on page 18

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

To configure identification details for the switch:

1. Select **Configure > System Properties > System Identity**. The System Identity page displays configuration details.
2. To modify the configuration, click **Edit**. Enter information into the System Identity page, as described in Table 6 on page 11.

Table 6: Set Up Configuration Summary

Field	Function	Your Action
Host Name	Defines the hostname of the switching platform.	Type the hostname.
Domain Name	Defines the network or subnetwork that the machine belongs to.	Type the domain name.
Root Password	Sets the root password that user root can use to log in to the switching platform.	Type a plain-text password. The system encrypts the password. NOTE: After a root password has been defined, it is required when you log in to the J-Web user interface or the CLI.
Confirm Root Password	Verifies that the root password has been typed correctly.	Retype the password.

Table 6: Set Up Configuration Summary (continued)

Field	Function	Your Action
DNS Name Servers	Specifies a DNS server for the switching platform to use to resolve hostnames into addresses.	To add an IP address, click Add . To edit an IP address, click Edit . To delete an IP address, click Delete .
Domain Search	Specifies the domains to be searched.	To add a domain, click Add . To edit a domain click Edit . To delete a domain, click Delete .

Related Topics ■ Configuring Date and Time for the EX-series Switch (J-Web Procedure) on page 16

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 Hypertext Transfer Protocol (HTTP). HTTP allows easy Web access but 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 HTTP over Secure Sockets Layer (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 JUNOScript 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 7 on page 12.
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 JUNOScript access— To use this option, you must have a JUNOScript client such as JUNOScope. For information about how to log into JUNOScope, see the *JUNOScope Software User Guide*.

Table 7: Secure Management Access Configuration Summary

Field	Function	Your Action
Management Access tab		

Table 7: Secure Management Access Configuration Summary (continued)

Field	Function	Your Action
Management Port IP	Specifies the management port IP address.	Type a 32-bit IP address, in dotted decimal notation.
Subnet Mask	Specifies the subnet mask.	Enter the subnet mask or address prefix. For example, 24 bits represents 255.255.255.0.
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.	Type a 32-bit IP address, in dotted decimal notation.
Services	Specifies services to be enabled: telnet and SSH.	Select to enable the required services.
Enable JUNOScript over Clear Text	Enables clear text access to the JUNOScript XML scripting API.	To enable clear text access, select the Enable JUNOScript over Clear Text check box.
Enable JUNOScript over SSL	Enables secure SSL access to the JUNOScript XML scripting API.	To enable SSL access, select the Enable JUNOScript over SSL check box.
JUNOScript 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 JUNOScript SSL Certificate list—for example, new .
HTTP Web Access		
Enable HTTP Access	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 all interfaces or specific interfaces.
HTTPS Web Access		
Enable HTTPS Access	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 all interfaces or specific interfaces. <p>NOTE: Specify the certificate to be used for HTTPS access.</p>
Certificates tab		

Table 7: 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 <i>Generating SSL Certificates</i> for more information. 2. Click Add. The Add a Local Certificate page opens. 3. Type a name in the Certificate Name box—for example, <i>new</i>. 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>
--------------	---	--

-
- Related Topics**
- Security Features for EX-series Switches Overview
 - Understanding J-Web User Interface Sessions on page 17

Managing Users (J-Web Procedure)

You can use the Users Configuration page for user information to add new users to a switching platform. 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. In the J-Web interface, 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 8 on page 15.
 - **Edit**—Select this option to edit an existing user's details. Enter details as described in Table 8 on page 15.
 - **Delete**—Select this option to delete a user.
4. Click any desired 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:
 - Add—Select this option to add an authentication server. Enter details as described in Table 9 on page 16.
 - Edit—Select this option to modify the authentication server details. Enter details as described in Table 9 on page 16.
 - Delete—Select this option to delete an authentication server from the list.
- TACACS server—Click one:
 - Add—Select this option to add an authentication server. Enter details as described in Table 9 on page 16.
 - Edit—Select this option to modify the authentication server details. Enter details as described in Table 9 on page 16.
 - Delete—Select this option to delete an authentication server from the list.

Table 8: User Management > Add a User 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.
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.	<p>Select the user's login class from the list:</p> <ul style="list-style-type: none"> ■ operator ■ read-only ■ super-user/superuser ■ unauthorized <p>This list also includes any user-defined login classes.</p>
Login Password (required)	Specifies the login password for this user.	<p>Type the login password for this user. The login password must meet these criteria:</p> <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.

Table 8: User Management > Add a User Configuration Page Summary (continued)

Field	Function	Your Action
Confirm Password (required)	Verifies the login password for this user.	Retype the login password for this user.

Table 9: 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 Number	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.
Timeout	Specifies the time interval to wait before the connection to the server is closed.	Type the interval in seconds.

Related Topics ■ Configuring Management Access for the EX-series Switch (J-Web Procedure) on page 12

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

To configure date and time:

1. Select **Configure>System Properties>Date & Time**.
2. To modify the information, click **Edit**. Enter information into the **Edit Date & Time** page, as described in Table 10 on page 16.
3. Click one:
 - To apply the configuration, click **OK**.
 - To cancel your entries and return to the System Properties page, click **Cancel**.

Table 10: Date and Time Settings

Time

Table 10: Date and Time Settings (continued)

Time Zone	Identifies the timezone that the switching platform is located in.	Select the appropriate time zone from the list.
Set Time	Synchronizes the system time with that of the NTP server. You can also manually set the system time and date.	To immediately set the time, click one: <ul style="list-style-type: none"> ■ Synchronize with PC time—The switch synchronizes the time with that of the PC. ■ NTP Servers—The switch sends a request to the NTP server and synchronizes the system time. ■ Manual—A pop-up window allows you to select the current date and time from a list.

Related Topics ■ J-Web User Interface for EX-series Switches Overview on page 3

Understanding J-Web User Interface Sessions

You establish a J-Web session with the switch through an HTTP-enabled or HTTPS-enabled Web browser. The HTTPS protocol, which uses 128-bit encryption, is available only in domestic versions of the JUNOS software. 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 17.

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 Topics ■ 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 12

Generating SSL Certificates to Be Used for Secure Web Access

To enable secure Web access, you must generate a digital SSL certificate and then enable HTTPS access on the switching platform.

To generate an SSL certificate:

1. Enter the following **openssl** command in your Secure Shell command-line interface. 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
```

Replace *filename* with the name of a file in which you want the SSL certificate to be written—for example, *new.pem*.

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 *new.pem*.

```
cat new.pem
```



NOTE: When you are ready to install the SSL certificate, open this file and copy its contents so you can paste it into the Certificate box on the Secure Access Configuration page.

You can use either J-Web Configuration or a configuration editor to install the SSL certificate and enable HTTPS.

- Related Topics**
- Security Features for EX-series Switches Overview
 - Configuring Management Access for the EX-series Switch (J-Web Procedure) on page 12

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 Topics ■ Starting the J-Web Interface on page 9

Part 2

Index

- Index on page 23

Index

A

- access privileges
 - specifying14
- Add a RADIUS Server page
 - field summary.....16
- Add a User Configuration page
 - field summary.....15
- authentication
 - specifying access privileges14

C

- certificates *See* SSL certificates
- chassis dashboard.....10
- Configuration
 - adding users.....14
 - secure Web access.....12
- Configuration text
 - editing.....6, 8
 - viewing.....6
- Configuring
 - management access.....12

D

- dashboard,
 - chassis view.....10
- default gateway
 - defining.....13
- DNS server
 - defining12
- domain name
 - defining11

E

- Edit
 - configuration text.....8

H

- halting a switching platform
 - with J-Web.....18

- halting a switching platform immediately
 - with J-Web18
- hostname
 - defining11
- HTTP (Hypertext Transfer Protocol)
 - enabling Web access12
- HTTPS (Hypertext Transfer Protocol over SSL)
 - enabling secure access12
 - Quick Configuration.....12
- Hypertext Transfer Protocol *See* HTTP
- Hypertext Transfer Protocol over SSL *See* HTTPS

J

- JUNOScript API
 - enabling secure access.....12
- JUNOScript over SSL.....12

L

- login classes
 - specifying14

M

- Management access
 - configuring.....12
- managing
 - reboots.....18

P

- passwords
 - RADIUS secret.....16

R

- RADIUS
 - secret16
- reboot immediately
 - with J-Web.....18
- rebooting
 - with J-Web18
- root password
 - defining11

S

- scheduling a reboot
 - with J-Web.....18
- secret
 - RADIUS16
- secure access
 - JUNOScript SSL access.....12
- Secure Access page
 - field summary.....12
- Set Up page
 - field summary.....11
- software
 - halting immediately (J-Web)18
- SSL (Secure Sockets Layer)
 - enabling secure access (Quick Configuration).....12
- SSL certificates
 - adding14
- switching platform
 - halting (J-Web).....18
 - rebooting (J-Web).....18
- System identity
 - configuring.....11
- system time
 - defining17

T

- time zone
 - defining17

U

- username
 - specifying14
- users
 - adding14

V

- View
 - configuration text.....6

W

Web access, secure *See* secure access