



JUNOS® Software for EX Series Ethernet Switches, Release 10.0: User and Access Management

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

Revision 1
Published: 2009-11-04

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, ScreenOS, and Steel-Belted Radius 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 Ethernet Switches, Release 10.0: User and Access Management

Copyright © 2009, Juniper Networks, Inc.

All rights reserved. Printed in USA.

Writing:

Editing:

Illustration:

Cover Design:

Revision History

4 November 2009—Revision 1

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

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 (i) Juniper Networks, Inc. (if the Customer’s principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer’s principal office is located outside the Americas) (such applicable entity being referred to herein as “Juniper”), and (ii) 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, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. “Software” also includes updates, upgrades and new releases of such software. “Embedded Software” means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the 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 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 or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations 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 Embedded Software on non-Juniper equipment; (j) use Embedded 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 payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer's payment of any withholding taxes; completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer's non-compliance or delay with its responsibilities herein. Customer's obligations under this Section shall survive termination or expiration of this Agreement.
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 rattache, 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 Release 10.0	ix
Downloading Software	x
Documentation Symbols Key	xi
Documentation Feedback	xii
Requesting Technical Support	xiii
Self-Help Online Tools and Resources	xiii
Opening a Case with JTAC	xiii

Part 1

User Access and Management on EX Series Switches

Chapter 1

User Access and Management on EX Series Switches	3
JUNOS Software—Overview	3
EX Series Switch Software Features Overview	3
Understanding Software Infrastructure and Processes	15
Routing Engine and Packet Forwarding Engine	15
JUNOS Software Processes	16
Configuring User Access	17
Configuring Management Access for the EX Series Switch (J-Web Procedure)	17
Generating SSL Certificates to Be Used for Secure Web Access	19
Monitoring the Switch, Users, and Traffic	20
Managing Users (J-Web Procedure)	20
Configuring MS-CHAPv2 to Provide Password-Change Support (CLI Procedure)	23
Monitoring Hosts Using the J-Web Ping Host Tool	23
Monitoring Switch Control Traffic	25
Monitoring Network Traffic Using Traceroute	27
Monitoring System Properties	28
Monitoring System Process Information	30

About This Topic Collection

- How to Use This Guide on page ix
- List of EX Series Guides for JUNOS Release 10.0 on page ix
- Downloading Software on page x
- Documentation Symbols Key on page xi
- Documentation Feedback on page xii
- Requesting Technical Support on page xiii

How to Use This Guide

Complete documentation for the EX Series product family is provided on webpages at http://www.juniper.net/techpubs/en_US/release-independent/information-products/pathway-pages/ex-series/product/index.html. We have selected content from these webpages 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.

The release notes are at

http://www.juniper.net/techpubs/en_US/junos10.0/information-products/topic-collections/release-notes/10.0/junos-release-notes-10.0.pdf.

List of EX Series Guides for JUNOS Release 10.0





Title	Description
<i>Complete Hardware Guide for EX3200 and EX4200 Switches</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX3200 and EX4200 switches
<i>Complete Hardware Guide for EX8208 Switches</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX8208 switches
<i>Complete Hardware Guide for EX8216 Switches</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX8216 switches
<i>Complete Software Guide for JUNOS® Software for EX Series Switches, Release 10.0</i>	Software feature descriptions, configuration examples, and tasks for JUNOS Software for EX Series switches

Title	Description
Software Topic Collections	Software feature descriptions, configuration examples and tasks, and reference pages for configuration statements and operational commands (This information also appears in the <i>Complete Software Guide</i> .)
<i>JUNOS® Software for EX Series Switches, Release 10.0: Access Control</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Alarms and System Log Messages</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Configuration and File Management</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Class of Service</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Device Security</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Ethernet Switching</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Interfaces</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Layer 3 Protocols</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: MPLS</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Multicast</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Network Management and Monitoring</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Port Security</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Routing Policy and Packet Filtering</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Spanning-Tree Protocols</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: System Setup</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: User and Access Management</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Virtual Systems</i>	

Downloading Software

You can download JUNOS Software for EX Series switches 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 <code>stub</code> statement at the [edit protocols ospf area area-id] hierarchy level. ■ The console port is labeled CONSOLE.

Text and Syntax Conventions		
Convention	Description	Examples
< > (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 e-mail to techpubs-comments@juniper.net with the following:

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

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at <http://www.juniper.net/customers/support/downloads/710059.pdf> .
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/> .
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/> .
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see [http://www.juniper.net/support/requesting support.html](http://www.juniper.net/support/requesting_support.html) .

Part 1

User Access and Management on EX Series Switches

- User Access and Management on EX Series Switches on page 3

Chapter 1

User Access and Management on EX Series Switches

- JUNOS Software—Overview on page 3
- Configuring User Access on page 17
- Monitoring the Switch, Users, and Traffic on page 20

JUNOS Software—Overview

- EX Series Switch Software Features Overview on page 3
- Understanding Software Infrastructure and Processes on page 15

EX Series Switch Software Features Overview

Table 1 on page 3 lists the Juniper Networks EX Series Ethernet Switch software features and the Juniper Networks JUNOS Software release in which they were introduced.

Table 1: Summary of Software Features Available on EX Series Switches

Feature Category	Feature	First Release EX3200 and EX4200 Switches	First Release EX8200 Switches
Activity Logging and Monitoring	J-Web event view for system log messages	JUNOS 9.0R2	JUNOS 9.4R1
	Real-time performance monitoring (RPM)	JUNOS 9.3R2	Not supported
	System logging (syslog) over IPv4	JUNOS 9.0R2	JUNOS 9.4R1
	System logging (syslog) over IPv6	JUNOS 9.3R2	Not supported
	Traceroute tool in J-Web interface	JUNOS 9.0R2	JUNOS 9.4R1

Table 1: Summary of Software Features Available on EX Series Switches (continued)

Feature Category	Feature	First Release EX3200 and EX4200 Switches	First Release EX8200 Switches
Administration	Automatic software download	JUNOS 9.6R1	Not supported
	Configuration rollback	JUNOS 9.0R2	JUNOS 9.4R1
	Confirmation of configuration changes	JUNOS 9.0R2	JUNOS 9.4R1
	Software upgrades	JUNOS 9.0R2	JUNOS 9.4R1
	Support for RADIUS external administrator databases	JUNOS 9.0R2	JUNOS 9.4R1
	Supports the following features for automating network operations and troubleshooting: <ul style="list-style-type: none"> <li data-bbox="505 810 704 842">■ Commit scripts <li data-bbox="505 846 724 877">■ Operation scripts <li data-bbox="505 882 691 913">■ Event policies 	JUNOS 9.0R2	JUNOS 9.4R1
Encapsulation	802.1Q encapsulation tags	JUNOS 9.0R2	JUNOS 9.4R1
	802.1Q filtering and forwarding	JUNOS 9.0R2	JUNOS 9.4R1
	Ethernet: <ul style="list-style-type: none"> <li data-bbox="505 1098 964 1129">■ Media access control (MAC) encapsulation <li data-bbox="505 1134 704 1165">■ 802.1p tagging 	JUNOS 9.0R2	JUNOS 9.4R1

Table 1: Summary of Software Features Available on EX Series Switches (continued)

Feature Category	Feature	First Release EX3200 and EX4200 Switches	First Release EX8200 Switches
High Availability and Resiliency	Graceful protocol restart for IS-IS	JUNOS 9.3R2	JUNOS 9.4R1
	Graceful protocol restart for OSPF and BGP	JUNOS 9.0R2	JUNOS 9.4R1
	Graceful Routing Engine switchover (GRES) for EX4200 Virtual Chassis configurations	JUNOS 9.1R1	Not applicable
	Graceful Routing Engine switchover (GRES) for ARP entries	JUNOS 9.2R1	JUNOS 9.4R1
	Graceful Routing Engine switchover (GRES) for the forwarding database	JUNOS 9.2R1	JUNOS 9.4R1
	Graceful Routing Engine switchover (GRES) for port security	JUNOS 9.2R1	JUNOS 9.6R1
	Link aggregation control protocol (LACP)	JUNOS 9.0R2	JUNOS 9.4R1
	Link aggregation control protocol (LACP) support for dual-homing applications in data centers	JUNOS 10.0R1	
	Link aggregation groups (LAGs)	JUNOS 9.0R2	JUNOS 9.4R1
	Link aggregation groups (LAGs) over Virtual Chassis ports (VCPs)	JUNOS 9.6R1	Not applicable
	Redundant trunk groups	JUNOS 9.0R2	JUNOS 9.4R1
	Virtual Chassis <ul style="list-style-type: none"> ■ Atomic software upgrade ■ Fast failover ■ Split and merge 	JUNOS 9.3R2	Not applicable
	Virtual Chassis <ul style="list-style-type: none"> ■ Automatic software update on prospective member switches ■ Front-panel configuration of uplink module ports as Virtual Chassis ports (VCPs) 	JUNOS 10.0R1	Not applicable
	Virtual Chassis <ul style="list-style-type: none"> ■ Autoprovisioning of Virtual Chassis ports (VCPs) 	JUNOS 9.5R1	Not applicable
	Virtual Chassis <ul style="list-style-type: none"> ■ Support for SFP uplink module ports 	JUNOS 9.2R1	Not applicable
Virtual Router Redundancy Protocol (VRRP)	JUNOS 9.0R2	JUNOS 9.4R1	

Table 1: Summary of Software Features Available on EX Series Switches (continued)

Feature Category	Feature	First Release EX3200 and EX4200 Switches	First Release EX8200 Switches
	Virtual Router Redundancy Protocol (VRRP) for IPv6 (except authentication-type and authentication key)	JUNOS 10.0R1	Not supported
Interfaces	Digital optical monitoring (DOM)	JUNOS 10.0R1	JUNOS 10.0R1
	Interface range support	JUNOS 10.0R1	JUNOS 10.0R1
	Power over Ethernet (PoE)	JUNOS 9.0R2	Not applicable
	VLAN-tagged Layer 3 subinterfaces	JUNOS 9.2R1	JUNOS 9.4R1
Internet Protocols	IPv4	JUNOS 9.0R2	JUNOS 9.4R1
	IPv6 (except multicast protocols)	JUNOS 9.3R2	Not supported
	A separate software license is required for IPv6. See Understanding Software Licenses for the EX Series Switch.		
IP Address Management	DHCP server and relay with option 82 for Layer 2 VLANs	JUNOS 9.3R2	JUNOS 9.4R1
	DHCPv6 and IPv6 DNS	JUNOS 9.3R2	Not supported
	Dynamic Host Configuration Protocol (DHCP)	JUNOS 9.0R2	JUNOS 9.4R1
	Local DHCP server	JUNOS 9.3R2	JUNOS 9.4R1
	Static addresses	JUNOS 9.0R2	JUNOS 9.4R1

Table 1: Summary of Software Features Available on EX Series Switches (continued)

Feature Category	Feature	First Release EX3200 and EX4200 Switches	First Release EX8200 Switches
Layer 2 Network Protocols	BPDU protection for spanning-tree protocols	JUNOS 9.1R1	JUNOS 9.4R1
	Extended Q-in-Q VLAN support for multiple S-VLANs per access interface, firewall-filter-based VLAN assignment, and routed VLAN interfaces (RVIs)	JUNOS 9.6R1	Not supported
	GARP VLAN Registration Protocol (GVRP)	JUNOS 9.1R1	JUNOS 9.4R1
	Layer 2 protocol tunneling (L2PT)	JUNOS 10.0	Not supported
	Link Layer Discovery Protocol (LLDP)	JUNOS 9.0R2	JUNOS 9.4R1
	Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) with voice over IP (VoIP) integration	JUNOS 9.0R2	Not supported
	Loop protection for spanning-tree protocols	JUNOS 9.1R1	JUNOS 9.4R1
	Multiple VLAN Registration Protocol (MVRP)	JUNOS 10.0R1	JUNOS 10.0R1
	Private VLANs (PVLANS)	JUNOS 9.3R2	Not supported
	Q-in-Q tunneling	JUNOS 9.3R2	Not supported
	Root protection for spanning-tree protocols	JUNOS 9.1R1	JUNOS 9.4R1
	Routed VLAN interfaces (RVIs)	JUNOS 9.0R2	JUNOS 9.4R1
	Spanning tree: <ul style="list-style-type: none"> ■ Spanning Tree Protocol (STP) ■ Rapid Spanning Tree Protocol (RSTP) ■ Multiple Spanning Tree Protocol (MSTP) 	JUNOS 9.0R2	JUNOS 9.4R1
	Spanning tree: <ul style="list-style-type: none"> ■ VLAN Spanning Tree Protocol (VSTP) 	JUNOS 9.4R1	JUNOS 9.6R1
	Storm control	JUNOS 9.1R1	JUNOS 9.4R1
	Unknown Layer 2 unicast forwarding	JUNOS 9.3R2	JUNOS 10.0R1
	Virtual routing and forwarding (VRF)—virtual routing instances	JUNOS 9.2R1	JUNOS 9.6R1
	Virtual routing and forwarding (VRF)—virtual routing instances for multicast traffic	JUNOS 10.0R1	JUNOS 10.0R1
	VLAN ID translation	JUNOS 10.0R1	Not supported
	VLAN range	JUNOS 9.2R1	JUNOS 9.4R1

Table 1: Summary of Software Features Available on EX Series Switches (continued)

Feature Category	Feature	First Release EX3200 and EX4200 Switches	First Release EX8200 Switches
Layer 3 Protocols	Bidirectional Forwarding Detection (BFD)	JUNOS 9.0R2	JUNOS 9.4R1
	Border Gateway Protocol (BGP)	JUNOS 9.0R2	JUNOS 9.4R1
	A separate software license is required for BGP and MBGP. See Understanding Software Licenses for the EX Series Switch.		
	Intermediate System-to-Intermediate System (IS-IS)	JUNOS 9.0R2	JUNOS 9.4R1
	A separate software license is required for IS-IS. See Understanding Software Licenses for the EX Series Switch.		
	IGMPv1 and IGMPv2	JUNOS 9.1R1	JUNOS 9.4R1
	IGMPv3	JUNOS 9.3R2	JUNOS 9.4R1
	Internet Group Management Protocol (IGMP)	JUNOS 9.0R2	JUNOS 9.4R1
	IPv6 protocols: Open Shortest Path First version 3 (OSPFv3), RIPng, IS-IS for IPv6, IPv6 BGP	JUNOS 9.3R2	Not supported
	Jumbo frames on routed VLAN interfaces (RVIs)	JUNOS 9.4R1	JUNOS 9.4R1
	Multicast Source Discovery Protocol (MSDP)	JUNOS 9.4R1	JUNOS 9.4R1
	See the <i>JUNOS Software Routing Protocols Guide</i> at http://www.juniper.net/techpubs/software/junos/junos100/index.html .		
	OSPF Multitopology Routing (MT-OSPF)	JUNOS 9.5R1	JUNOS 9.5R1
	See the <i>JUNOS Software Routing Protocols Guide</i> at http://www.juniper.net/techpubs/software/junos/junos100/index.html .		
OSPFv2	JUNOS 9.0R2	JUNOS 9.4R1	
Protocol Independent Multicast dense mode (PIM DM)	JUNOS 9.2R1	JUNOS 9.4R1	
See the <i>JUNOS Software Multicast Configuration Guide</i> at http://www.juniper.net/techpubs/software/junos/junos100/index.html .			
Protocol Independent Multicast source specific multicast (PIM SSM)	JUNOS 9.2R1	Not supported	
See the <i>JUNOS Software Multicast Configuration Guide</i> at http://www.juniper.net/techpubs/software/junos/junos100/index.html .			

Table 1: Summary of Software Features Available on EX Series Switches (continued)

Feature Category	Feature	First Release EX3200 and EX4200 Switches	First Release EX8200 Switches
	Protocol Independent Multicast sparse mode (PIM SM) See the <i>JUNOS Software Multicast Configuration Guide</i> at http://www.juniper.net/techpubs/software/junos/junos100/index.html .	JUNOS 9.0R2	JUNOS 9.4R1
	Routing Information Protocol version 1 (RIPv1) and RIPv2	JUNOS 9.0R2	JUNOS 9.4R1
	Single-source multicast	JUNOS 9.0R2	JUNOS 9.4R1
	Static routes	JUNOS 9.0R2	JUNOS 9.4R1
Multicast	IGMP snooping with routed VLAN interfaces (RVIs)	JUNOS 9.2R1	JUNOS 9.4R1
	IGMPv3 snooping	JUNOS 9.6R1	JUNOS 9.6R1
	Multicast VLAN registration (MVR)	JUNOS 9.6R1	Not supported
MPLS	MPLS with RSVP-based label switched paths (LSPs) and MPLS-based circuit cross-connects (CCCs) A separate software license is required for MPLS. See Understanding Software Licenses for the EX Series Switch.	JUNOS 9.5R1	Not supported

Table 1: Summary of Software Features Available on EX Series Switches (continued)

Feature Category	Feature	First Release EX3200 and EX4200 Switches	First Release EX8200 Switches
Network Management and Monitoring	Class of service (CoS)—Class-based queuing with prioritization	JUNOS 9.0R2	JUNOS 9.4R1
	Class of service (CoS)—DSCP, IEEE 801 .p, and IP precedence packet rewrites are enabled on routed VLAN interfaces (RVIs).	JUNOS 9.5R1	Not supported
	Class of service (CoS)—Interface-specific classifiers on routed VLAN interfaces (RVIs)	JUNOS 9.4R1	Not supported
	Class of service (CoS) multidestination	Not applicable	JUNOS 9.5R1
	Class-of-service (CoS) support on LAGs	JUNOS 9.2R1	JUNOS 9.4R1
	Class-of-service (CoS) support on routed VLAN interfaces (RVIs)	JUNOS 9.4R1	JUNOS 9.4R1
	Ethernet OAM link fault management (LFM)	JUNOS 9.4R1	JUNOS 10.0R1
	Interface-specific CoS rewrite rules	JUNOS 9.4R1	Not supported
	JUNOS EZQoS for CoS	JUNOS 9.3R2	JUNOS 9.4R1
	Policing	JUNOS 9.0R2	JUNOS 9.4R1
	Port shaping and queue shaping	JUNOS 9.3R2	Not supported
	Port mirroring	JUNOS 9.0R2	JUNOS 9.4R1
	Port mirroring enhancements <ul style="list-style-type: none"> ■ Multiple VLAN support ■ Layer 3 interface support 	JUNOS 9.5R1	JUNOS 9.5R1
	Port mirroring enhancements <ul style="list-style-type: none"> ■ Support for setting ingress-only and egress-only attributes on members of a VLAN to avoid the flooding of mirrored traffic to the member interfaces of a VLAN in the intermediate switch 	JUNOS 10.0R1	Not supported
	RMON	JUNOS 9.0R2	JUNOS 9.4R1
	Real-time performance monitoring (RPM)	JUNOS 9.3R2	Not supported
	sFlow monitoring technology	JUNOS 9.3R2	JUNOS 10.0R1
	Simple Network Management Protocol version 1 (SNMPv1), SNMPv2, and SNMPv3	JUNOS 9.0R2	JUNOS 9.4R1
	System snapshot	JUNOS 10.0R1	JUNOS 10.0R1

Table 1: Summary of Software Features Available on EX Series Switches *(continued)*

Feature Category	Feature	First Release EX3200 and EX4200 Switches	First Release EX8200 Switches
	Transparent bridging	JUNOS 9.0R2	JUNOS 9.4R1

Table 1: Summary of Software Features Available on EX Series Switches (continued)

Feature Category	Feature	First Release EX3200 and EX4200 Switches	First Release EX8200 Switches
Security	802.1X authentication	JUNOS 9.0R2	Not supported
	Denial-of-service (DoS) and distributed DoS (DDoS) protection	JUNOS 9.0R2	JUNOS 9.4R1
	Dynamic allocation of TCAM memory to firewall filters	JUNOS 10.0R1	Not supported
	Dynamic firewall filters for 802.1X authentication	JUNOS 9.0R2	Not supported
	Filter-based forwarding	JUNOS 9.4R1	JUNOS 9.6R1
	Firewall filters and rate limiting	JUNOS 9.0R2	JUNOS 9.4R1
	Firewall filters on LAGs	JUNOS 9.0R2	JUNOS 10.0R1
	Firewall filter on loopback interface	JUNOS 9.2R1	JUNOS 9.6R1
	Firewall filter processing points, additional	JUNOS 9.3R2	Not applicable
	MAC-based VLAN	JUNOS 9.2R1	Not supported
	MAC RADIUS authentication	JUNOS 9.3R2	Not supported
	Port security: ■ DHCP option 82	JUNOS 9.3R2	Not supported
	Port security: ■ DHCP snooping ■ Dynamic ARP inspection (DAI) ■ MAC limiting ■ MAC move limiting	JUNOS 9.0R2	Not supported
	Port security: ■ IP source guard	JUNOS 9.2R1	Not supported
	Port security: ■ Persistent storage for DHCP snooping	JUNOS 9.4R1	Not supported
	Port security: ■ Static ARP support	JUNOS 9.0R2	JUNOS 9.4R1
	Port security and storm control: ■ Automatic recovery for port error disable conditions	JUNOS 9.6R1	JUNOS 10.0R1
	Proxy ARP ■ Restricted proxy ARP	JUNOS 10.0R1	JUNOS 10.0R1

Table 1: Summary of Software Features Available on EX Series Switches (continued)

Feature Category	Feature	First Release EX3200 and EX4200 Switches	First Release EX8200 Switches
	Proxy ARP ■ Unrestricted proxy ARP	JUNOS 9.6R1	Not supported
	Server fail fallback	JUNOS 9.3R2	JUNOS 9.4R1
	TACACS +	JUNOS 9.0R2	JUNOS 9.4R1
	Unicast reverse-path forwarding (RPF)	JUNOS 9.3R2	JUNOS 9.4R1

Table 1: Summary of Software Features Available on EX Series Switches (continued)

Feature Category	Feature	First Release EX3200 and EX4200 Switches	First Release EX8200 Switches
System Management	Autoinstallation	JUNOS 9.4R1	Not supported
	IP directed broadcast	JUNOS 9.4R1	JUNOS 9.4R1
	JUNOS command-line interface (CLI)—For switch configuration and management through the console, Telnet, SSH, or J-Web CLI editor	JUNOS 9.0R2	JUNOS 9.4R1
	J-Web interface, for switch configuration and management	JUNOS 9.0R2	JUNOS 9.4R1
	J-Web interface enhancements: <ul style="list-style-type: none"> ■ The dashboard displays the DC power supply. ■ The Monitoring Chassis Information page displays details about the DC power supply. ■ The Virtual Chassis Monitoring page displays details of Virtual Chassis port (VCP) error and drop counts, VCP maximum bandwidth, and VCP actual bandwidth. 	JUNOS 9.4R1	Not applicable
	J-Web interface enhancements: <ul style="list-style-type: none"> ■ The Interface Configuration page displays details about port role configuration. ■ The Link Aggregation Configuration page supports aggregating interfaces with any speed setting. ■ Configuring spanning-tree protocols, GVRP, IGMP snooping, and redundant trunk groups is supported. ■ Monitoring Ethernet switching, spanning-tree protocols, GVRP, and IGMP snooping is supported. ■ Setting up real-time performance monitoring (RPM) and viewing monitoring results is supported. 	JUNOS 9.5R1	JUNOS 9.5R1
	J-Web license-management tool	JUNOS 9.1R1	JUNOS 9.4R1
	J-Web Port Troubleshooting tool	JUNOS 9.2R1	JUNOS 9.4R1
	Online insertion and removal (OIR) of uplink modules	JUNOS 10.0R1	Not supported
	Platform-specific JUNOS Software installation packages—EX Series switches have specific installation packages for each family of switches. Names of the installation packages include the switch family name.	JUNOS 9.4R1	JUNOS 9.4R1
Power over Ethernet (PoE) power management mode	JUNOS 9.3R2	Not supported	
Related Topics	<ul style="list-style-type: none"> ■ Features in JUNOS Software for EX-series Switches, Release 9.2 ■ New Features in JUNOS Software for EX-series Switches, Release 9.3 ■ New Features in JUNOS Software for EX-series Switches, Release 9.4 		

- New Features in JUNOS Software for EX-series Switches, Release 9.5
- New Features in JUNOS Release 10.0 for EX Series Switches
- EX3200 and EX4200 Switches Hardware Overview
- EX8208 Switch Hardware Overview
- EX8216 Switch Hardware Overview
- High Availability Features for EX Series Switches Overview
- Layer 3 Protocols Supported on EX Series Switches
- Layer 3 Protocols Not Supported on EX Series Switches

Understanding Software Infrastructure and Processes

Each switch runs the Juniper Networks JUNOS Software for Juniper Networks EX Series Ethernet Switches on its general-purpose processors. JUNOS Software includes processes for Internet Protocol (IP) routing and for managing interfaces, networks, and the chassis.

The JUNOS Software runs on the Routing Engine. The Routing Engine kernel coordinates communication among the JUNOS Software processes and provides a link to the Packet Forwarding Engine.

With the J-Web interface and the command-line interface (CLI) to the JUNOS Software, you configure switching features and routing protocols and set the properties of network interfaces on your switch. After activating a software configuration, use either the J-Web or CLI user interface to monitor the switch, manage operations, and diagnose protocol and network connectivity problems.

- Routing Engine and Packet Forwarding Engine on page 15
- JUNOS Software Processes on page 16

Routing Engine and Packet Forwarding Engine

A switch has two primary software processing components:

- Packet Forwarding Engine—Processes packets; applies filters, routing policies, and other features; and forwards packets to the next hop along the route to their final destination.
- Routing Engine—Provides three main functions:
 - Creates the packet forwarding switch fabric for the switch, providing route lookup, filtering, and switching on incoming data packets, then directing outbound packets to the appropriate interface for transmission to the network
 - Maintains the routing tables used by the switch and controls the routing protocols that run on the switch.
 - Provides control and monitoring functions for the switch, including controlling power and monitoring system status.

JUNOS Software Processes

The JUNOS Software running on the Routing Engine and Packet Forwarding Engine consists of multiple processes that are responsible for individual functions.

The separation of functions provides operational stability, because each process accesses its own protected memory space. In addition, because each process is a separate software package, you can selectively upgrade all or part of the JUNOS Software, for added flexibility.

Table 2 on page 16 describes the primary JUNOS Software processes.

Table 2: JUNOS Software Processes

Process	Name	Description
Chassis process	chassisd	<p>Detects hardware on the system that is used to configure network interfaces.</p> <p>Monitors the physical status of hardware components and field-replaceable units (FRUs), detecting when environment sensors such as temperature sensors are triggered.</p> <p>Relays signals and interrupts—for example, when devices are taken offline, so that the system can close sessions and shut down gracefully.</p>
Ethernet switching process	eswd	<p>Handles Layer 2 switching functionality such as MAC address learning, Spanning Tree protocol and access port security. The process is also responsible for managing Ethernet switching interfaces, VLANs, and VLAN interfaces.</p> <p>Manages Ethernet switching interfaces, VLANs, and VLAN interfaces.</p>
Forwarding process	pfem	<p>Defines how routing protocols operate on the switch. The overall performance of the switch is largely determined by the effectiveness of the forwarding process.</p>
Interface process	dcd	<p>Configures and monitors network interfaces by defining physical characteristics such as link encapsulation, hold times, and keepalive timers.</p>
Management process	mgd	<p>Provides communication between the other processes and an interface to the configuration database.</p> <p>Populates the configuration database with configuration information and retrieves the information when queried by other processes to ensure that the system operates as configured.</p> <p>Interacts with the other processes when commands are issued through one of the user interfaces on the switch.</p> <p>If a process terminates or fails to start when called, the management process attempts to restart it a limited number of times to prevent thrashing and logs any failure information for further investigation.</p>
Routing protocol process	rpd	<p>Defines how routing protocols such as RIP, OSPF, and BGP operate on the device, including selecting routes and maintaining forwarding tables.</p>

Related Topics ■ For more information about processes, see the *JUNOS Network Operations Guide* at <http://www.juniper.net/techpubs/software/junos/junos90/index.html>.

- For more information about basic system parameters, supported protocols, and software processes, see *JUNOS System Basics Configuration Guide* at <http://www.juniper.net/techpubs/software/junos/junos94/index.html>.

Configuring User Access

- Configuring Management Access for the EX Series Switch (J-Web Procedure) on page 17
- Generating SSL Certificates to Be Used for Secure Web Access on page 19

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 3 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 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 3: Secure Management Access Configuration Summary

Field	Function	Your Action
Management Access tab		

Table 3: Secure Management Access Configuration Summary (continued)

Field	Function	Your Action
Management Port IP/Management Port IPv6	Specifies the management port IP address. The software supports both IPv4 (displayed as IP) and IPv6 address. NOTE: IPv6 is not supported on EX8200 switches.	To specify an IPv4 address: <ol style="list-style-type: none"> 1. Select the check box IPv4 address. 2. Type an IP address — for example: 10.10.10.10. 3. Enter the subnet mask or address prefix. For example, 24 bits represents 255.255.255.0. 4. Click OK. To specify an IPv6 address: <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.
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 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 .
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 all interfaces or specific interfaces.

Table 3: Secure Management Access Configuration Summary (continued)

Field	Function	Your Action
Enable HTTPS	Enables HTTPS access on interfaces.	<p>To enable HTTPS access, select the Enable HTTPS access check box.</p> <p>Select and deselect interfaces by clicking the direction arrows:</p> <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		
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>
Related Topics	<ul style="list-style-type: none"> ■ Security Features for EX Series Switches Overview ■ Understanding J-Web User Interface Sessions 	

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, *new*.

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 new.pem
```



NOTE: When you are ready to install the SSL certificate, copy the file containing the certificate from the BSD or Linux system to the switch. Open the file and copy its contents so that you can paste it into the Certificate box on the J-Web Secure Access Configuration page.

You can use J-Web Configuration page to install the SSL certificate and enable HTTPS.

- Related Topics**
- Configuring Management Access for the EX Series Switch (J-Web Procedure) on page 17
 - Security Features for EX Series Switches Overview

Monitoring the Switch, Users, and Traffic

- Managing Users (J-Web Procedure) on page 20
- Configuring MS-CHAPv2 to Provide Password-Change Support (CLI Procedure) on page 23
- Monitoring Hosts Using the J-Web Ping Host Tool on page 23
- Monitoring Switch Control Traffic on page 25
- Monitoring Network Traffic Using Traceroute on page 27
- Monitoring System Properties on page 28
- Monitoring System Process Information on page 30

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 4 on page 21.
 - Edit—Select this option to edit an existing user's details. Enter details as described in Table 4 on page 21.
 - 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 5 on page 22.
 - Edit—Select this option to modify the authentication server details. Enter details as described in Table 5 on page 22.
 - 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 5 on page 22.
 - Edit—Select this option to modify the authentication server details. Enter details as described in Table 5 on page 22.
 - Delete—Select this option to delete an authentication server from the list.

Table 4: 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.
User Id	Specifies the user identification.	Type the user's ID.
Full Name	Specifies the user's full name.	Type the user's full name. If the full name contains spaces, enclose it in quotation marks. Do not include colons or commas.

Table 4: User Management > Add a User Configuration Page Summary (continued)

Field	Function	Your Action
Login Class (required)	Defines the user's access privilege.	Select the user's login class from the list: <ul style="list-style-type: none"> ■ operator ■ read-only ■ super-user/superuser ■ unauthorized <p>This list also includes any user-defined login classes.</p>
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 5: 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 Topics** ■ Configuring Management Access for the EX Series Switch (J-Web Procedure) on page 17

Configuring MS-CHAPv2 to Provide Password-Change Support (CLI Procedure)

JUNOS Software for EX Series switches enables you to configure the Microsoft Corporation implementation of the Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) on the switch to provide password-change support. Configuring MS-CHAPv2 on the switch provides users accessing a switch the option of changing the password when the password expires, is reset, or is configured to be changed at next login.

See RFC 2433 at <http://www.faqs.org/rfcs/rfc2433.html>, Microsoft PPP CHAP Extensions, for information about MS-CHAP.

Before you configure MS-CHAPv2 to provide password-change support, ensure that you have:

- Configured RADIUS server authentication. Configure users on the authentication server and set the first-trying option in the authentication order to radius. See Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch.

To configure MS-CHAPv2, specify the following:

```
[edit system radius-options]
user@switch# set password-protocol mschap-v2
```

You must have the required access permission on the switch in order to change your password.

- Related Topics** ■ Managing Users (J-Web Procedure) on page 20
- For more about configuring user access, see the *JUNOS Software Access Privilege Configuration Guide* at <http://www.juniper.net/techpubs/software/junos/junos100/index.html>

Monitoring Hosts Using the J-Web Ping Host Tool

Purpose Use the J-Web ping host tool to verify that the host can be reached over the network. The output is useful for diagnosing host and network connectivity problems. The switch sends a series of ICMP echo (ping) requests to a specified host and receives ICMP echo responses.

Action To use the J-Web ping host tool:

1. Select Troubleshoot>Ping Host.
2. Next to Advanced options, click the expand icon.
3. Enter information into the Ping Host page, as described in Table 6 on page 24.

The Remote Host field is the only required field.

4. Click **Start**.

The results of the ping operation are displayed in the main pane . If no options are specified, each ping response is in the following format:

```
bytes bytes from ip-address: icmp_seq=number ttl=number time=time
```

- To stop the ping operation before it is complete, click **OK**.

Meaning Table 6 on page 24 lists the fields.

Table 6: J-Web Ping Host Field Summary

Field	Function	Your Action
Remote Host	Identifies the host to ping.	Type the hostname or IP address of the host to ping.
Advanced Options		
Don't Resolve Addresses	Determines whether to display hostnames of the hops along the path.	<ul style="list-style-type: none"> ■ To suppress the display of the hop hostnames, select the check box. ■ To display the hop hostnames, clear the check box.
Interface	Specifies the interface on which the ping requests are sent.	Select the interface on which ping requests are sent from the list. If you select any , the ping requests are sent on all interfaces.
Count	Specifies the number of ping requests to send.	Select the number of ping requests to send from the list.
Don't Fragment	Specifies the Don't Fragment (DF) bit in the IP header of the ping request packet.	<ul style="list-style-type: none"> ■ To set the DF bit, select the check box. ■ To clear the DF bit, clear the check box.
Record Route	Sets the record route option in the IP header of the ping request packet. The path of the ping request packet is recorded within the packet and displayed in the main pane.	<ul style="list-style-type: none"> ■ To record and display the path of the packet, select the check box. ■ To suppress the recording and display of the path of the packet, clear the check box.
Type-of-Service	Specifies the type-of-service (TOS) value in the IP header of the ping request packet.	Select the decimal value of the TOS field from the list.
Routing Instance	Name of the routing instance for the ping attempt.	Select the routing instance name from the list.
Interval	Specifies the interval, in seconds, between transmissions of individual ping requests.	Select the interval from the list.
Packet Size	Specifies the size of the ping request packet.	Type the size, in bytes, of the packet. The size can be from 0 through 65468. The switch adds 8 bytes of ICMP header to the size.
Source Address	Specifies the source address of the ping request packet.	Type the source IP address.
Time-to-Live	Specifies the time-to-live (TTL) hop count for the ping request packet.	Select the TTL value from the list.

Table 6: J-Web Ping Host Field Summary (continued)

Field	Function	Your Action
Bypass Routing	<p>Determines whether ping requests are routed by means of the routing table.</p> <p>If the routing table is not used, ping requests are sent only to hosts on the interface specified in the Interface box. If the host is not on that interface, ping responses are not sent.</p>	<ul style="list-style-type: none"> ■ To bypass the routing table and send the ping requests to hosts on the specified interface only, select the check box. ■ To route the ping requests using the routing table, clear the check box.

Related Topics ■ Monitoring Interface Status and Traffic

Monitoring Switch Control Traffic

Purpose Use the packet capture feature when you need to quickly capture and analyze switch control traffic on a switch. The packet capture feature allows you to capture traffic destined for or originating from the Routing Engine.

Action To use the packet capture feature in the J-Web interface, select **Troubleshoot>Packet Capture**.

To use the packet capture feature in the CLI, enter the following CLI command:

```
monitor traffic
```

Meaning You can use the packet capture feature to compose expressions with various matching criteria to specify the packets that you want to capture. You can decode and view the captured packets in the J-Web interface as they are captured. The packet capture feature does not capture transient traffic.

Table 7: Packet Capture Field Summary

Field	Function	Your Action
Interface	Specifies the interface on which the packets are captured. If you select default, packets on the Ethernet management port 0, are captured.	From the list, select an interface—for example, <code>ge-0/0/0</code> .
Detail level	<p>Specifies the extent of details to be displayed for the packet headers.</p> <ul style="list-style-type: none"> ■ Brief—Displays the minimum packet header information. This is the default. ■ Detail—Displays packet header information in moderate detail. ■ Extensive—Displays the maximum packet header information. 	From the list, select Detail .
Packets	Specifies the number of packets to be captured. Values range from 1 to 1000. Default is 10. Packet capture stops capturing packets after this number is reached.	From the list, select the number of packets to be captured—for example, 10.

Table 7: Packet Capture Field Summary (continued)

Field	Function	Your Action
Addresses	<p>Specifies the addresses to be matched for capturing the packets using a combination of the following parameters:</p> <ul style="list-style-type: none"> ■ Direction—Matches the packet headers for IP address, hostname, or network address of the source, destination or both. ■ Type—Specifies if packet headers are matched for host address or network address. <p>You can add multiple entries to refine the match criteria for addresses.</p>	<p>Select address-matching criteria. For example:</p> <ol style="list-style-type: none"> 1. From the Direction list, select source. 2. From the Type list, select host. 3. In the Address box, type 10.1.40.48. 4. Click Add.
Protocols	Matches the protocol for which packets are captured. You can choose to capture TCP, UDP, or ICMP packets or a combination of TCP, UDP, and ICMP packets.	From the list, select a protocol—for example, tcp .
Ports	Matches packet headers containing the specified source or destination TCP or UDP port number or port name.	<p>Select a direction and a port. For example:</p> <ul style="list-style-type: none"> ■ From the Type list, select src. ■ In the Port box, type 23.
Advanced Options		
Absolute TCP Sequence	Specifies that absolute TCP sequence numbers are to be displayed for the packet headers.	To display absolute TCP sequence numbers in the packet headers, select this check box.
Layer 2 Headers	Specifies that link-layer packet headers are to be displayed.	To include link-layer packet headers while capturing packets, select this check box.
Non-Promiscuous	Specifies not to place the interface in promiscuous mode, so that the interface reads only packets addressed to it. In promiscuous mode, the interface reads every packet that reaches it.	To read all packets that reach the interface, select this check box.
Display Hex	Specifies that packet headers, except link-layer headers, are to be displayed in hexadecimal format.	To display the packet headers in hexadecimal format, select this check box.
Display ASCII and Hex	Specifies that packet headers are to be displayed in hexadecimal and ASCII format.	To display the packet headers in ASCII and hexadecimal formats, select this check box.
Header Expression	Specifies the match condition for the packets to be captured. The match conditions you specify for Addresses, Protocols, and Ports are displayed in expression format in this field.	You can enter match conditions directly in this field in expression format or modify the expression composed from the match conditions you specified for Addresses, Protocols, and Ports. If you change the match conditions specified for Addresses, Protocols, and Ports again, packet capture overwrites your changes with the new match conditions.
Packet Size	Specifies the number of bytes to be displayed for each packet. If a packet header exceeds this size, the display is truncated for the packet header. The default value is 96 bytes.	Type the number of bytes you want to capture for each packet header—for example, 256 .

Table 7: Packet Capture Field Summary (continued)

Field	Function	Your Action
Don't Resolve Addresses	Specifies that IP addresses are not to be resolved into hostnames in the packet headers displayed.	To prevent packet capture from resolving IP addresses to hostnames, select this check box.
No Timestamp	Suppresses the display of packet header timestamps.	To stop displaying timestamps in the captured packet headers, select this check box.
Write Packet Capture File	Writes the captured packets to a file in PCAP format in /var/tmp. The files are named with the prefix jweb-pcap and the extension .pcap. If you select this option, the decoded packet headers are not displayed on the packet capture page.	To decode and display the packet headers on the J-Web page, clear this check box.

Related Topics ■ Using the CLI Terminal

Monitoring Network Traffic Using Traceroute

Purpose Use the Traceroute page in the J-Web interface to trace a route between the switch and a remote host. You can use a traceroute task to display a list of waypoints between the switch and a specified destination host. The output is useful for diagnosing a point of failure in the path from the switch platform to the destination host and addressing network traffic latency and throughput problems.

Action To use the traceroute tool:

1. Select **Troubleshoot>Traceroute**.
2. Next to **Advanced options**, click the expand icon.
3. Enter information into the Traceroute page.

The **Remote Host** field is the only required field.

4. Click **Start**.
5. To stop the traceroute operation before it is complete, click **OK** while the results of the traceroute operation are being displayed.

Meaning The switch generates the list of waypoints by sending a series of ICMP traceroute packets in which the time-to-live (TTL) value in the messages sent to each successive waypoint is incremented by 1. (The TTL value of the first traceroute packet is set to 1.) In this manner, each waypoint along the path to the destination host replies with a Time Exceeded packet from which the source IP address can be obtained.

The results of the traceroute operation are displayed in the main pane. If no options are specified, each line of the traceroute display is in the following format:

```
hop-number host (ip-address) [as-number] time1 time2 time3
```

The switch sends a total of three traceroute packets to each waypoint along the path and displays the round-trip time for each traceroute operation. If the switch times out before receiving a **Time Exceeded** message, an asterisk (*) is displayed for that round-trip time.

Table 8: Traceroute field summary

Field	Function	Your Action
Remote Host	Identifies the destination host of the traceroute.	Type the hostname or IP address of the destination host.
Advanced Options		
Don't Resolve Addresses	Determines whether hostnames of the hops along the path are displayed, in addition to IP addresses.	To suppress the display of the hop hostnames, select the check box.
Gateway	Specifies the IP address of the gateway to route through.	Type the gateway IP address.
Source Address	Specifies the source address of the outgoing traceroute packets.	Type the source IP address.
Bypass Routing	Determines whether traceroute packets are routed by means of the routing table. If the routing table is not used, traceroute packets are sent only to hosts on the interface specified in the Interface box. If the host is not on that interface, traceroute responses are not sent.	To bypass the routing table and send the traceroute packets to hosts on the specified interface only, select the check box.
Interface	Specifies the interface on which the traceroute packets are sent.	From the list, select the interface on which traceroute packets are sent. If you select any, the traceroute requests are sent on all interfaces.
Time-to-live	Specifies the maximum time-to-live (TTL) hop count for the traceroute request packet.	From the list, select the TTL.
Type-of-Service	Specifies the type-of-service (TOS) value to include in the IP header of the traceroute request packet.	From the list, select the decimal value of the TOS field.
Resolve AS Numbers	Determines whether the autonomous system (AS) number of each intermediate hop between the router and the destination host is displayed.	To display the AS numbers, select the check box.

- Related Topics**
- Connecting and Configuring an EX Series Switch (CLI Procedure)
 - Connecting and Configuring an EX Series Switch (J-Web Procedure)
 - Configuring Gigabit Ethernet Interfaces (J-Web Procedure)
 - Monitoring Interface Status and Traffic

Monitoring System Properties

Purpose Use the monitoring functionality to view system properties such as the name and IP address of the switch and resource usage.

Action To monitor system properties in the J-Web interface, select **Monitor > System View > System Information**.

To monitor system properties in the CLI, enter the following commands:

- show system uptime
- show system users
- show system storage

Meaning Table 9 on page 29 summarizes key output fields in the system properties display.

Table 9: Summary of Key System Properties Output Fields

Field	Values	Additional Information
General Information		
Serial Number	Serial number for the switch.	
JUNOS Software Version	Version of JUNOS Software active on the switch, including whether the software is for domestic or export use.	Export software is for use outside of the U.S. and Canada.
Hostname	The name of switch.	
IP Address	The IP address of the switch.	
Loopback Address	The loopback address.	
Domain Name Server	The address of the domain name server.	
Time Zone	The time zone on the switch.	
Time		
Current Time	Current system time, in Coordinated Universal Time (UTC).	
System Booted Time	Date and time when the switch was last booted and how long it has been running.	
Protocol Started Time	Date and time when the switching protocols were last started and how long they have been running.	
Last Configured Time	Date and time when a configuration was last committed. This field also shows the name of the user who issued the last commit command, through either the J-Web interface or the CLI.	
Load Average	The CPU load average for 1, 5, and 15 minutes.	

Table 9: Summary of Key System Properties Output Fields (continued)

Field	Values	Additional Information
Storage Media		
Internal Flash Memory	Memory usage details of internal flash.	
External Flash Memory	Usage details of external flash memory.	
Logged in Users Details		
User	Username of any user logged in to the switching platform.	
Terminal	Terminal through which the user is logged in.	
From	System from which the user has logged in. A hyphen indicates that the user is logged in through the console.	
Login Time	Time when the user logged in.	This is the LOGIN@ field in show system users command output.
Idle Time	How long the user has been idle.	

- Related Topics**
- Monitoring System Process Information on page 30
 - Understanding J-Web User Interface Sessions

Monitoring System Process Information

Purpose Use the monitoring functionality to view the processes running on the switch.

Action To view the software processes running on the switch in the J-Web interface, select **Monitor > System View > Process Details**.

To view the software processes running on the switch in the CLI, enter the following command.

```
show system processes
```

Meaning Table 10 on page 31 summarizes the output fields in the system process information display.

The display includes the total CPU load and total memory utilization.

Table 10: Summary of System Process Information Output Fields

Field	Values	Additional Information
PID	Identifier of the process.	
Name	Owner of the process.	
State	Current state of the process.	
CPU Load	Percentage of the CPU that is being used by the process.	
Memory Utilization	Amount of memory that is being used by the process.	
Start Time	Time of day when the process started.	

- Related Topics**
- Monitoring System Properties on page 28
 - For more information about show system properties command, see show system uptime

