JUNOS Enhanced Services

Migration Guide

Release 8.5

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

Part Number: 530-021757-01, Revision 1

JUNOS Enhanced Services Migration Guide, Release 8.5
Writing: Genie Mak
Editing: Taffy Everts
Illustration: Nathaniel Woodward
Cover design: Edmonds Design

Revision History
15 November 2007—Revision 1

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 NONINFRINGEMENT. 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 présentés confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattaché, soient redigés 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 Guide

This preface provides the following guidelines for using the *JUNOS Enhanced Services Migration Guide* and related Juniper Networks, Inc., technical documents:

Objectives

This guide shows you how to perform the following software tasks:

- Migrate ScreenOS software on an SSG 300M-series or SSG 500M-series security device to JUNOS Enhanced Services software on a J-series Services Router (hardware conversion kit also required).
- Migrate the JUNOS software on a J-series router to JUNOS Enhanced Services.
- Convert the JUNOS software on a J-series router to ScreenOS software on an SSG 300M-series or SSG 500M-series security device (hardware conversion kit also required).
- Downgrade the JUNOS Enhanced Services software on a J-series router to the JUNOS software.

For a list of the SSG security devices and J-series routers on which you can perform these tasks, see “Supported Routing Platforms” on page viii.

NOTE: This manual documents Release 8.5 of the JUNOS Enhanced Services software. For additional information—either corrections to or information that might have been omitted from this manual—see the *JUNOS Enhanced Services Release Notes* at http://www.juniper.net/.

Audience

This manual is designed for anyone needing to migrate from ScreenOS or JUNOS software to JUNOS Enhanced Services software, or downgrade from JUNOS Enhanced Services to the JUNOS software. This manual is intended for the following audiences:

- Customers with technical knowledge of and experience with networks and network security, the Internet, and Internet routing protocols
- Network administrators who install, configure, and manage Internet routers

Personnel operating the equipment must be trained and competent; must not conduct themselves in a careless, wilfully negligent, or hostile manner; and must abide by the instructions provided in the documentation.

Supported Routing Platforms

For the features described in this manual, the JUNOS Enhanced Services software currently supports only the J-series Services Routers listed in Table 1.

Table 1: SSG Security Devices and J-series Services Routers Supported for Migration

SSG Security Device	J-series Services Router
SSG 320M	J2320
SSG 350M	J2350
SSG 520M	J4350
SSG 550M	J6350

How to Use This Manual

This manual and the other JUNOS Enhanced Services manuals explain how to install, configure, and manage J-series Services Routers that are running the JUNOS Enhanced Services software. To configure and operate these routers, you must also use the configuration statements and operational mode commands documented in the JUNOS configuration guides and command references.

Table 2 identifies the tasks required to configure and manage the routers and shows where to find task information and instructions.

For an annotated list of the documentation referred to in Table 2, see "JUNOS Enhanced Services and Related Documentation" on page xii. All documents are available at http://www.juniper.net/techpubs/.

Table 2: JUNOS Enhanced Services Tasks and Documentation for J-series Routers

JUNOS Enhanced Services Tasks	JUNOS Enhanced Services Documentation	Related JUNOS Documentation
Basic Router Installation and Setup		
■ Reviewing safety warnings and compliance statements ■ Installing hardware and establishing basic connectivity ■ Initially setting up the router	■ *JUNOS Enhanced Services J-series Services Router Quick Start* ■ *JUNOS Enhanced Services J-series Services Router Getting Started Guide* ■ *JUNOS Enhanced Services CLI Reference* ■ *JUNOS Enhanced Services Release Notes*	■ *JUNOS System Basics Configuration Guide* ■ *JUNOS System Basics and Services Command Reference*
Migration from ScreenOS or JUNOS to JUNOS Enhanced Services		
■ Migrating from JUNOS Release 8.3 or later to JUNOS Enhanced Services software ■ Migrating from ScreenOS Release 5.4 or later to JUNOS Enhanced Services software	*JUNOS Enhanced Services Migration Guide*	—
Context—Changing to Secure Context or Router Context		
Changing the router from one context to another and understanding the factory default settings	*JUNOS Enhanced Services Administration Guide*	—
Router Interface Configuration		
Configuring router interfaces	■ *JUNOS Enhanced Services Interfaces and Routing Configuration Guide* ■ *JUNOS Enhanced Services CLI Reference*	■ *JUNOS System Basics Configuration Guide* ■ *JUNOS System Basics and Services Command Reference*
Secure Router Deployment Planning and Configuration		
■ Understanding and gathering information required to design network firewalls and IPSec VPNs ■ Implementing a JUNOS Enhanced Services firewall from a sample scenario ■ Implementing a policy-based IPSec VPN from a sample scenario	*JUNOS Enhanced Services Design and Implementation Guide*	—

Table 2: JUNOS Enhanced Services Tasks and Documentation for J-series Routers (continued)

JUNOS Enhanced Services Tasks	JUNOS Enhanced Services Documentation	Related JUNOS Documentation
Configuring and managing the following security services: ■ Stateful firewall policies ■ Zones and their interfaces and address books ■ IPSec VPNs ■ Firewall screens ■ Interfaces modes: Network Address Translation (NAT) mode and Route mode ■ Public Key Cryptography ■ Application Layer Gateways (ALGs)	■ *JUNOS Enhanced Services Security Configuration Guide* ■ *JUNOS Enhanced Services CLI Reference*	—
Routing Protocols and Services Configuration		
Configuring routing protocols, including static routes and the dynamic routing protocols RIP, OSPF, BGP, and IS-IS	■ *JUNOS Enhanced Services Interfaces and Routing Configuration Guide* ■ *JUNOS Enhanced Services CLI Reference*	■ *JUNOS Routing Protocols Configuration Guide* ■ *JUNOS Routing Protocols and Policies Command Reference*
Configuring class-of-service (CoS) features, including traffic shaping and policing		■ *JUNOS Class of Service Configuration Guide* ■ *JUNOS System Basics and Services Command Reference*
Configuring packet-based stateless firewall filters (access control lists) to control access and limit traffic rates		■ *JUNOS Policy Framework Configuration Guide* ■ *JUNOS Routing Protocols and Policies Command Reference*
WAN Acceleration Module Installation (Optional)		
Installing and initially configuring a WXC Integrated Services Module (ISM 200)	*WXC Integrated Services Module Installation and Configuration Guide*	—
User and System Administration		
Administering user authentication and access	*JUNOS Enhanced Services Administration Guide*	■ *JUNOS System Basics Configuration Guide* ■ *JUNOS System Basics and Services Command Reference*
Monitoring the router, routing protocols, and related operations		
Configuring and monitoring system alarms and events, real-time performance (RPM) probes, and performance		
Monitoring the firewall and other security-related services		—
Managing system log files		*JUNOS System Log Messages Reference*
Upgrading software		—
Diagnosing common problems		

Table 2: JUNOS Enhanced Services Tasks and Documentation for J-series Routers (continued)

JUNOS Enhanced Services Tasks	JUNOS Enhanced Services Documentation	Related JUNOS Documentation
User Interfaces		
Understanding and using the J-Web interface	■ *JUNOS Enhanced Services J-series Services Router Quick Start*	*J-Web Interface User Guide*
Understanding and using the JUNOS CLI	■ *JUNOS Enhanced Services J-series Services Router Getting Started Guide*	*JUNOS CLI User Guide*

Documentation Conventions

Table 3 defines notice icons used in this manual.

Table 3: 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.

Table 4 defines the text and syntax conventions used in this manual.

Table 4: Text and Syntax Conventions (Sheet 1 of 2)

Convention	Element	Example
Bold sans serif typeface	Represents text that you type.	To enter configuration mode, type the configure command: user@host> **configure**
`Fixed-width typeface`	Represents output on the terminal screen.	`user@host> show chassis alarms` `No alarms currently active`
Italic typeface	■ Introduces important new terms. ■ Identifies book names. ■ Identifies RFC and Internet draft titles.	■ A policy *term* is a named structure that defines match conditions and actions. ■ *JUNOS System Basics Configuration Guide* ■ RFC 1997, *BGP Communities Attribute*
Italic sans serif typeface	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** *domain-name*
Sans serif typeface	Represents names of configuration statements, commands, files, and directories; IP addresses; configuration hierarchy levels; or labels on routing platform components.	■ 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 *metric*>;
| (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 (*string1* | *string2* | *string3*)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only

Table 4: Text and Syntax Conventions (Sheet 2 of 2)

Convention	Element	Example
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	community name members [*community-ids*]

Indention and braces ({ })	Identify a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

JUNOS Enhanced Services and Related Documentation

Table 5 lists the JUNOS Enhanced Services manuals and release notes.

To configure and operate a J-series Services Router running JUNOS Enhanced Services software, you must also use the configuration statements and operational mode commands documented in JUNOS configuration guides and command references. To configure and operate a WXC integrated Services Module, you must also use WX documentation. Table 6 lists the JUNOS software manuals and release notes and WX manuals.

All documents are available at http://www.juniper.net/techpubs/.

Table 5: JUNOS Enhanced Services Documentation

Document	Description
JUNOS Enhanced Services Design and Implementation Guide	Provides guidelines and examples for designing and implementing IP Security (IPSec) virtual private networks (VPNs), firewalls, and routing on J-series routers running the JUNOS Enhanced Services software.
JUNOS Enhanced Services J-series Services Router Quick Start	Explains how to quickly set up a J-series router. This document contains router declarations of conformity.
JUNOS Enhanced Services J-series Services Router Getting Started Guide	Provides an overview, basic instructions, and specifications for J-series Services Routers. This guide explains how to prepare a site, unpack and install the router, replace router hardware, and establish basic router connectivity. This guide contains hardware descriptions and specifications.
Read This First (SSG 300M-series)	Provides instructions for registering your new hardware configuration after converting hardware with Juniper Networks Customer Service.
Conversion Instructions for SSG 300M-series Security Devices and J-series Services Routers	Provides instructions for converting an SSG 300M-series security device to a J-series Services Router and converting a J-series Services Router to an SSG 300M-series security device.
Read This First (SSG 500M-series)	Provides instructions for registering your new hardware configuration after converting hardware with Juniper Networks Customer Service.
Conversion Instructions for SSG 500M-series Security Devices and J-series Services Routers	Provides instructions for converting an SSG 500M-series security device to a J-series Services Router and converting a J-series Services Router to an SSG 500M-series security device.
JUNOS Enhanced Services Migration Guide	Provides instructions for migrating a J-series router from ScreenOS software or the JUNOS software to the JUNOS Enhanced Services software.

Table 5: JUNOS Enhanced Services Documentation (continued)

Document	Description
JUNOS Enhanced Services Interfaces and Routing Configuration Guide	Explains how to configure J-series router interfaces for basic IP routing with standard routing protocols, ISDN service, firewall filters (access control lists), and class-of-service (CoS) traffic classification.
JUNOS Enhanced Services Security Configuration Guide	Explains how to configure and manage security services such as stateful firewall policies, IPSec VPNs, firewall screens, Network Address Translation (NAT) and Route interface modes, Public Key Cryptography, and Application Layer Gateways (ALGs).
JUNOS Enhanced Services Administration Guide	Shows how to monitor the router and routing operations, firewall and security services, system alarms and events, and network performance. This guide also shows how to administer user authentication and access, upgrade software, and diagnose common problems.
JUNOS Enhanced Services CLI Reference	Provides the complete JUNOS Enhanced Services configuration hierarchy and describes the configuration statements and operational mode commands not documented in the standard JUNOS manuals listed in Table 6.
WXC Integrated Services Module Installation and Configuration Guide	Explains how to install and initially configure a WXC Services Module in a J-series router, for application acceleration.
JUNOS Enhanced Services Release Notes	Summarize new features and known problems for a particular JUNOS Enhanced Services software release on J-series routers, including J-Web interface features and problems. The release notes also contain corrections and updates to JUNOS Enhanced Services manuals and software upgrade and downgrade instructions.

Table 6: Related JUNOS and WX Documentation

Document	Description
JUNOS Software Configuration Guides	
JUNOS Class of Service Configuration Guide	Provides an overview of the class-of-service (CoS) functions of the JUNOS software and describes how to configure CoS features, including configuring multiple forwarding classes for transmitting packets, defining which packets are placed into each output queue, scheduling the transmission service level for each queue, and managing congestion through the random early detection (RED) algorithm.
JUNOS Feature Guide	Provides a detailed explanation and configuration examples for several of the most complex features in the JUNOS software.
JUNOS Multicast Protocols Configuration Guide	Provides an overview of multicast concepts and describes how to configure multicast routing protocols.
JUNOS Network Interfaces Configuration Guide	Provides an overview of the network interface functions of the JUNOS software and describes how to configure the network interfaces on the routing platform.
JUNOS Network Management Configuration Guide	Provides an overview of network management concepts and describes how to configure various network management features, such as SNMP and accounting options.
JUNOS Policy Framework Configuration Guide	Provides an overview of policy concepts and describes how to configure routing policy, firewall filters, forwarding options, and cflowd.
JUNOS Routing Protocols Configuration Guide	Provides an overview of routing concepts and describes how to configure routing, routing instances, and unicast routing protocols.
JUNOS Services Interfaces Configuration Guide	Provides an overview of the services interfaces functions of the JUNOS software and describes how to configure the services interfaces on the routing platform.
JUNOS Software Installation and Upgrade Guide	Provides a description of JUNOS software components and packaging, and includes detailed information about how to initially configure, reinstall, and upgrade the JUNOS system software. This material was formerly covered in the *JUNOS System Basics Configuration Guide*.

Table 6: Related JUNOS and WX Documentation (continued)

Document	Description
JUNOS System Basics Configuration Guide	Describes Juniper Networks routing platforms, and provides information about how to configure basic system parameters, supported protocols and software processes, authentication, and a variety of utilities for managing your router on the network.
JUNOS References	
JUNOS Hierarchy and RFC Reference	Describes the JUNOS configuration mode commands. Provides a hierarchy reference that displays each level of a configuration hierarchy, and includes all possible configuration statements that can be used at that level. This material was formerly covered in the *JUNOS System Basics Configuration Guide*.
JUNOS Interfaces Command Reference	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot interfaces.
JUNOS Routing Protocols and Policies Command Reference	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot routing protocols and policies, including firewall filters.
JUNOS System Basics and Services Command Reference	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot system basics, including commands for real-time monitoring and route (or path) tracing, system software management, and chassis management. Also describes commands for monitoring and troubleshooting services such as CoS, IP Security (IPSec), stateful firewalls, flow collection, and flow monitoring.
JUNOS System Log Messages Reference	Describes how to access and interpret system log messages generated by JUNOS software modules and provides a reference page for each message.
User Interface Guides	
J-Web Interface User Guide	Describes how to use the J-Web GUI to configure, monitor, and manage Juniper Networks routing platforms.
JUNOS CLI User Guide	Describes how to use the JUNOS command-line interface (CLI) to configure, monitor, and manage Juniper Networks routing platforms. This material was formerly covered in the *JUNOS System Basics Configuration Guide*.
JUNOS API and Scripting Documentation	
JUNOScript API Guide	Describes how to use the JUNOScript application programming interface (API) to monitor and configure Juniper Networks routing platforms.
JUNOS XML API Configuration Reference	Provides reference pages for the configuration tag elements in the JUNOS XML API.
JUNOS XML API Operational Reference	Provides reference pages for the operational tag elements in the JUNOS XML API.
JUNOS Configuration and Diagnostic Automation Guide	Describes how to use the commit script and self-diagnosis features of the JUNOS software. This guide explains how to enforce custom configuration rules defined in scripts, how to use commit script macros to provide simplified aliases for frequently used configuration statements, and how to configure diagnostic event policies.
NETCONF API Guide	Describes how to use the NETCONF API to monitor and configure Juniper Networks routing platforms.
JUNOScope Documentation	
JUNOScope Software User Guide	Describes the JUNOScope software GUI, how to install and administer the software, and how to use the software to manage routing platform configuration files and monitor routing platform operations.
Release Notes	
JUNOS Release Notes	Summarize new features and known problems for a particular software release, provide corrections and updates to published JUNOS, JUNOScript, and NETCONF manuals, provide information that might have been omitted from the manuals, and describe upgrade and downgrade procedures.
JUNOScope Software Release Notes	Contain corrections and updates to the published JUNOScope manual, provide information that might have been omitted from the manual, and describe upgrade and downgrade procedures.

Table 6: Related JUNOS and WX Documentation (continued)

Document	Description
WX Manuals	
WX Central Management System (CMS) Administrator's Guide	Describes how to manage, monitor, and configure up to 2000 WAN acceleration platforms and WXC Integrated Services Modules.
WX/WXC Operator's Guide	Describes how to use the WXOS Web and CLI interfaces to configure, monitor, and manage individual WAN acceleration platforms and WXC Integrated Services Modules.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. Send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at http://www.juniper.net/techpubs/docbug/docbugreport.html. If you are using e-mail, be sure to include the following information with your comments:

- Document name
- Document part number
- Page number
- Software release version

Requesting Support

For technical support, open a support case using 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).

Chapter 1

Preparing for Migration

Before migrating ScreenOS or JUNOS software to JUNOS Enhanced Services software, become familiar with the effects of migration on your existing software. Before performing any migration, be sure you meet the hardware and software requirements and understand the migration process and tools.

This chapter contains the following sections:

Secure and Router Contexts and Effects on Migration

A J-series Services Router running JUNOS Enhanced Services software can operate as either a stateful firewall or a router. When a Services Router is initially configured as a firewall, it operates in *secure context*. When a Services Router is initially configured as a router, it operates in *router context*.

- Secure context—Allows a Services Router to act as a stateful firewall with only management access. To allow traffic to pass through a Services Router, you must explicitly configure a security policy for that purpose. In secure context, a Services Router forwards packets only if a security policy permits it.
- Router context—Allows a Services Router to act as a router in which all management and transit traffic is allowed. In router context, a security policy is created that specifies that the Services Router forwards all packets. To deny specific traffic, you must configure a security policy to do so.

On ScreenOS Migration

An SSG security device running ScreenOS requires that security policies be defined to ensure that traffic is forwarded appropriately. During the migration process to JUNOS Enhanced Services software, ScreenOS security policy commands are converted to JUNOS Enhanced Services security policy configuration statements.

A J-series Services Router using a configuration file that was migrated from a ScreenOS configuration file operates in secure context.

On JUNOS Migration

During the migration process from the JUNOS software to JUNOS Enhanced Services, JUNOS configurations without stateful-firewall, services nat, or services ipsec-vpn configuration statements defined are converted so that no security policy is required to forward packets. In this case, the Services Router operates in router context.

JUNOS configurations with stateful-firewall, services nat, or services ipsec-vpn configuration statements defined are converted so that JUNOS Enhanced Services security policies are created, based on the original configuration statements.

Hardware and System Software Requirements

To migrate between ScreenOS, JUNOS software, and JUNOS Enhanced Services, your system must meet certain requirements:

SSG Required Hardware and Operating System Software

For ScreenOS users, Table 7 lists the SSG security devices running ScreenOS Release 5.4 or later that you can convert to J-series Services Routers to run JUNOS Enhanced Services. If you have not already done so, you must obtain the appropriate conversion kit from Juniper Networks to convert the hardware.

All SSG security devices must have a compact flash card with at least 256 MB of storage capacity.

Table 7: Convertible SSG Hardware and Software

SSG Security Device with ScreenOS 5.4 or Later	Conversion Kit	Resulting Services Router
SSG 320M	SSG-320M-J-CONV-S	J2320
SSG 350M	SSG-350M-J-CONV-S	J2350
SSG 520M	SSG-520M-J-CONV-S	J4350
SSG 550M	SSG-550M-J-CONV-S	J6350

J-series Required Hardware and Operating System Software

For JUNOS users, Table 8 lists the J-series Services Routers running JUNOS Release 8.3 or later that you can migrate to JUNOS Enhanced Services.

You can also convert the routers listed in Table 8 to SSG security devices. If you have not already done so, you must obtain the appropriate conversion kit from Juniper Networks to convert the hardware.

All Services Routers must have a compact flash card with at least 256 MB of storage capacity.

Table 8: Migratable and Convertible J-series Hardware and Software

Services Router with JUNOS 8.3 or Later	Conversion Kit (if applicable)	Resulting SSG Security Device (if applicable)
J2320	J2320-SSG-CONV-S	SSG 320M
J2350	J2350-SSG-CONV-S	SSG 350M
J4350	J4350-SSG-CONV-S	SSG 520M
J6350	J6350-SSG-CONV-S	SSG 550M

Web Browser Requirements

To use the Juniper Networks migration tools, you need one of the following Web browsers:

- Microsoft Internet Explorer 5.5 or later
- Netscape Navigator 6.1 or later
- Mozilla Firefox 2.0 or later

Any Web browser you use must support 128-bit encryption.

Juniper Network Web Account Requirement

To access the migration tools, you need a Web account with Juniper Networks. To obtain an account, complete the registration form at the Juniper Networks Web site https//www.juniper.net/registration/Register.jsp.

Introducing the JUNOS Enhanced Services Migration Tools

As part of the migration process, you migrate a ScreenOS or JUNOS configuration file to a JUNOS Enhanced Services configuration file. You must migrate the original configuration file before you can use JUNOS Enhanced Services software.

To assist you with the migration of the configuration file, use one of the following Juniper Networks Migration Tools:

- ScreenOS-to-JUNOS Enhanced Services Migration Tool
- JUNOS-to-JUNOS Enhanced Services Migration Tool

The Migration Tools are Web-based tools available on the Juniper Networks Web site that allow you to input your original configuration and convert that configuration to a configuration file in JUNOS Enhanced Services format.

For a task overview of the migration from ScreenOS or JUNOS to JUNOS Enhanced Services, see “ScreenOS-to-JUNOS Enhanced Services Software Migration Overview” on page 6 and “JUNOS-to-JUNOS Enhanced Services Migration Overview” on page 20.

If you are migrating to JUNOS Enhanced Services software on multiple devices, there are likely common elements in the configuration files across devices. Use the migration tool as part of your overall migration process and not as the only tool for migration.

Chapter 2

Migrating ScreenOS to JUNOS Enhanced Services by Compact-Flash Method

You can convert certain SSG security devices running ScreenOS software to J-series Services Routers running JUNOS Enhanced Services software with the appropriate conversion kit. (See Table 9.)

Table 9: Convertible SSG Hardware and Software

SSG Security Device with ScreenOS 5.4 or Later	Conversion Kit	Resulting Services Router
SSG 320M	SSG-320M-J-CONV-S	J2320
SSG 350M	SSG-350M-J-CONV-S	J2350
SSG 520M	SSG-520M-J-CONV-S	J4350
SSG 550M	SSG-550M-J-CONV-S	J6350

After converting your hardware, you migrate your ScreenOS configuration to a JUNOS Enhanced Services configuration, upload the file to the router, thoroughly test the configuration, and register the new hardware configuration.

This chapter contains the following sections:

ScreenOS-to-JUNOS Enhanced Services Software Migration Overview

To migrate ScreenOS software to JUNOS Enhanced Services software, you perform the following tasks:

1. Convert your SSG security device to a J-series Services Router by following the instructions in your conversion kit documentation.

2. Migrate the ScreenOS configuration to JUNOS Enhanced Services format. (See "Migrating the ScreenOS Configuration to JUNOS Enhanced Services Format" on page 6.)

3. Upload the migrated JUNOS Enhanced Services configuration file to the router. (See "Uploading the Migrated JUNOS Enhanced Services Configuration File to the Router" on page 7.)

4. Register the new hardware configuration. (See "Registering the New Hardware Configuration" on page 8.)

Before You Begin

Before you migrate a ScreenOS configuration to JUNOS Enhanced Services, you need to perform the following tasks. For more information, see your conversion kit documentation.

- Download a copy of the ScreenOS configuration (so that you can migrate it to JUNOS Enhanced Services format later).

- Enter the set boot junos command to change the hardware platform's boot settings.

- Power off the SSG security device and remove it from a rack mount, if applicable.

- Replace the ScreenOS internal compact flash with the compact flash (with JUNOS Enhanced Services software) contained in your conversion kit.

- Place the device back in a rack mount, if applicable, and power on the device.

The device boots with the JUNOS Enhanced Services software. You now must complete the migration process, as described in "ScreenOS-to-JUNOS Enhanced Services Software Migration Overview" on page 6.

Migrating the ScreenOS Configuration to JUNOS Enhanced Services Format

You use the ScreenOS-to-JUNOS Enhanced Services Migration Tool to convert the ScreenOS configuration file to a JUNOS Enhanced Services configuration file. For more information, see "Using the ScreenOS-to-JUNOS Enhanced Services Migration Tool" on page 9.

Uploading the Migrated JUNOS Enhanced Services Configuration File to the Router

After reviewing the migrated JUNOS Enhanced Services configuration file, you upload it to the router. We recommend that you test the new configuration file in a lab or staging environment so that you can verify that the new configuration supports your network design. After you are satisfied that the configuration meets your network requirements, you can deploy the configuration to a production router.

To upload a migrated JUNOS Enhanced Services configuration file to the router:

1. Connect a PC or laptop to the console port of the router.

   For information about how to connect to the router's console port, see the *JUNOS Enhanced Services J-series Services Router Getting Started Guide*.

2. Using an asynchronous terminal emulation application, such as Microsoft HyperTerminal, log in as root. If you are logging in for the first time after using a conversion kit to convert an SSG security device to a J-series router, you do not need a password.

3. Enter the cli command at the console prompt to invoke the CLI and enter operational mode:

   ```
   root% cli
   root>
   ```

4. From operational mode in the CLI, enter the configure command to enter CLI configuration mode:

   ```
   root> configure
   root#
   ```

5. From configuration mode in the CLI, use the following command to configure a root password for the router so that you can commit configuration changes:

   ```
   root# set system root-authentication plain-text-password
   New password:
   Retype new password:

   [edit]
   root#
   ```

   The password does not appear as you type.

6. Make sure that you are at the top level of the configuration mode hierarchy. If you are below the top level, enter exit to return to the top level.

7. From the top level of the configuration hierarchy, enter the load override terminal command:

   ```
   root# load override terminal
   [Type ^D at a new line to end input]
   ```

8. Using a text editor, open the migrated JUNOS Enhanced Services configuration file.

9. Select all the text in the file, and copy the text.

10. Make the asynchronous terminal emulation application the active application.

11. Paste the text from the configuration file into the CLI.

12. Press Enter once. Make sure that you perform this step before proceeding.

13. Press Ctrl + d to indicate the end of the pasted text.

14. To verify the configuration but not activate it, use the commit check command:

    ```
    root# commit check
    ```

    If the validation is successful, go to Step 15. Otherwise, review any error messages and use the CLI to change the configuration and resolve errors.

15. Commit the configuration to activate it:

    ```
    root# commit
    commit complete
    ```

    The migrated JUNOS Enhanced Services configuration file is activated and is now the running configuration on the router.

Registering the New Hardware Configuration

After thoroughly testing the configuration and deciding to make the hardware conversion permanent, make sure to register the new hardware configuration and validate it with Juniper Networks Customer Service, as described in the *Read This First* document included with your OS conversion kit. You can register the new hardware configuration only once.

After registering the new hardware configuration, allow up to 45 days for restocking of the new hardware configuration to support any Next Day or Same Day contracts. Juniper Networks Customer Service will provide best-effort support until restocking of the converted product is complete. After the registration process is completed, your Customer Support Center access profile is updated so that you can access the software and tools that support your new hardware configuration.

Chapter 3

Using the ScreenOS-to-JUNOS Enhanced Services Migration Tool

After converting an SSG security device to a J-series router, you need to migrate the ScreenOS configuration file to a JUNOS Enhanced Services configuration file before you can use JUNOS Enhanced Services software. To migrate your ScreenOS configuration file, use the ScreenOS-to-JUNOS Enhanced Services Migration Tool, which is a Web-based tool available on the Juniper Networks Web site.

JUNOS Enhanced Services software requires security zone information before you can manage the router remotely. The ScreenOS-to-JUNOS Enhanced Services Migration Tool takes interface information in the ScreenOS configuration and binds the interfaces to the security zones that were defined in the original configuration. When using the Migration Tool, you have the option to map ScreenOS interfaces to JUNOS Enhanced Services interfaces.

This chapter contains the following sections:

ScreenOS Features Supported and Not Supported by the Migration Tool

For the list of ScreenOS features that are supported and not supported by the ScreenOS to JUNOS Enhanced Services Migration Tool, see http://migration-tools.juniper.net/s2jes/s2jes-feature-status.jsp.

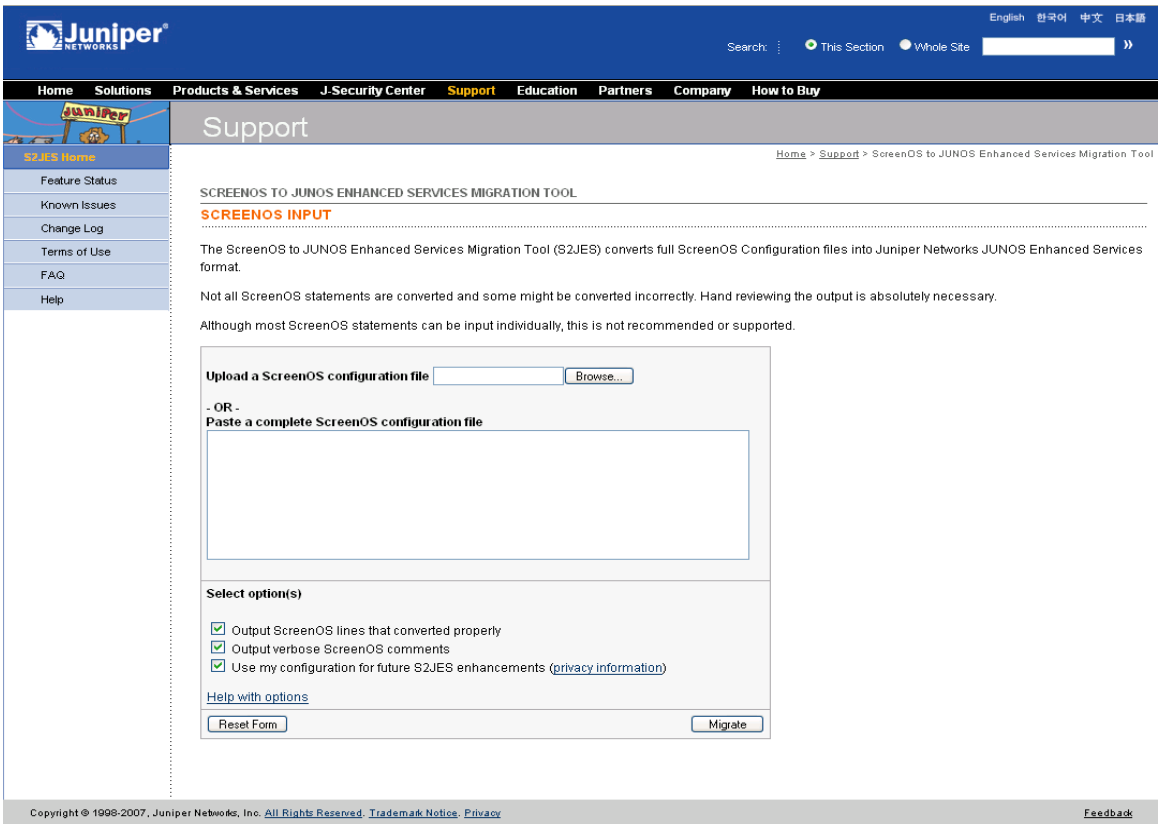
Migrating a ScreenOS Configuration File to a JUNOS Enhanced Services Configuration File

To migrate your downloaded ScreenOS configuration file to a JUNOS Enhanced Services configuration file, use the ScreenOS-to-JUNOS Enhanced Services Migration Tool (S2JES).

To migrate the ScreenOS configuration to a JUNOS Enhanced Services configuration:

1. Using a Web browser, navigate to http://migration-tools.juniper.net.
2. Log in using your Juniper Networks support username and password.

   If you do not have a Juniper Networks user account, go to https://www.juniper.net/registration/Register.jsp and complete the registration form.
3. On the Migration Tools home page, select **ScreenOS to JUNOS-ES**. The Terms of Use page appears.
4. Read the contents of the Terms of Use page.
5. If you agree to the terms of use, click **I Agree**. The ScreenOS to JUNOS Enhanced Services Migration Tool page appears.



6. On the ScreenOS to JUNOS Enhanced Services Migration Tool page, click the **Browse** button (next to the Upload an JUNOS config file box).

NOTE: To migrate an entire configuration, upload the configuration file to the ScreenOS to JUNOS Enhanced Services Migration Tool page. Use the copy and paste feature to convert a small set of ScreenOS commands.

7. Navigate to the directory that contains the ScreenOS configuration file that you downloaded.

8. Select the ScreenOS configuration file, and click **Open**.

9. Select or clear any conversion options. By default, all options are selected.

   - **Output ScreenOS lines that converted properly**—Select this option to display all ScreenOS configuration statements, even those that have no warnings, errors, or informational messages associated with them after the conversion.

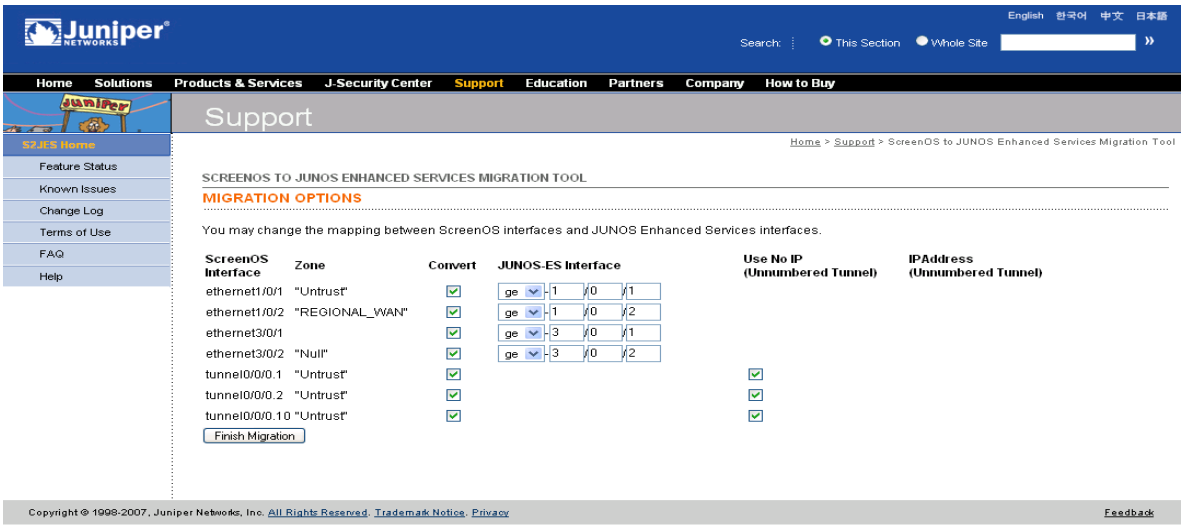
   - **Output verbose ScreenOS comments**—Select this option to display informational messages associated with certain statements. These informational messages usually describe differences between defaults in ScreenOS and JUNOS Enhanced Services software.

   - **Use my configuration for future S2JES enhancements**—Select this option to save your configuration and possibly have it used by Juniper Networks for Migration Tool testing and future enhancements. Go to http://migration-tools.juniper.net/s2jes/s2jes-security.jsp for more information about how your configuration information might be used.

   For online help for these options, click the **Help with options** link on the ScreenOS to JUNOS Enhanced Services Migration Tool page.

10. Click **Migrate**.

    The ScreenOS configuration is analyzed, and if interfaces are defined in the configuration, the Migration Options page appears.



The Migration Options page lists all of the interfaces in the configuration.

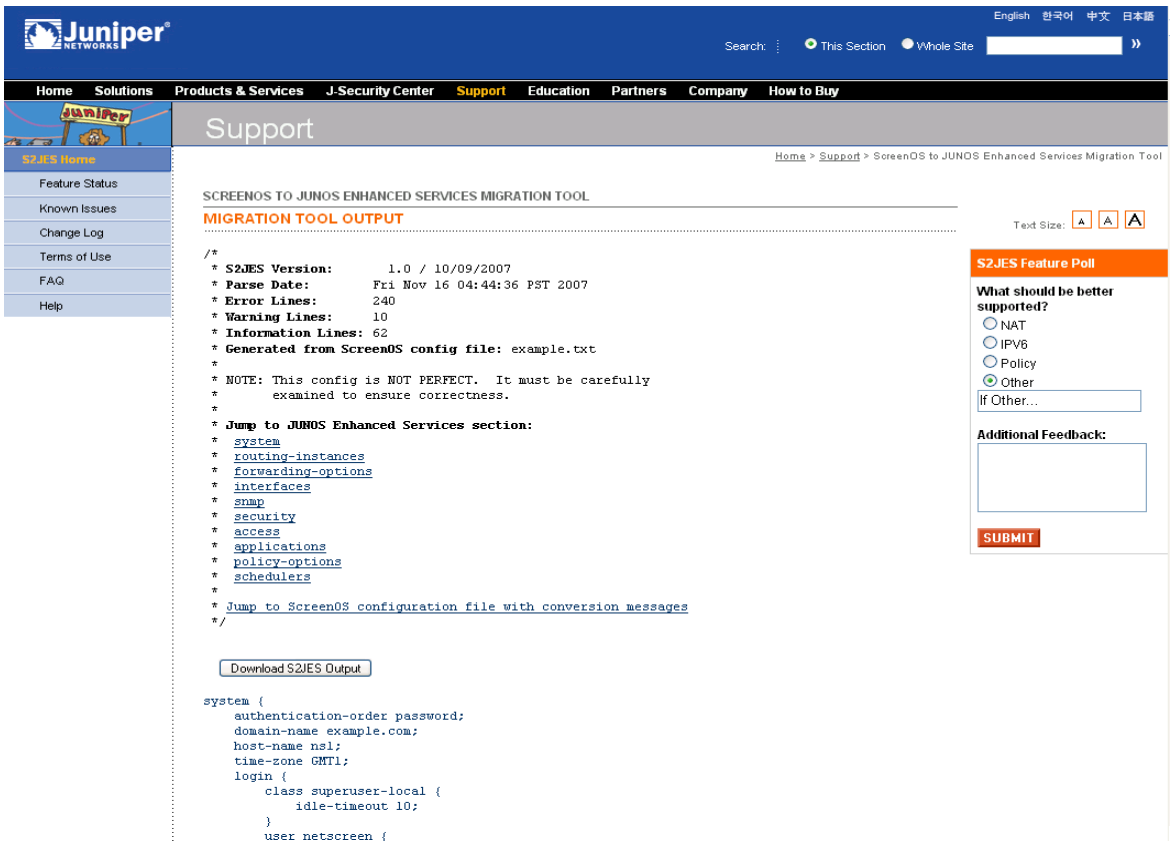
11. You can specify the following options from the Migration Options page:

    - To convert a ScreenOS interface to a JUNOS Enhanced Services interface—Select the **Convert** box. To prevent conversion of a ScreenOS interface, clear the **Convert** box. By default, all ScreenOS interfaces are converted to JUNOS Enhanced Services interfaces.

    - To change the mapping between a ScreenOS interface and JUNOS Enhanced Services interface—Select the interface type from the list, and type the Physical Interface Module (PIM) slot and port number.

    - To assign no IP address to a tunnel interface (if the ScreenOS configuration had tunnel interfaces defined)—Select the **Use No IP (Unnumbered Tunnel)** box. To assign an IP address, clear the box and then type the IP address and subnet mask in classless interdomain routing (CIDR) format in the two fields that appear.

12. Click **Finish Migration**. The Migration Tool Output page appears, listing the newly migrated JUNOS Enhanced Services configuration. After the JUNOS Enhanced Services configuration, the original ScreenOS configuration is listed with any errors, warnings, or comments associated with the conversion.



For more information about reviewing the newly migrated configuration, see “Downloading and Reviewing the Migrated Configuration File” on page 13.

Migrating Small ScreenOS Configuration Files or Partial Configurations

You can migrate small ScreenOS configuration files or partial ScreenOS configurations to JUNOS Enhanced Services configurations by copying the ScreenOS statements directly into the ScreenOS-to-JUNOS Enhanced Services Migration Tool page:

1. If you are migrating a configuration file, open the ScreenOS configuration file in a text editor.
2. Copy the text in the configuration file.
3. In the ScreenOS to JUNOS Enhanced Services Migration Tool page, paste the text in the Paste a complete JUNOS config file box.
4. Click **Migrate**. The Migration Tool Output page appears, listing the newly migrated JUNOS Enhanced Services configuration. After the JUNOS Enhanced Services configuration, the original ScreenOS configuration is listed with any errors, warnings, or comments associated with the conversion.

Downloading and Reviewing the Migrated Configuration File

After migrating the ScreenOS configuration to a JUNOS Enhanced Services configuration, download it and carefully review each line to ensure that your configuration was migrated properly. Also use the migration output, which is the original ScreenOS configuration and the associated messages listed on the Migration Tool Output page, to assist you. If necessary, identify the commands that the ScreenOS-to-JUNOS Enhanced Services Migration Tool could not convert.

When reviewing the migration output, make sure that the following areas were properly converted:

- Interface configuration—Verify that the IP addresses that were configured to remotely manage the security device are properly converted in the migration output.
- System services—Verify that the protocols used to manage the security device are listed at the [edit system services] and [edit security zones security-zone *security-zone* host-inbound-traffic system-services] hierarchy levels.
- Security policies—Verify that the JUNOS Enhanced Services security policies correctly allow and deny network and VPN traffic.

Interpreting Messages in the Migration Output

Errors, warnings, and comments are indicated as follows in the migration output:

- Any ScreenOS configuration statements that could not be converted are listed in red.
- Any warnings or comments associated with configuration statements are listed in blue.
- Any previously displayed errors or warnings are listed in magenta.

Here are some of the common messages that you might see in the migration output and their explanations:

- "Line not recognized by S2JES" (error)—The ScreenOS-to-JUNOS Enhanced Services Migration Tool does not recognize this ScreenOS command. There might be an equivalent configuration statement in JUNOS Enhanced Services software.
- "Line not yet supported by S2JES" (error)—Currently, this ScreenOS command is not supported by the ScreenOS-to-JUNOS Enhanced Services Migration Tool. The feature might be supported in JUNOS Enhanced Services software.
- "This is not supported in JUNOS-ES" (error)—The feature for this command is not supported in JUNOS Enhanced Services software.
- "Command-name is not supported in JUNOS-ES" (warning)—The feature for this command is not supported in JUNOS Enhanced Services software.
- "Feature is not currently supported" (warning)—The feature for this command is not currently supported.

Downloading the Migrated Configuration File

After you are satisfied that the configuration statements are properly translated, click the **Download S2JES Output** button on the ScreenOS to JUNOS Enhanced Services Migration Tool page to download the translated JUNOS Enhanced Services configuration file (for example, s2jesOutput) to your local system.

After you have downloaded the JUNOS Enhanced Services configuration file, you need to edit it to add passwords and other encrypted keys. For more information, see "Editing the Migrated Configuration File" on page 14.

Editing the Migrated Configuration File

For security purposes, the ScreenOS-to-JUNOS Enhanced Services Migration Tool does not include the encrypted passwords for users from the ScreenOS configuration in the migrated configuration file. Before you upload the migrated configuration file to the router, if you have a valid JUNOS configuration file, you can include the encrypted passwords for the root user and one local user account by editing the migrated configuration file. If you do not have a valid JUNOS configuration file, use the set system root-authentication statement to set the root password.

If the original ScreenOS configuration contained encrypted keys, such as preshared keys for IKE policy authentication, the keys are not included in the migrated configuration file and are replaced by ASCII text. You must replace the ASCII text with each actual preshared key. The keys are encrypted when you upload the migrated configuration file to the router.

To edit the migrated configuration file:

1. On your system, open the migrated configuration file in a text editor.

2. Open a valid JUNOS configuration file that contains the encrypted passwords for the root user and a local user account.

3. In the JUNOS configuration file, copy the encrypted-password statement for the root user. This statement is located at the [system root-authentication] hierarchy level.

4. In the migrated configuration file, replace the plain-text-password statement for the root user with the encrypted-password statement from the JUNOS configuration file.

5. In the JUNOS configuration file, copy the encrypted-password statement for a local user. This statement is located at the [system login user authentication] hierarchy level.

6. In the migrated configuration file, replace the plain-text-password statement for the local user with the encrypted-password statement from the JUNOS configuration file.

7. Replace the ASCII text for any encrypted keys with the actual keys.

   For example, replace the ASCII text for any preshared keys for IKE policy authentication with the actual preshared key. The keys are encrypted when you upload the file to the router.

8. Save the migrated configuration file.

You are now ready to upload the migrated configuration file to the router. For more information, see “Uploading the Migrated JUNOS Enhanced Services Configuration File to the Router” on page 7.

Chapter 4

Converting JUNOS or JUNOS Enhanced Services Software to ScreenOS by Compact-Flash Method

You can convert certain J-series Services Routers running JUNOS or JUNOS Enhanced Services software to SSG security devices with the appropriate conversion kit. (See Table 10.)

Table 10: Convertible J-series Hardware and Software

Services Router with JUNOS 8.3 or Later	Conversion Kit (if applicable)	Resulting SSG Security Device (if applicable)
J2320	J2320-SSG-CONV-S	SSG 320M
J2350	J2350-SSG-CONV-S	SSG 350M
J4350	J4350-SSG-CONV-S	SSG 520M
J6350	J6350-SSG-CONV-S	SSG 550M

Use the appropriate conversion kit in the following situations:

- Convert a J-series Services Router to an SSG security device.
- After converting an SSG security device to a J-series Services Router and registering the new hardware configuration, convert the J-series router back to an SSG security device.

For information about converting J-series Services Routers to SSG security devices, see the documentation included with your conversion kit.

Chapter 5

Migrating JUNOS to JUNOS Enhanced Services

You can migrate a J2320, J2350, J4350, or J6350 Services Router running JUNOS 8.3 or later, with basic network connectivity, to the JUNOS Enhanced Services software.

If you follow the procedures in this chapter, the router retains connectivity to the network and can be managed remotely.

NOTE: J-series Services Routers are currently shipped with the JUNOS software. Before using the procedures in this chapter, you must first establish basic network connectivity for the router. For more information, see the *JUNOS Enhanced Services J-series Services Router Getting Started Guide*.

This chapter contains the following sections:

JUNOS-to-JUNOS Enhanced Services Migration Overview

Migrating JUNOS software to JUNOS Enhanced Services is similar to upgrading JUNOS software, except that you must first convert your JUNOS configuration file to a JUNOS Enhanced Services configuration file. After the conversion, you download the JUNOS Enhanced Services software image in a software package, install the image on the router, and reboot the router so the software and configuration take effect.

JUNOS-to-JUNOS Enhanced Services Migration Tasks

To migrate JUNOS software to JUNOS Enhanced Services, you perform the following tasks:

CAUTION: Be sure to follow this sequence of tasks when migrating to JUNOS Enhanced Services. If you try to install JUNOS Enhanced Services on the router before uploading your migrated configuration file, you lose IP-based remote management access and must use the console port to access the router. (Console access is not affected.)

1. Backing Up the JUNOS Configuration File on page 22
2. Downloading and Decompressing the JUNOS Configuration File on page 22
3. Migrating the JUNOS Configuration to a JUNOS Enhanced Services Configuration on page 23
4. Renaming and Uploading the New JUNOS Enhanced Services Configuration File on page 23
5. Downloading JUNOS Enhanced Services Software from Juniper Networks on page 24
6. Verifying Available Compact Flash Space on page 25
7. Managing Compact Flash Space on page 26
8. Installing JUNOS Enhanced Services Software with the CLI on page 35

Understanding Software Packages

All JUNOS and JUNOS Enhanced Services software is delivered in signed packages that contain digital signatures to ensure official Juniper software. For more information about signed software packages, see the *JUNOS Software Installation and Upgrade Guide*.

An upgrade software package name is in the following format: *package-name-m.nZx.y-distribution*.tgz.

- *package-name* is the name of the package—for example, junos-jsr.
- *m.n* is the software release, with *m* representing the major release number and *n* representing the minor release number—for example, 8.5.

- *Z* indicates the type of software release. For example, R indicates released software, and B indicates beta-level software.
- *x.y* represents the software build number and spin number—for example, 1.1.
- *distribution* indicates the area for which the software package is provided—domestic for the United States and Canada and export for worldwide distribution.

A sample JUNOS Enhanced Services software package name is junos-jsr-8.5R1.1-domestic.tgz.

Before You Begin

Before you upgrade a J-series Services Router running the JUNOS software to the JUNOS Enhanced Services software, make sure that the following requirements are met:

- The version of JUNOS software running on the router must be JUNOS Release 8.3 or later.
- Make sure that the Services Router has basic connectivity to your network and that you have remote management access to the router. Also make sure that you have configured a root user account for the router.
- Before a migration, you can optionally back up your primary boot device onto a secondary storage device, such as a USB storage drive. If you have a power failure during a migration, the primary boot device can fail or become corrupted. In either case, if a backup device is not available, the router might be unable to boot and come back online. Creating a backup also stores your active configuration files and log files and ensures that you recover to a known, stable environment in case of an unsuccessful migration.

  During a successful migration, the software package completely reinstalls the existing software. The process retains configuration files, log files, and similar information from the previous version.
- The router must have FTP or SSH enabled to allow file transfers to and from the router.
- The router must allow login with start shell operational command privileges.
- You must know the root password for the router and have one of the following types of user accounts:
  - Account with access and privileges for the superuser class
  - Account with start shell operational command privileges

Backing Up the JUNOS Configuration File

Make a backup copy of the JUNOS configuration file you want to migrate, juniper.conf.gz, which is located in the /config directory.

In operational mode on the router, enter the start shell command to start a shell session:

```
user@host> start shell
%
```

At the shell prompt (%), enter the following command:

```
% cp /config/juniper.conf.gz /path/juniper.conf.junos.gz
```

Replace */path* with the path of the directory to which you want to copy the configuration file. If you want to copy the backup file to the /config directory, make sure you have root privileges (using the su UNIX command) before using the cp command.

After creating a backup file of the JUNOS configuration file, you now need to download and compress it. See "Downloading and Decompressing the JUNOS Configuration File" on page 22.

Downloading and Decompressing the JUNOS Configuration File

The /config/juniper.conf.gz file is a file compressed file by the GNU zip (gzip) utility. The gzip utility is available on most UNIX-based systems. Third-party compression utilities such as WinZip also support this compression format. For more information about gzip, see http://www.gnu.org/software/gzip/.

As part of the migration process, you need to download and decompress the JUNOS configuration and file and then convert it to JUNOS Enhanced Services format. Use a utility such as gunzip or a third-party compression utility that supports the .gz format, such as WinZip, to decompress the configuration file. After decompression, you have an ASCII file named juniper.conf, which contains the JUNOS configuration statements. You convert the file with the JUNOS-to-JUNOS Enhanced Services Migration Tool, which is a Web-based tool available on the Juniper Networks Web site.

You can download and decompress the existing JUNOS configuration file using one of the following methods, depending on whether you have gunzip or a compression utility (such as WinZip) on the system to which you download the configuration file:

- If you have gunzip or another compression utility that supports .gz files on your local system:

    1. Using FTP or SCP, download the /config/juniper.conf.gz file to a local system so that you can decompress the file. If you use FTP to download /config/juniper.conf.gz, use binary as the transfer method.

2. Use gunzip or another compression utility to decompress the juniper.conf.gz file. Refer to your compression utility's documentation for information about using the utility.

   After you have decompressed juniper.conf.gz, the resulting file is juniper.conf.

- If you do not have gunzip or another compression utility that supports .gz files on your local system:

  1. At the shell prompt (%) on the Services Router, navigate to the user account's home directory and create a copy of /config/juniper.conf.gz in the user's home directory:

     % **cd**
     % **cp /config/juniper.conf.gz ./juniper.conf.gz**

  2. Decompress the juniper.conf.gz file by entering the following command:

     % **gunzip juniper.conf.gz**

     The resulting juniper.conf file is now in the user account's home directory.

  3. Use FTP or SCP to download the juniper.conf file to your local system. If you use FTP to download juniper.conf, use ASCII as the transfer method.

After you have downloaded and decompressed juniper.conf, you need to migrate the juniper.conf file. See "Migrating the JUNOS Configuration to a JUNOS Enhanced Services Configuration" on page 23.

Migrating the JUNOS Configuration to a JUNOS Enhanced Services Configuration

You use the JUNOS-to-JUNOS Enhanced Services Migration Tool to convert the JUNOS configuration file to a JUNOS Enhanced Services configuration file. For more information, see "Using the JUNOS-to-JUNOS Enhanced Services Migration Tool" on page 37.

Renaming and Uploading the New JUNOS Enhanced Services Configuration File

After downloading the new JUNOS Enhanced Services configuration file, you rename it and upload it to the router. We recommend that you test the new configuration file in a lab or staging environment so that you can verify that the new configuration supports your network design. After you are satisfied that the configuration meets your network requirements, you can deploy the configuration to a production router.

To rename and upload the new JUNOS Enhanced Services configuration file:

1. On your local system, navigate to the migrated JUNOS Enhanced Services configuration file (for example, juniper-j2jesOutput.conf) that you downloaded in "Migrating the JUNOS Configuration to a JUNOS Enhanced Services Configuration" on page 23.

2. Rename the migrated file to juniper.conf. If you rename the file from a text editor, make sure that the line breaks, or end-of-line (EOL) characters, are compatible with UNIX,

3. If you are not at the shell prompt on the router, use the start shell operational command to start a shell.

4. At the shell prompt, type the su UNIX command to switch to a user with root privileges:

   ```
   % su
   root@host%
   ```

5. Use FTP or SCP to upload the juniper.conf file to the /var/tmp directory. If you use FTP to upload juniper.conf, use ASCII as the transfer method.

   Verify that the juniper.conf file is intact, with UNIX-compatible line breaks, using a text editor such as vi or emacs.

6. Create a new directory to store existing configuration files:

   ```
   root@host% mkdir /config/backup
   ```

7. Move the existing configuration files to the new backup directory:

   ```
   root@host% mv /config/backup/juniper.conf* /config/backup
   ```

8. Copy the juniper.conf file to /config:

   ```
   root@host% cp /var/tmp/juniper.conf /config/juniper.conf
   ```

   After you have uploaded the new JUNOS Enhanced Services configuration file, you can download the JUNOS Enhanced Services software. For more information, see "Downloading JUNOS Enhanced Services Software from Juniper Networks" on page 24.

Downloading JUNOS Enhanced Services Software from Juniper Networks

To download JUNOS Enhanced Services software:

1. If you have not already created a Web account with Juniper Networks, complete the registration form at the Juniper Networks Web site: https://www.juniper.net/registration/Register.jsp.

2. Using a Web browser, follow the links to the download URL on the Juniper Networks Web page. Depending on your location, select either **Canada and U.S. Version** or **Worldwide Version**:
   - https://www.juniper.net/support/csc/swdist-domestic/
   - https://www.juniper.net/support/csc/swdist-ww/
3. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
4. Select the appropriate JUNOS Enhanced Services software package.
5. Download the software to a local host or to an internal software distribution site.
6. After you have downloaded JUNOS Enhanced Services software, verify that the router has enough space on the compact flash to install the software. You can delete unneeded files, if necessary. For more information, see "Verifying Available Compact Flash Space" on page 25.

Verifying Available Compact Flash Space

Before you install JUNOS Enhanced Services software, verify that you have enough space on the compact flash to successfully complete the installation. If you need more compact flash space, you can delete unnecessary files.

To see how much space is available on the compact flash, use the CLI operational mode command show system storage:

```
user@host> show system storage
Filesystem             Size       Used      Avail  Capacity   Mounted on
/dev/ad0s1a            213M       119M       92M       57%  /
devfs                  1.0K       1.0K        0B      100%  /dev
devfs                  1.0K       1.0K        0B      100%  /dev/
/dev/md0               155M       155M        0B      100%  /junos
/cf                    213M       119M       92M       57%  /junos/cf
devfs                  1.0K       1.0K        0B      100%  /junos/dev/
procfs                 4.0K       4.0K        0B      100%  /proc
/dev/bo0s1e             24M        16K       24M        0%  /config
/dev/md1               168M       7.2M      147M        5%  /mfs
/dev/md2                58M        42K       53M        0%  /jail/tmp
/dev/md3               7.7M       100K      7.0M        1%  /jail/var/etc
devfs                  1.0K       1.0K        0B      100%  /jail/dev
/dev/md4               1.9M       6.0K      1.7M        0%  /jail/html/oem
```

The show system storage command output displays information about the root file system on the compact flash on the line that contains only a forward slash (/) in the "Mounted on" column. In this example, the compact flash has 92 MB of available space.

To determine whether you have sufficient compact flash space to install the JUNOS Enhanced Services software Release 8.5R1, follow these guidelines:

- To copy the software image to the router and install using that image, you need at least 130 MB of available space on the compact flash.
- To install the software, you need at least 68 MB of available space on the compact flash to install the software without copying the software image to the router. To upgrade without copying the software image to the router, you use the no-copy and unlink options with the request system software add CLI command.

If the router has enough space, you can now install JUNOS Enhanced Services software. For more information, see "Installing JUNOS Enhanced Services Software with the CLI" on page 35.

If you do not have the minimum amount of compact flash space to successfully install the software, see "Managing Compact Flash Space" on page 26 for information about deleting unused files from the compact flash.

Managing Compact Flash Space

To increase the amount of available space on the compact flash, you can delete unused files in one or more of the following ways:

- Deleting the Backup Software Image on page 26.
- Cleaning Up Log, Temporary, and Diagnostic Files on page 28.
- Deleting Remaining Temporary Files and Old Software Images on page 29.
- Verifying and Removing the Swap Partition on page 33.

Deleting the Backup Software Image

When you install software on the router, it creates a backup image of the software that was previously installed so that you can downgrade to that software version if necessary. You can delete this image to free available compact flash space.

CAUTION: If you delete this image, you cannot roll back to this software release (using **Manage > Software > Downgrade** in the J-Web interface or the request system software rollback operational command in the CLI).

Deleting the Backup Software Image with the J-Web Interface

To delete the backup software image using J-Web:

1. In the J-Web interface, select **Manage > Files**.
2. In the Delete Backup JUNOS Package section, review the backup image information listed.

3. To delete the backup image, click the **Delete backup JUNOS package** link.

4. Click one of the following buttons on the confirmation page:

   - To delete the backup image and return to the Files page, click **OK**.

   - To cancel the deletion of the backup image and return to the Files page, click **Cancel**.

5. After deleting the backup software image, use the show system storage command to see if you have enough available space on the compact flash to perform an upgrade. (See "Verifying Available Compact Flash Space" on page 25.)

6. Do one of the following:

   - If enough space is available, see "Installing JUNOS Enhanced Services Software with the CLI" on page 35 to proceed with the installation.

   - If you do not have enough available space, see "Cleaning Up Log, Temporary, and Diagnostic Files" on page 28 for information about other files you can delete.

Deleting the Backup Software Image with the CLI

To delete the backup software image using the CLI:

1. In operational mode in the CLI, enter the request system software delete-backup command:

   user@host> **request system software delete-backup**

2. Enter yes when prompted:

   Delete backup system software package [yes,no] (no) **yes**

3. After deleting the backup software image, use the show system storage command to see if you have enough available space on the compact flash to install the software. (See "Verifying Available Compact Flash Space" on page 25.)

4. Do one of the following:

   - If enough space is available, see "Installing JUNOS Enhanced Services Software with the CLI" on page 35 to proceed with the installation.

   - If you do not have enough available space, see "Cleaning Up Log, Temporary, and Diagnostic Files" on page 28 for information about other files you can delete.

Cleaning Up Log, Temporary, and Diagnostic Files

You can use the J-Web interface or the CLI request system storage cleanup command to rotate log files and delete unnecessary files on the Services Router. If you are running low on storage space, this file cleanup procedure quickly identifies files that can be deleted.

The file cleanup procedure performs the following tasks:

- Rotates log files—All information in the current log files is archived, old archives are deleted, and fresh log files are created.
- Deletes log files in /var/log—Any files that are not currently being written to are deleted.
- Deletes temporary files in /var/tmp—Any files that have not been accessed within two days are deleted.
- Deletes all diagnostic files in /var/crash—Any core files that the router has written during an error are deleted.
- Deletes all software images (*.tgz files) in /var/sw/pkg—Any software images copied to this directory during software upgrades are deleted.

Cleaning Up Files with the J-Web Interface

To rotate log files and delete unnecessary files with the J-Web interface:

1. In the J-Web interface, select **Manage > Files**.
2. In the Clean Up Files section, click **Clean Up Files**. The router rotates log files and identifies the files that can be safely deleted.

   The J-Web interface displays the files that you can delete and the amount of space that will be freed on the file system.
3. Click one of the following buttons on the confirmation page:
   - To delete the files and return to the Files page, click **OK**.
   - To cancel your entries and return to the list of files in the directory, click **Cancel**.
4. After cleaning up files, use the show system storage command to see if you have enough available space on the compact flash to install the software. (See “Verifying Available Compact Flash Space” on page 25.)
5. Do one of the following:
   - If enough space is available, see “Installing JUNOS Enhanced Services Software with the CLI” on page 35 to proceed with the installation.
   - If you do not have enough available space, see “Deleting Remaining Temporary Files and Old Software Images” on page 29 for information about other files you can delete.

Cleaning Up Files with the CLI

To rotate log files and delete unnecessary files with the CLI:

1. Enter operational mode in the CLI.
2. To rotate log files and identify the files that can be safely deleted, enter the following command:

   user@host> **request system storage cleanup**

   The router rotates log files and displays the files that you can delete.
3. Enter yes at the prompt to delete the files.

NOTE: You can issue the request system storage cleanup dry-run command to review the list of files that can be deleted with the request system storage cleanup command, without actually deleting the files.

4. After cleaning up files, use the show system storage command to see if you have enough available space on the compact flash to install the software. (See "Verifying Available Compact Flash Space" on page 25.)
5. Do one of the following:
   - If enough space is available, see "Installing JUNOS Enhanced Services Software with the CLI" on page 35 to proceed with the installation.
   - If you do not have enough available space, see "Deleting Remaining Temporary Files and Old Software Images" on page 29 for information about other files you can delete.

Deleting Remaining Temporary Files and Old Software Images

After you complete the procedure "Cleaning Up Log, Temporary, and Diagnostic Files" on page 28, some temporary files might remain (for example, files that have been accessed within the last two days) in the /cf/var/tmp directory, as well as old software images in the /var/sw/pkg directory. Check for any remaining temporary files or old software images, and manually delete them.

Deleting Files with the J-Web Interface

To delete files with the J-Web interface:

1. In the J-Web interface, select **Manage > Files**.
2. In the Download and Delete Files section, click **Temporary Files**.

   The J-Web interface displays the files located in the directory.
3. Check the box next to each file you plan to delete.

4. Click **Delete**.

   The J-Web interface displays the files that you can delete and the amount of space that will be freed on the file system.

5. Click one of the following buttons on the confirmation page:

   - To delete the files and return to the Files page, click **OK**.
   - To cancel your entries and return to the list of files in the directory, click **Cancel**.

6. In the Download and Delete Files section on the Files page, click **Old JUNOS Software**.

   The J-Web interface displays the files located in the directory.

7. Check the box next to each file you plan to delete.

8. Click **Delete**.

   The J-Web interface displays the files that you can delete and the amount of space that will be freed on the file system.

9. Click one of the following buttons on the confirmation page:

   - To delete the files and return to the Files page, click **OK**.
   - To cancel your entries and return to the list of files in the directory, click **Cancel**.

10. After manually deleting any remaining temporary files, use the show system storage command to see if you have enough available space on the compact flash to install the software. (See “Verifying Available Compact Flash Space” on page 25.)

11. Do one of the following:

    - If enough space is available, see “Installing JUNOS Enhanced Services Software with the CLI” on page 35 to proceed with the installation.
    - If you do not have enough available space, see “Verifying and Removing the Swap Partition” on page 33.

Deleting Files with the CLI

You can use the CLI to manually delete any remaining temporary files or old software images.

To delete files using the CLI:

1. From operational mode in the CLI, enter the following command to display a list of the files in the /cf/var/tmp directory:

```
user@host> file list /cf/var/tmp detail
/cf/var/tmp:
total 178
-rw-r--r--  1 root  wheel       3916 Oct 22 15:45 cleanup-pkgs.log
drwxrwxrwx  2 root  wheel        512 Jan 1   2001 install/
-rw-r--r--  1 jdoe  wheel      18005 Jul 17 06:53 cli.txt
-rw-r-----  1 root  wheel       2670 Oct 22 15:45 sampled.pkts
drwxrwxrwT  2 root  wheel        512 Oct 28 12:41 vi.recover/
```

2. From operational mode in the CLI, enter the following command to delete a file:

   user@host> **file delete /cf/var/tmp/***filename*
   user@host>

   To remove all files, enter the following command:

   user@host> **file delete /cf/var/tmp/***
   user@host>

NOTE: The file delete command does not delete files that are owned by root.

3. After manually deleting any remaining temporary files, use the show system storage command, as described in "Verifying Available Compact Flash Space" on page 25, to see if you have enough available space on the compact flash to install the software.

4. Do one of the following:

   - If enough space is available, see "Installing JUNOS Enhanced Services Software with the CLI" on page 35 to proceed with the installation.
   - If you do not have enough available space, go to Step 5.

5. To delete any remaining temporary files owned by root, you can manually delete them from the file system by using a UNIX shell. To do so, you must know the root password for the router and have one of the following types of user accounts:

   - Account with access and privileges for the superuser class
   - Account with start shell operational command privileges

6. In operational mode in the CLI, enter the following command:

   ```
   user@host> start shell
   %
   ```

7. At the shell prompt, enter the following command:

   ```
   % su
   ```

8. Enter the root password. The password does not appear as you type.

   ```
   Password:
   root@host%
   ```

9. Enter the following commands:

   ```
   root@host% cd /var/tmp
   root@host% ls
   ```

   Verify that the files listed in this directory are files that you want to delete.

10. Enter the following command:

    ```
    root@host% rm -rf /var/tmp/*
    root@host%
    ```

    This command removes all files in the /var/tmp directory and recursively removes directories (even those with files in them) without any prompting for confirmation. If no matching files are found, a "No match." message appears.

11. Enter the following command to remove all old software images in the /var/sw/pkg directory:

    ```
    root@host% rm -rf /var/sw/pkg/*.tgz
    root@host%
    ```

    This command removes all software images (*.tgz files) and recursively removes directories without any prompting for confirmation. If no matching files are found, a "No match." message appears.

12. Return to the default shell prompt by using the exit command:

    ```
    root@host% exit
    %
    ```

13. Enter the exit command to return to the operational mode in the CLI:

    ```
    % exit
    user@host>
    ```

14. After manually deleting any remaining temporary files, use the show system storage command to see if you have enough available space on the compact flash to install the software. (See "Verifying Available Compact Flash Space" on page 25.)

15. Do one of the following:

    - If enough space is available, see "Installing JUNOS Enhanced Services Software with the CLI" on page 35 to proceed with the installation.

    - If you do not have enough available space, see "Verifying and Removing the Swap Partition" on page 33.

Verifying and Removing the Swap Partition

If you tried to recover available compact flash space as described in "Managing Compact Flash Space" on page 26 and are still unable to install the JUNOS Enhanced Services software successfully, you can increase the available space on the internal compact flash by configuring the internal compact flash so that it no longer has a swap partition. Only remove the swap partition for an internal compact flash with a storage capacity of 256 MB.

To remove the swap partition, you use a Juniper Networks 256-MB USB storage device to take a snapshot of the existing software image and then reboot the router using the USB storage device as the boot medium. You then configure the swap space to zero and reboot the router again using the compact flash as the boot medium.

NOTE: If you remove the swap partition, you can no longer specify the internal compact flash as the medium used to store system software failure memory snapshots when using the set system dump-device CLI command. For J4350 or J6350 Services Routers, you need to specify a USB storage device (usb option) as the medium. For J2320 and J2350 Services Routers, you can specify a USB storage device (usb option) or the external compact flash (removable-compact-flash option) as the medium.

To verify whether the internal compact flash has a swap partition, see "Verifying the Swap Partition" on page 33.

Verifying the Swap Partition

To verify the swap partition:

1. In operational mode in the CLI, enter the following command:

   ```
   user@host> start shell
   %
   ```

2. At the shell prompt, enter the following command:

   ```
   % su
   ```

3. Enter the root password. The password does not appear as you type.

   ```
   Password:
   root@host%
   ```

4. Enter the following command:

   ```
   root@host% /sbin/disklabel /dev/ad0s1 | grep swap
     b:   174080   278449      swap                        # (Cyl.  552*- 897*)
   ```

5. Return to the default shell prompt by using the exit command:

   ```
   root@host% exit
   %
   ```

6. Enter the exit command to return to the operational mode in the CLI:

   ```
   % exit
   user@host>
   ```

7. Do one of the following:

   - If output is listed after you enter the command in Step 4, the compact flash has a swap partition. For information about removing the swap partition, see “Removing the Swap Partition” on page 34.
   - If no output is listed after you enter the command in Step 4, the compact flash does not have a swap partition. Contact the Juniper Networks Technical Assistance Center (JTAC). See “Requesting Support” on page xv.

Removing the Swap Partition

To remove the swap partition on the compact flash:

1. Insert a Juniper Networks 256-MB USB storage device into an available USB port of the Services Router to be upgraded.

2. From the operational mode in the CLI, enter the following command:

   ```
   user@host> request system snapshot as-primary partition swap-size 0 media usb
   ```

3. Enter the following command:

   ```
   user@host> request system reboot media usb
   ```

   This command will reboot the router and boot from the USB storage device with the original configuration file intact. After rebooting, the router is online and uses the configuration file as the running configuration.

4. Enter the following command:

   ```
   user@host> request system snapshot as-primary partition swap-size 0 media
   compact-flash
   ```

   This command repartitions the internal compact flash so that it has no swap partition.

5. Enter the following command:

   user@host> **request system reboot media compact-flash**

   This command reboots the router from the internal compact flash. After rebooting, the router is online with your running configuration, but the swap partition on the compact flash is removed.

6. Remove the USB storage device.

7. Use the show system storage command to check the available storage capacity on the compact flash. (See "Verifying Available Compact Flash Space" on page 25.)

8. Do one of the following:

   - If enough space is available, see "Installing JUNOS Enhanced Services Software with the CLI" on page 35 to proceed with the installation.

   - If you do not have enough available space, contact the Juniper Networks Technical Assistance Center (JTAC). See "Requesting Support" on page xv.

Installing JUNOS Enhanced Services Software with the CLI

To install JUNOS Enhanced Services software with the CLI:

1. Before installing the software, verify the available space on the compact flash, as described in "Verifying Available Compact Flash Space" on page 25.

2. If you have not already done so, download the software package, as described in "Downloading JUNOS Enhanced Services Software from Juniper Networks" on page 24.

3. To install the software package from a local directory on the router, copy the software package to the router. We recommend that you copy it to the /var/tmp directory.

   You do not need to copy the software package to the router to install the software. If you posted the software package to an FTP or Web server after downloading the package, you can use the server as the source from which to install.

4. From operational mode in the CLI, enter the following command to install the new package on the router:

   user@host> **request system software add no-validate unlink no-copy** *source-path*

   Replace *source-path* with one of the following paths:

   - For a software package that is installed from a local directory on the router—*/pathname/package-name* (for example, /var/tmp/junos-jsr-8.5R1.1-domestic.tgz).
   - For software packages that are downloaded and installed from a remote location:
     - ftp://*hostname/pathname/package-name*

     or

     - http://*hostname/pathname/package-name*

NOTE: The no-validate option prevents the JUNOS software from validating the software package against the current active configuration as a prerequisite to adding the software package. You need to specify this option because the configuration that is running on the router is still the JUNOS configuration (not the JUNOS Enhanced Services configuration file that you uploaded). The JUNOS Enhanced Services configuration file that you uploaded takes effect after the router reboots.

   The unlink option removes the package at the earliest opportunity so that the router has enough storage capacity to complete the installation.

   (Optional) The no-copy option specifies that a software package is installed, but a copy of the package is not saved in /var/sw/pkg. Include this option if you do not have enough space on the compact flash to perform an upgrade that keeps a copy of the package on the router.

5. After the software package is installed, reboot the router:

   user@host> **request system reboot**

   When the reboot is complete, you are able to establish IP-based remote access to the router.

   The router is now running JUNOS Enhanced Services software, and the JUNOS Enhanced Services configuration file that you uploaded before the software installation is now the active configuration.

6. To verify the JUNOS Enhanced Services configuration file, enter the show configuration command from operational mode in the CLI.

For information about configuring secure Web access and installing and managing J-series licenses, see the *JUNOS Enhanced Services J-series Services Router Getting Started Guide.*

Chapter 6

Using the JUNOS-to-JUNOS Enhanced Services Migration Tool

You need to migrate the JUNOS configuration file to a JUNOS Enhanced Services configuration file before you can use JUNOS Enhanced Services software. To migrate your JUNOS configuration file, use the JUNOS-to-JUNOS Enhanced Services Migration Tool, which is a Web-based tool available on the Juniper Networks Web site.

JUNOS Enhanced Services software requires security zone information before you can manage the router remotely. The JUNOS-to-JUNOS Enhanced Services Migration Tool takes interface information in the JUNOS configuration and binds the interfaces to a security zone named "Trust." Each interface is also assigned the types of incoming traffic to accept based on the protocols defined at the [edit system-services] hierarchy level in the original JUNOS configuration.

This chapter contains the following sections:

JUNOS Features Supported and Not Supported by the Migration Tool

For a list of JUNOS features that are supported and not supported by the JUNOS-to-JUNOS Enhanced Services Migration Tool, see http://migration-tools.juniper.net/j2jes/j2jes-feature-status.jsp.

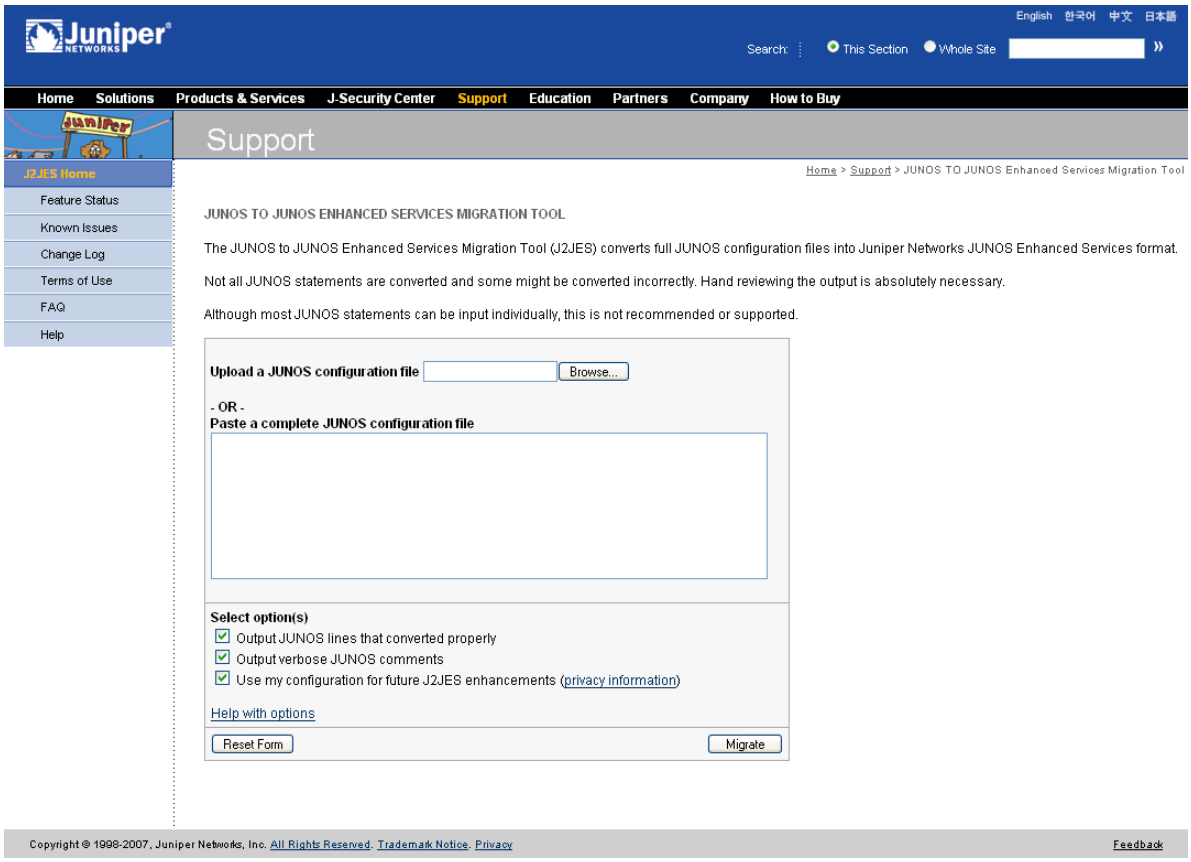
Migrating a JUNOS Configuration File to a JUNOS Enhanced Services Configuration File

To migrate your juniper.conf ASCII file to a JUNOS Enhanced Services configuration file, you use the Juniper Networks JUNOS-to-JUNOS Enhanced Services Migration Tool (J2JES).

To convert the JUNOS configuration to a JUNOS Enhanced Services configuration:

1. Using a Web browser, navigate to http://migration-tools.juniper.net.
2. Log in using your Juniper Networks support username and password.

   If you do not have a Juniper Networks user account, go to https://www.juniper.net/registration/Register.jsp and complete the registration form.
3. On the Migration Tools home page, select **JUNOS to JUNOS-ES**. The Terms of Use page appears.
4. Read the contents of the Terms of Use page. If you agree to the terms of use, click **I Agree**. The JUNOS to JUNOS Enhanced Services Migration Tool page appears.



5. On the JUNOS to JUNOS Enhanced Services Migration Tool page, click the **Browse** button (next to the Upload an JUNOS configuration file box).

NOTE: To migrate an entire configuration, upload the configuration file to the JUNOS to JUNOS Enhanced Services Migration Tool page. Use the copy and paste feature to convert a small set of configuration statements.

6. Navigate to the directory that contains the juniper.conf file (JUNOS configuration file).

7. Select the JUNOS configuration file, and click **Open**.

8. Select or clear any conversion options. By default, all options are selected.

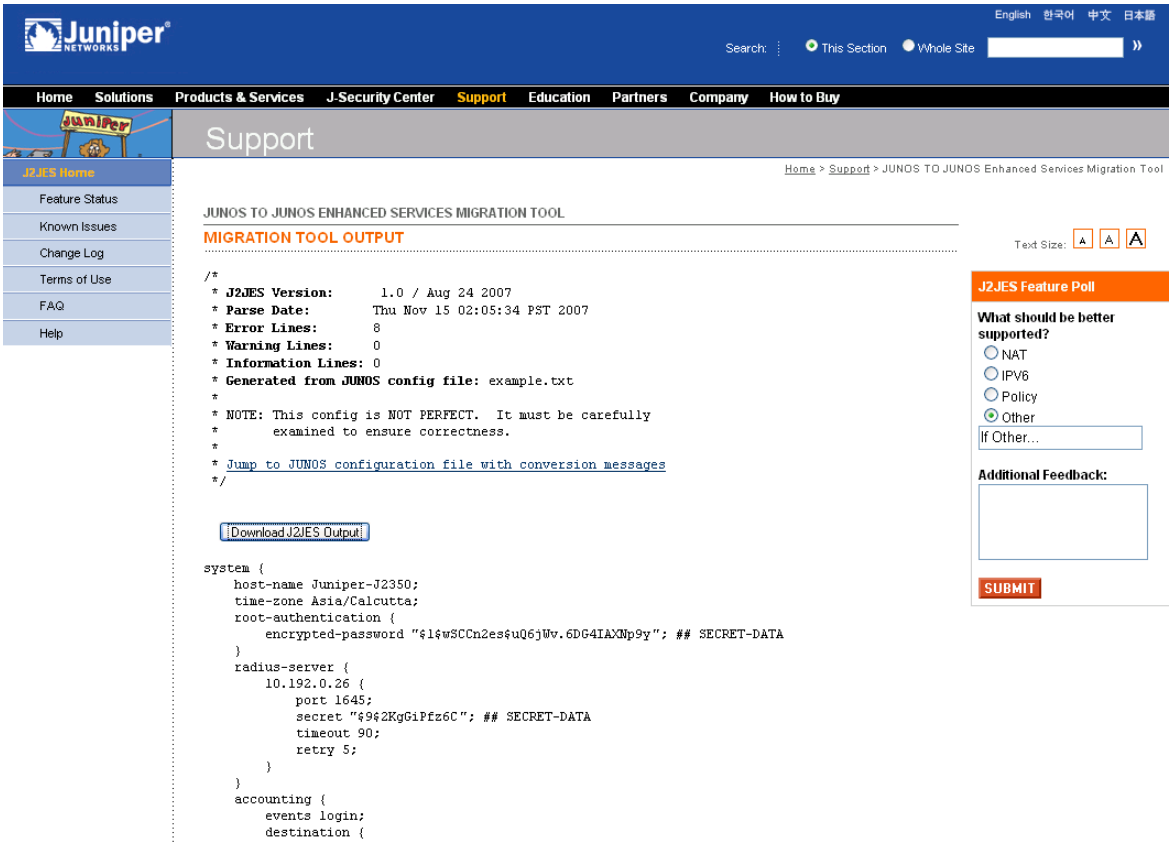
   - **Output JUNOS lines that converted properly**—Select this option to display all JUNOS configuration statements, even those that have no warnings, errors, or informational messages associated with them after the conversion.

   - **Output verbose JUNOS comments**—Select this option to display informational messages associated with certain statements. These informational messages usually describe differences between defaults in JUNOS and JUNOS Enhanced Services software.

   - **Use my configuration for future J2JES enhancements**—Select this option to save your configuration and possibly have it used by Juniper Networks for Migration Tool testing and future enhancements. Go to http:/migration-tools.juniper.net/j2jes/j2jes-security.jsp for more information about how your configuration information might be used.

   For online Help for these options, click the **Help with options** link on the JUNOS to JUNOS Enhanced Services Migration Tool page.

9. Click **Migrate**. The Migration Tool Output page appears, listing the newly migrated JUNOS Enhanced Services configuration. After the JUNOS Enhanced Services configuration, the original JUNOS configuration is listed with any errors, warnings, or comments associated with the conversion.



For more information about reviewing the newly migrated configuration, see “Downloading and Reviewing the Migrated Configuration File” on page 41.

Migrating Small JUNOS Configuration Files or Partial Configurations

You can migrate small JUNOS configuration files or partial JUNOS configurations to JUNOS Enhanced Services configurations by copying the JUNOS statements directly into the JUNOS to JUNOS Enhanced Services Migration Tool page:

1. If you are migrating a configuration file, open the JUNOS configuration file in a text editor.
2. Copy the text in the configuration file.
3. In the JUNOS to JUNOS Enhanced Services Migration Tool page, paste the text in the Paste a complete JUNOS configuration file box.
4. Click **Migrate**. The Migration Tool Output page appears, listing the newly migrated JUNOS Enhanced Services configuration. After the JUNOS Enhanced Services configuration, the original JUNOS configuration is listed with any errors, warnings, or comments associated with the conversion.

Downloading and Reviewing the Migrated Configuration File

After migrating the JUNOS configuration to a JUNOS Enhanced Services configuration, download it and carefully review each line to ensure that your configuration was migrated properly. Also use the migration output, which is the original JUNOS configuration and the associated messages listed on the Migration Tool Output page, to assist you. If necessary, identify the commands that the JUNOS-to-JUNOS Enhanced Services Migration Tool could not convert.

Downloading the Migrated Configuration File

Click the **Download J2JES Output** button on the JUNOS to JUNOS Enhanced Services Migration Tool page to download the migrated JUNOS Enhanced Services configuration file (for example, j2jesOutput) to your local system.

Reviewing the Migrated Configuration File

When reviewing the migrated configuration, make sure that the following areas were properly converted:

- Interface configuration—Verify that the IP addresses that were configured to remotely manage the router are properly converted in the migrated configuration.
- System services—Verify that the protocols listed at the [edit system services] hierarchy are now listed at the [edit system services] and [edit security zones security-zone Trust host-inbound-traffic system-services] hierarchy levels in the migrated configuration. These protocols are used to manage the router.
- Security policies—If stateful-firewall, services nat, or services ipsec-vpn configuration statements were defined in the JUNOS configuration, verify that the JUNOS Enhanced Services security policies correctly allow and deny network and VPN traffic.

Interpreting Messages in the Migration Output

Errors, warnings, and comments are indicated as follows in the migration output:

- Any JUNOS configuration statements that could not be converted are listed in red.
- Any warnings or comments associated with configuration statements are listed in blue.
- Any previously displayed errors or warnings are listed in magenta.

Here are some of the common messages that you might see in the migration output and their explanations:

- "Line not recognized by J2JES" (error)—The JUNOS-to-JUNOS Enhanced Services Migration Tool does not recognize this JUNOS command. There might be an equivalent configuration statement in JUNOS Enhanced Services software.
- "Line not yet supported by J2JES" (error)—Currently, this JUNOS command is not supported by the JUNOS-to-JUNOS Enhanced Services Migration Tool. The feature might be supported in JUNOS Enhanced Services software.
- "This is not supported in JUNOS-ES" (error)—The feature for this command is not supported in JUNOS Enhanced Services software.
- "Command-name is not supported in JUNOS-ES" (warning)—The feature for this command is not supported in JUNOS Enhanced Services software.
- "Feature is not currently supported." (warning)—The feature for this command is not currently supported.

Adding Key Information to the Migrated Configuration File

For security purposes, the JUNOS-to-JUNOS Enhanced Services Migration Tool does not include encrypted data for keys, such as preshared keys for IKE policy authentication, in the migrated configuration file.

Any keys that are in the migrated configuration file are replaced by ASCII text. For example, a preshared key for IKE policy authentication in the migrated configuration file contains the following ASCII text: "Key MUST be changed to become valid." To change the preshared key, open the migrated configuration file in a text editor, and replace the ASCII text with the actual preshared key. Be sure to replace the ASCII text for all keys with the actual keys and save the migrated configuration file. The keys are encrypted when you upload the migrated configuration file to the router.

You are now ready to rename and upload the migrated configuration file to the router. For more information, see "Renaming and Uploading the New JUNOS Enhanced Services Configuration File" on page 23.

Chapter 7

Downgrading JUNOS Enhanced Services to JUNOS Software

When you install the JUNOS Enhanced Services software, the router creates a backup image of the software that was previously installed, as well as installs the requested software.

If you migrated JUNOS software to JUNOS Enhanced Services software, you can downgrade the software by using the backup image of the software that was previously installed, which is saved on the router. If you revert to the previous image, this backup image is used, and the image of the running software is deleted. With this method, you can downgrade to only the software release that was installed on the router before the current release.

If the software backup image that was previously installed does not exist on the router, use the procedures in "Installing JUNOS Enhanced Services Software with the CLI" on page 35 and specify a JUNOS software image as the source image to be upgraded.

This chapter contains the following sections:

Backing Up and Replacing the JUNOS Enhanced Services Configuration

To back up and replace the JUNOS Enhanced Services configuration file;

1. Use the start shell operational command to start a shell session.
2. Use the su UNIX command to switch to a user with superuser privileges:

   ```
   % su
   root@host%
   ```

3. At the shell prompt, make a backup file of the JUNOS Enhanced Services configuration file (/config/juniper.conf.gz):

   % **cp /config/juniper.conf.gz** */path*/**juniper.conf.junos-es.gz**

   Replace */path* with the absolute path to which you want to store the backup file.

4. Replace the JUNOS Enhanced Services configuration file with the JUNOS configuration file that you created in "Backing Up the JUNOS Configuration File" on page 22:

   root@host% **cp** */path*/**juniper.conf.junos.gz /config/juniper.conf.gz**

   Replace */path* with the absolute path to the JUNOS configuration file.

5. Return to the shell prompt by using the exit command:

   root@host% **exit**
   %

6. Enter the exit command to return to operational mode in the CLI:

   % **exit**
   user@host>

After backing up and replacing the JUNOS Enhanced Services configuration file, verify whether a backup software image exists on the router, as described in "Verifying Whether the Backup Software Image Exists on the Router" on page 44.

Verifying Whether the Backup Software Image Exists on the Router

You can verify whether the backup software image is available on the router by using the J-Web interface or the CLI:

- "Verifying the Backup Software Image with the J-Web Interface" on page 44
- "Verifying the Backup Software Image with the CLI" on page 45

Verifying the Backup Software Image with the J-Web Interface

To verify whether the backup software image exists on the router:

1. In the J-Web interface, select **Manage > Files**.
2. In the Delete Backup JUNOS Package section, verify that a backup software image is available and whether it is the release to which you want to downgrade.

3. Do one of the following:

   - If a backup software image is available, you can revert to JUNOS software by using the procedure described in "Reverting to JUNOS Software Using the Backup Software Image" on page 45 or in "Reverting to JUNOS Software by Installing the Software Image" on page 47.

   - If no backup software image is available, see "Reverting to JUNOS Software by Installing the Software Image" on page 47.

Verifying the Backup Software Image with the CLI

To verify whether the backup software image exists on the router:

1. From operational mode in the CLI, enter the following command:

   user@host> **file list /cf/packages**

   ```
   /cf/packages:
   junos@ -> junos-8.5R1.8-domestic
   junos-8.5R1.8-domestic
   junos-8.5R1.8-domestic.md5
   junos-8.5R1.8-domestic.sha1
   junos.old@ -> junos-8.4R1.3-domestic
   mnt/
   ```

2. Verify that junos.old@ links to the appropriate JUNOS software image to which you want to downgrade.

3. Do one of the following:

   - If a backup software image is available, you can revert to JUNOS software by using the procedure described in "Reverting to JUNOS Software Using the Backup Software Image" on page 45 or in "Reverting to JUNOS Software by Installing the Software Image" on page 47.

   - If no backup software image is available, see "Reverting to JUNOS Software by Installing the Software Image" on page 47.

Reverting to JUNOS Software Using the Backup Software Image

If the backup software image is available on the router, you can revert to JUNOS software with the J-Web interface or with the request system software rollback command in the CLI. For the changes to take effect, you must reboot the router. If the backup software image is not available, see "Reverting to JUNOS Software by Installing the Software Image" on page 47.

This section contains the following topics:

Reverting to JUNOS Software with the J-Web Interface

To revert to JUNOS software with the J-Web interface:

1. If you have not already created a backup of the JUNOS Enhanced Services configuration file and replaced it with the backup of the JUNOS configuration file, see "Backing Up and Replacing the JUNOS Enhanced Services Configuration" on page 43.

2. In the J-Web interface, select **Manage > Software > Downgrade**. The image of the previous software version is displayed on this page.

NOTE: After you perform this operation, you cannot undo it.

3. Select **Downgrade** to downgrade to the previous version of the software or **Cancel** to cancel the downgrade process.

4. When the downgrade process is complete, for the new software to take effect, select **Manage > Reboot** from the J-Web interface to reboot the router.

After you downgrade the software, the previous release is loaded, and you cannot reload the running version of software again. To downgrade to an earlier version of software, follow the procedure for upgrading, using the JUNOS software image labeled with the appropriate release.

Reverting to JUNOS Software with the CLI

To revert to JUNOS software with the CLI:

1. If you have not already created a backup of the JUNOS Enhanced Services configuration file and replaced it with the backup of the JUNOS configuration file, see "Backing Up and Replacing the JUNOS Enhanced Services Configuration" on page 43.

2. Enter the request system software rollback command to return to the previous JUNOS software version:

   user@host> **request system software rollback**

   The previous JUNOS software version is now ready to become active when you next reboot the router.

3. Reboot the router:

   user@host> **request system reboot**

   The router is now running JUNOS software.

Reverting to JUNOS Software by Installing the Software Image

If you do not have a backup software image on the router, you can revert back to JUNOS software on the Services Router by using the request system software add operational command, as described in "Installing JUNOS Enhanced Services Software with the CLI" on page 35.

To revert to JUNOS software from JUNOS Enhanced Services software by installing the software image:

1. If you have not already created a backup of the JUNOS Enhanced Services configuration file and replaced it with the backup of the JUNOS configuration file, see "Backing Up and Replacing the JUNOS Enhanced Services Configuration" on page 43.

2. Follow the instructions in "Installing JUNOS Enhanced Services Software with the CLI" on page 35. Be sure to use the JUNOS software image to which you want to downgrade.

The router is now running JUNOS software.