

Junos[®] OS

FIPS Evaluated Configuration Guide for EX4300 Devices

Published
2021-03-14

Release
19.4R1

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

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

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

Junos[®] OS FIPS Evaluated Configuration Guide for EX4300 Devices

19.4R1

Copyright © 2021 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <https://support.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About the Documentation | v

Documentation and Release Notes | v

Documentation Conventions | v

Documentation Feedback | viii

Requesting Technical Support | viii

Self-Help Online Tools and Resources | ix

Creating a Service Request with JTAC | ix

1

Overview

Understanding Junos OS in FIPS Mode | 11

About the Cryptographic Boundary on Your EX Series Switch | 11

How FIPS Mode Differs from Non-FIPS Mode | 12

Validated Version of Junos OS in FIPS Mode | 12

Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms | 13

FIPS Terminology | 13

Supported Cryptographic Algorithms | 14

Identifying Secure Product Delivery | 16

Understanding Management Interfaces | 17

2

Configuring Roles and Authentication Methods

Understanding Roles and Services for Junos OS in FIPS Mode | 19

Crypto Officer Role and Responsibilities | 19

FIPS User Role and Responsibilities | 20

What Is Expected of All FIPS Users | 20

Understanding the Operational Environment for Junos OS in FIPS Mode | 21

Hardware Environment for Junos OS in FIPS Mode | 22

Software Environment for Junos OS in FIPS Mode | 22

Critical Security Parameters | 23

Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode | 26

Downloading Software Packages from Juniper Networks | 27

Installing Software on EX Series devices with a Single Routing Engine | 28

Understanding Zeroization to Clear System Data for FIPS Mode | 32

Why Zeroize? | 32

When to Zeroize? | 33

Zeroizing the System | 33

Enabling FIPS Mode | 34

Configuring Crypto Officer and FIPS User Identification and Access | 36

Configuring Crypto Officer Login Access | 36

Configuring FIPS User Login Access | 38

3

Performing Self-Tests on a Device

Understanding FIPS Self-Tests | 41

4

Operational Commands

request system zeroize | 45

About the Documentation

IN THIS SECTION

- Documentation and Release Notes | v
- Documentation Conventions | v
- Documentation Feedback | viii
- Requesting Technical Support | viii

Use this guide to operate the EX4300 device in Federal Information Processing Standards (FIPS) 140-2 Level 1 environment. FIPS 140-2 defines security levels for hardware and software that perform cryptographic functions.

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <https://www.juniper.net/documentation/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <https://www.juniper.net/books>.

Documentation Conventions

Table 1 on page vi defines notice icons used in this guide.

Table 1: Notice Icons







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

Table 2 on page vi defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

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

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i> >;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

GUI Conventions

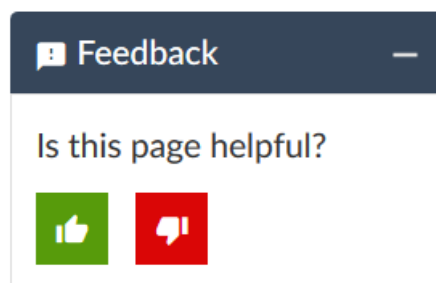
Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are

covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

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

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net>

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

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://myjuniper.juniper.net>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <https://support.juniper.net/support/requesting-support/>.

1

CHAPTER

Overview

Understanding Junos OS in FIPS Mode | 11

Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms | 13

Identifying Secure Product Delivery | 16

Understanding Management Interfaces | 17

Understanding Junos OS in FIPS Mode

IN THIS SECTION

- [About the Cryptographic Boundary on Your EX Series Switch | 11](#)
- [How FIPS Mode Differs from Non-FIPS Mode | 12](#)
- [Validated Version of Junos OS in FIPS Mode | 12](#)

Federal Information Processing Standards (FIPS) 140-2 defines security levels for hardware and software that perform cryptographic functions. By meeting the applicable overall requirements within the FIPS standard, Juniper Networks EX4300-48MP Series switches running the Juniper Networks Junos operating system (Junos OS) in *FIPS mode* comply with the FIPS 140-2 Level 1 standard.

Operating EX Series switches in a FIPS 140-2 Level 1 environment requires enabling and configuring FIPS mode on the switches from the Junos OS CLI.

The *Crypto Officer* enables FIPS mode in Junos OS and sets up keys and passwords for the system and other *FIPS users* who can view the configuration.

For regulatory compliance information about Common Criteria, and FIPS for Juniper Networks products, see the [Juniper Networks Compliance Advisor](#).

About the Cryptographic Boundary on Your EX Series Switch

FIPS 140-2 compliance requires a defined *cryptographic boundary* around each *cryptographic module* on a switch. Junos OS in FIPS mode prevents the cryptographic module from executing any software that is not part of the FIPS-certified distribution, and allows only FIPS-approved cryptographic algorithms to be used. No critical security parameters (CSPs), such as passwords and keys, can cross the cryptographic boundary of the module in unencrypted format.

For the Juniper Networks EX switches that are certified at FIPS-140-2 Level 1, the cryptographic boundary of the module is determined by the chassis type. For a list of FIPS-certified switches and the cryptographic boundary of each switch, see [Table 3 on page 12](#).

Table 3: Cryptographic Boundaries on FIPS-Certified EX Series Switches

Switch	Chassis Type	Cryptographic Boundary
EX4300-48MP switch	Fixed configuration	Switch case



CAUTION: Virtual Chassis features are not supported in FIPS mode. Do not configure a Virtual Chassis in FIPS mode.

How FIPS Mode Differs from Non-FIPS Mode

Unlike Junos OS in non-FIPS mode, Junos OS in FIPS mode is a *non-modifiable operational environment*. In addition, Junos OS in FIPS mode differs in the following ways from Junos OS in non-FIPS mode:

- Self-tests of all cryptographic algorithms are performed at startup.
- Self-tests of random number and key generation are performed continuously.
- Weak cryptographic algorithms such as Data Encryption Standard (DES) and Message Digest 5 (MD5) are disabled.
- Weak or unencrypted management connections must not be configured.
- Passwords must be encrypted with strong one-way algorithms that do not permit decryption.
- Administrator passwords must be at least 10 characters long.

Validated Version of Junos OS in FIPS Mode

To determine whether a Junos OS release is NIST-validated, see the software download page on the Juniper Networks Web site (<https://www.juniper.net/>) or the National Institute of Standards and Technology site.

RELATED DOCUMENTATION

Identifying Secure Product Delivery | 16

Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms

IN THIS SECTION

- [FIPS Terminology | 13](#)
- [Supported Cryptographic Algorithms | 14](#)

Use the definitions of FIPS terms and supported algorithms to help you understand Junos OS in FIPS mode.

FIPS Terminology

Critical security parameter (CSP)—Security-related information—for example, secret and private cryptographic keys and authentication data such as passwords and personal identification numbers (PINs)—whose disclosure or modification can compromise the security of a cryptographic module or the information it protects. For details, see [“Understanding the Operational Environment for Junos OS in FIPS Mode” on page 21](#).

Cryptographic module—The set of hardware, software, and firmware that implements approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary. For fixed-configuration switches, the cryptographic module is the switch case. For modular switches, the cryptographic module is the Routing Engine.

Crypto Officer—Person with appropriate permissions who is responsible for securely enabling, configuring, monitoring, and maintaining Junos OS in FIPS mode on a switch. For details, see [“Understanding Roles and Services for Junos OS in FIPS Mode” on page 19](#).

FIPS—Federal Information Processing Standards. FIPS 140-2 specifies requirements for security and cryptographic modules. Junos OS in FIPS mode complies with FIPS 140-2 Level 1.

FIPS maintenance role—The role the Crypto Officer assumes to perform physical maintenance or logical maintenance services such as hardware or software diagnostics. For FIPS 140-2 compliance, the Crypto Officer zeroizes the Routing Engine on entry to and exit from the FIPS maintenance role to erase all plain-text secret and private keys and unprotected CSPs.

NOTE: The FIPS maintenance role is not supported on Junos OS in FIPS mode.

KATs—Known answer tests. System self-tests that validate the output of cryptographic algorithms approved for FIPS and test the integrity of some Junos OS modules. For details, see [“Understanding FIPS Self-Tests” on page 41](#).

SSH—A protocol that uses strong authentication and encryption for remote access across a nonsecure network. SSH provides remote login, remote program execution, file copy, and other functions. It is intended as a secure replacement for **rlogin**, **rsh**, and **rcp** in a UNIX environment. To secure the information sent over administrative connections, use SSHv2 for CLI configuration. In Junos OS, SSHv2 is enabled by default, and SSHv1, which is not considered secure, is disabled.

Zeroization—Erasure of all CSPs and other user-created data on a switch before its operation as a FIPS cryptographic module—or in preparation for repurposing the switch for non-FIPS operation. The Crypto Officer can zeroize the system with a CLI operational command. For details, see [“Understanding Zeroization to Clear System Data for FIPS Mode” on page 32](#).

Supported Cryptographic Algorithms

[Table 4 on page 14](#) summarizes the high level protocol algorithm support.

Table 4: Protocols Allowed in FIPS Mode

Protocol	Key Exchange	Authentication	Cipher	Integrity
SSHv2	<ul style="list-style-type: none"> • ECDH-sha2-nistp256 • ECDH-sha2-nistp384 • ECDH-sha2-nistp521 	Host (module): <ul style="list-style-type: none"> • ECDSA P-256 • SSH-RSA Client (user): <ul style="list-style-type: none"> • ECDSA P-256 • ECDSA P-384 • ECDSA P-521 • SSH-RSA 	<ul style="list-style-type: none"> • 3 Key Triple-DES CBC • AES CTR 128 • AES CTR 192 • AES CTR 256 • AES CBC 128 • AES CBC 192 • AES CBC 256 	<ul style="list-style-type: none"> • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-512

Each implementation of an algorithm is checked by a series of known answer test (KAT) self-tests. Any self-test failure results in a FIPS error state.

The following cryptographic algorithms are supported in FIPS mode. Symmetric methods use the same key for encryption and decryption, while asymmetric methods use different keys for encryption and decryption.

AES—The Advanced Encryption Standard (AES), defined in FIPS PUB 197. The AES algorithm uses keys of 128, 192, or 256 bits to encrypt and decrypt data in blocks of 128 bits.

Diffie-Hellman—A method of key exchange across a nonsecure environment (such as the Internet). The Diffie-Hellman algorithm negotiates a session key without sending the key itself across the network by allowing each party to pick a partial key independently and send part of that key to the other. Each side then calculates a common key value. This is a symmetrical method—keys are typically used only for a short time, discarded, and regenerated.

ECDH—Elliptic Curve Diffie-Hellman. A variant of the Diffie-Hellman key exchange algorithm that uses cryptography based on the algebraic structure of elliptic curves over finite fields. ECDH allows two parties, each having an elliptic curve public-private key pair, to establish a shared secret over an insecure channel. The shared secret can be used either as a key or to derive another key for encrypting subsequent communications using a symmetric key cipher.

ECDSA—Elliptic Curve Digital Signature Algorithm. A variant of the Digital Signature Algorithm (DSA) that uses cryptography based on the algebraic structure of elliptic curves over finite fields. The bit size of the elliptic curve determines the difficulty of decrypting the key. The public key believed to be needed for ECDSA is about twice the size of the security strength, in bits.

HMAC—Defined as “Keyed-Hashing for Message Authentication” in RFC 2104, HMAC combines hashing algorithms with cryptographic keys for message authentication.

SHA-256, SHA-384, and SHA-512—Secure hash algorithms (SHA) belonging to the SHA-2 standard defined in FIPS PUB 180-2. Developed by NIST, SHA-256 produces a 256-bit hash digest, SHA-384 produces a 384-bit hash digest, and SHA-512 produces a 512-bit hash digest.

3DES (3des-cbc)—Encryption standard based on the original Data Encryption Standard (DES) from the 1970s that used a 56-bit key and was cracked in 1997. The more secure 3DES is DES enhanced with three multiple stages and effective key lengths of about 112 bits. For Junos OS in FIPS mode, 3DES is implemented with cipher block chaining (CBC).

RELATED DOCUMENTATION

[Understanding FIPS Self-Tests | 41](#)

[Understanding Zeroization to Clear System Data for FIPS Mode | 32](#)

Identifying Secure Product Delivery

There are several mechanisms provided in the delivery process to ensure that a customer receives a product that has not been tampered with. The customer should perform the following checks upon receipt of a device to verify the integrity of the platform.

- Shipping label—Ensure that the shipping label correctly identifies the correct customer name and address as well as the device.
- Outside packaging—Inspect the outside shipping box and tape. Ensure that the shipping tape has not been cut or otherwise compromised. Ensure that the box has not been cut or damaged to allow access to the device.
- Inside packaging—Inspect the plastic bag and seal. Ensure that the bag is not cut or removed. Ensure that the seal remains intact.

If the customer identifies a problem during the inspection, he or she should immediately contact the supplier. Provide the order number, tracking number, and a description of the identified problem to the supplier.

Additionally, there are several checks that can be performed to ensure that the customer has received a box sent by Juniper Networks and not a different company masquerading as Juniper Networks. The customer should perform the following checks upon receipt of a device to verify the authenticity of the device:

- Verify that the device was ordered using a purchase order. Juniper Networks devices are never shipped without a purchase order.
- When a device is shipped, a shipment notification is sent to the e-mail address provided by the customer when the order is taken. Verify that this e-mail notification was received. Verify that the e-mail contains the following information:
 - Purchase order number
 - Juniper Networks order number used to track the shipment
 - Carrier tracking number used to track the shipment
 - List of items shipped including serial numbers
 - Address and contacts of both the supplier and the customer
- Verify that the shipment was initiated by Juniper Networks. To verify that a shipment was initiated by Juniper Networks, you should perform the following tasks:
 - Compare the carrier tracking number of the Juniper Networks order number listed in the Juniper Networks shipping notification with the tracking number on the package received.

- Log on to the Juniper Networks online customer support portal at <https://www.juniper.net/customers/csc/management> to view the order status. Compare the carrier tracking number or the Juniper Networks order number listed in the Juniper Networks shipment notification with the tracking number on the package received.

Understanding Management Interfaces

The following management interfaces can be used in the evaluated configuration:

- Local Management Interfaces—The RJ-45 console port on the rear panel of a device is configured as RS-232 data terminal equipment (DTE). You can use the command-line interface (CLI) over this port to configure the device from a terminal.
- Remote Management Protocols—The device can be remotely managed over any Ethernet interface. SSHv2 is the only permitted remote management protocol that can be used in the evaluated configuration. The remote management protocols J-Web and Telnet are not available for use on the device.

2

CHAPTER

Configuring Roles and Authentication Methods

Understanding Roles and Services for Junos OS in FIPS Mode | 19

Understanding the Operational Environment for Junos OS in FIPS Mode | 21

Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode | 26

Downloading Software Packages from Juniper Networks | 27

Installing Software on EX Series devices with a Single Routing Engine | 28

Understanding Zeroization to Clear System Data for FIPS Mode | 32

Zeroizing the System | 33

Enabling FIPS Mode | 34

Configuring Crypto Officer and FIPS User Identification and Access | 36

Understanding Roles and Services for Junos OS in FIPS Mode

IN THIS SECTION

- [Crypto Officer Role and Responsibilities | 19](#)
- [FIPS User Role and Responsibilities | 20](#)
- [What Is Expected of All FIPS Users | 20](#)

The Juniper Networks Junos operating system (Junos OS) running in non-FIPS mode allows a wide range of capabilities for users, and authentication is identity-based. In contrast, the FIPS 140-2 standard defines two user roles: *Crypto Officer* and *FIPS user*. These roles are defined in terms of Junos OS user capabilities.

All other user types defined for Junos OS in FIPS mode (read-only, administrative user, and so on) must fall into one of the two categories: Crypto Officer or FIPS user. For this reason, user authentication in Junos is identity based with role based authorization.

Crypto Officer perform all FIPS-mode-related configuration tasks and issue all statements and commands for Junos OS in FIPS mode. Crypto Officer and FIPS user configurations must follow the guidelines for Junos OS in FIPS mode.

Crypto Officer Role and Responsibilities

The Crypto Officer is the person responsible for enabling, configuring, monitoring, and maintaining Junos OS in FIPS mode on a switch. The Crypto Officer securely installs Junos OS on the switch, enables FIPS mode, establishes keys and passwords for other users and software modules, and initializes the switch before network connection.

BEST PRACTICE: We recommend that the Crypto Officer administer the system in a secure manner by keeping passwords secure.

The permissions that distinguish the Crypto Officer from other FIPS users are **secret**, **security**, **maintenance**, and **control**. For FIPS compliance, assign the Crypto Officer to a login class that contains all of these

permissions. A user with the Junos OS maintenance permission can read files containing critical security parameters (CSPs).

NOTE: Junos OS in FIPS mode does not support the *FIPS 140-2 maintenance role*, which is different from the Junos OS maintenance permission.

Among the tasks related to Junos OS in FIPS mode, the Crypto Officer is expected to:

- Set the initial root password. The length of the password should be at least 10 characters.
- Reset user passwords for FIPS-approved algorithms during upgrades from Junos OS.
- Examine log and audit files for events of interest.
- Erase user-generated files, keys, and data by zeroizing the switch

FIPS User Role and Responsibilities

All FIPS users, including the Crypto Officer, can view the configuration. Only the user assigned as the Crypto Officer can modify the configuration.

The permissions that distinguish Crypto Officer from other FIPS users are **secret**, **security**, **maintenance**, and **control**. For FIPS compliance, assign the FIPS user to a class that contains *none* of these permissions.

FIPS user can view status output but cannot reboot or zeroize the switch.

What Is Expected of All FIPS Users

All FIPS users, including the Crypto Officer, must observe security guidelines at all times.

All FIPS users must:

- Keep all passwords confidential.
- Store switches and documentation in a secure area.
- Deploy switches in secure areas.
- Check audit files periodically.

- Conform to all other FIPS 140-2 security rules.
- Follow these guidelines:
 - Users are trusted.
 - Users abide by all security guidelines.
 - Users do not deliberately compromise security.
 - Users behave responsibly at all times.

RELATED DOCUMENTATION

[Zeroizing the System | 33](#)

[Configuring Crypto Officer and FIPS User Identification and Access | 36](#)

Understanding the Operational Environment for Junos OS in FIPS Mode

IN THIS SECTION

- [Hardware Environment for Junos OS in FIPS Mode | 22](#)
- [Software Environment for Junos OS in FIPS Mode | 22](#)
- [Critical Security Parameters | 23](#)

EX Series switches running the Junos operating system (Junos OS) in FIPS mode forms a special type of hardware and software operational environment that is different from the environment of a switch in non-FIPS mode:

Hardware Environment for Junos OS in FIPS Mode

Junos OS in FIPS mode establishes a cryptographic boundary in the switch that no critical security parameters (CSPs) can cross using plain text. Each hardware component of the switch that requires a cryptographic boundary for FIPS 140-2 compliance is a separate cryptographic module.

For more information about the cryptographic boundary on your switch, see [“Understanding Junos OS in FIPS Mode” on page 11](#).

Cryptographic methods are not a substitute for physical security. The hardware must be located in a secure physical environment. Users of all types must not reveal keys or passwords, or allow written records or notes to be seen by unauthorized personnel.

Software Environment for Junos OS in FIPS Mode

EX Series switches running Junos OS in FIPS mode forms a special type of non-modifiable operational environment. To achieve this environment on the switch, the system prevents the execution of any binary file that was not part of the certified Junos OS distribution. When a switch is in FIPS mode, it can run only Junos OS.

FIPS mode on EX4300-48MP Series switches are available starting with Junos OS Release 19.4R1. The Junos OS in FIPS mode software environment is established after the Crypto Officer successfully enables FIPS mode on EX Series switches. The Junos OS Release 19.4R1 image that includes fips-mode package is available on the Juniper Networks website and can be installed on EX4300-48MP Series switches. See [“Downloading Software Packages from Juniper Networks” on page 27](#) for more information on image names.

For FIPS 140-2 compliance, we recommend deleting all user-created files and data from (zeroizing) the system before enabling FIPS mode.

Enabling FIPS mode disables many of the usual Junos OS protocols and services. In particular, you cannot configure the following services in Junos OS in FIPS mode:

- finger
- ftp
- rlogin
- telnet
- tftp
- xnm-clear-text

Attempts to configure these services, or load configurations with these services configured, result in a configuration syntax error. You can use only SSHv2 as a remote access service.

All passwords established for users after upgrading to Junos OS in FIPS mode must conform to Junos OS in FIPS mode specifications. Passwords must be between 10 and 20 characters in length and require the use of at least three of the five defined character sets (uppercase and lowercase letters, digits, punctuation marks, and keyboard characters, such as % and &, not included in the other four categories). Attempts to configure passwords that do not conform to these rules result in an error. All passwords and keys used to authenticate peers must be at least 10 characters in length, and in some cases the length must match the digest size.

NOTE: Do not attach the switch to a network until you, the Crypto Officer, complete the configuration from the local console connection.

Critical Security Parameters

Critical security parameters (CSPs) are security-related information such as cryptographic keys and passwords that can compromise the security of the cryptographic module or the security of the information protected by the module if they are disclosed or modified.

Zeroization of the system erases all traces of CSPs in preparation for operating the switch as a cryptographic module.

Table 5 on page 23 lists CSPs on switches running Junos OS.

Table 5: Critical Security Parameters

CSP	Description	Zeroization Method	Use
SSHv2 private host key	ECDSA / RSA key used to identify the host, generated the first time SSH is configured.	Zeroize command.	Used to identify the host.

Table 5: Critical Security Parameters (continued)

CSP	Description	Zeroization Method	Use
SSHv2 session key	<p>Session key used with SSHv2. and as a Diffie-Hellman private key.</p> <p>Encryption: 3DES, AES-128, AES-192, and AES-256.</p> <p>MACs: HMAC-SHA-1, HMAC-SHA-2-256, and HMAC-SHA2-512.</p> <p>Key exchange: ECDH-sha2-nistp256, ECDH-sha2-nistp384, and ECDH-sha2-nistp521</p>	Power cycle and terminate session.	Symmetric key used to encrypt data between host and client.
User authentication key	Hash of the user's password: SHA-256, SHA-512.	Zeroize command.	Used to authenticate a user to the cryptographic module.
Crypto Officer authentication key	Hash of the Crypto Officer's password: SHA-256, SHA-512.	Zeroize command.	Used to authenticate the Crypto Officer to the cryptographic module.
HMAC DRBG seed	Seed for deterministic random bit generator (DRBG).	Seed is not stored by the cryptographic module.	Used for seeding DRBG.
HMAC DRBG V value	The value (V) of output block length (outlen) in bits, which is updated each time another outlen bits of output are produced.	Power cycle.	A critical value of the internal state of DRBG.
HMAC DRBG key value	The current value of the outlen-bit key, which is updated at least once each time that the DRBG mechanism generates pseudorandom bits.	Power cycle.	A critical value of the internal state of DRBG.
NDRNG entropy	Used as entropy input string to the HMAC DRBG.	Power cycle.	A critical value of the internal state of DRBG.

In Junos OS in FIPS mode, all CSPs must enter and leave the cryptographic module in encrypted form. Any CSP encrypted with a non-approved algorithm is considered plain text by FIPS. .

BEST PRACTICE: For FIPS compliance, configure the switch over SSH connections because they are encrypted connections.

Local passwords are hashed with the secure hash algorithm SHA-256, or SHA-512. Password recovery is not possible in Junos OS in FIPS mode. Junos OS in FIPS mode cannot boot into single-user mode without the correct root password.

RELATED DOCUMENTATION

[Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode | 26](#)

[Understanding Zeroization to Clear System Data for FIPS Mode | 32](#)

Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode

All passwords established for users by the Crypto Officer must conform to the following Junos OS in FIPS mode requirements. Attempts to configure passwords that do not conform to the following specifications result in an error.

- **Length.** Passwords must contain between 10 and 20 characters.
- **Character set requirements.** Passwords must contain at least three of the following five defined character sets:
 - Uppercase letters
 - Lowercase letters
 - Digits
 - Punctuation marks
 - Keyboard characters not included in the other four sets—such as the percent sign (%) and the ampersand (&)
- **Authentication requirements.** All passwords and keys used to authenticate peers must contain at least 10 characters, and in some cases the number of characters must match the digest size.
- **Password encryption.** To change the default encryption method (SHA512) include the format statement at the `[edit system login password]` hierarchy level.

Guidelines for strong passwords. Strong, reusable passwords can be based on letters from a favorite phrase or word and then concatenated with other unrelated words, along with added digits and punctuation. In general, a strong password is:

- Easy to remember so that users are not tempted to write it down.
- Made up of mixed alphanumeric characters and punctuation. For FIPS compliance include at least one change of case, one or more digits, and one or more punctuation marks.
- Changed periodically.
- Not divulged to anyone.

Characteristics of weak passwords. Do not use the following weak passwords:

- Words that might be found in or exist as a permuted form in a system files such as `/etc/passwd`.
- The hostname of the system (always a first guess).

- Any word or phrase that appears in a dictionary or other well-known source, including dictionaries and thesauruses in languages other than English; works by classical or popular writers; or common words and phrases from sports, sayings, movies or television shows.
- Permutations on any of the above—for example, a dictionary word with letters replaced with digits (**root**) or with digits added to the end.
- Any machine-generated password. Algorithms reduce the search space of password-guessing programs and so must not be used.

RELATED DOCUMENTATION

| [Understanding the Operational Environment for Junos OS in FIPS Mode](#) | 21

Downloading Software Packages from Juniper Networks

You can download the following Junos OS software packages for EX Series switches from the Juniper Networks website:

- Junos OS for EX Series switches, Release 19.4R1

Before you begin to download the software, ensure that you have a Juniper Networks Web account and a valid support contract. To obtain an account, complete the registration form at the Juniper Networks website: <https://www.juniper.net/registration/Register.jsp>.

NOTE: For EX4300-48MP, FIPS is supported only on non-flex image. You have to upgrade to the non-flex image to enable FIPS mode. Also, the Junos OS Release 19.4R1 image **jinstall-host-ex-4300mp-x86-64-19.4R1-secure.tgz** that includes FIPS package is available on the Juniper Networks website and the same image can be installed on EX4300-48MP switches.

To download software packages from Juniper Networks:

1. Using a Web browser, follow the links to the download URL on the Juniper Networks webpage.
 - To download the software image for EX4300-48MP, click the <https://support.juniper.net/support/downloads/> link.
2. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. Select the software package that you want to download. You can select software that supports a specific platform or technology:
 - For Junos OS package, ensure that the name contains the correct switch name and the Junos OS release that is FIPS-certified on the switches.

The software image name for EX4300-48MP is **jinstall-host-ex-4300mp-x86-64-19.4R1-secure.tgz**.
4. Download the software to a local host or to an internal software distribution site.
5. Install the Junos OS. See [“Installing Software on EX Series devices with a Single Routing Engine” on page 28](#).

RELATED DOCUMENTATION

| [Installing Software on EX Series devices with a Single Routing Engine](#) | 28

Installing Software on EX Series devices with a Single Routing Engine

You can use this procedure to upgrade Junos OS on switch with a single Routing Engine.

To install software upgrades on a switch with a single Routing Engine:

1. Download the software package as described in [“Downloading Software Packages from Juniper Networks” on page 27](#).
2. If you have not already done so, connect to the console port on the switch from your management device, and log in to the Junos OS CLI. (For instructions, see [Configuring Junos OS on the EX4300](#).)

3. (Optional) Back up the current software configuration to a second storage option. See the [Junos OS Installation and Upgrade Guide](#) for instructions on performing this task.
4. (Optional) Copy the software package to the switch. We recommend that you use FTP to copy the file to the `/var/tmp/` directory.

This step is optional because Junos OS can also be upgraded when the software image is stored at a remote location. These instructions describe the software upgrade process for both scenarios.

5. Install the new package on the switch:

```
user@switch> request system software add <package>
```

Replace **package** with one of the following paths:

- For a software package in a local directory on the switch, use `/var/tmp/package.tgz`.
- For a software package on a remote server, use one of the following paths, replacing *package* with the software package name—for example, `jinstall-host-ex-4300mp-x86-64-19.4R1.1-secure.tgz`.
 - `ftp://hostname/pathname/package.tgz`
 - `http://hostname/pathname/package.tgz`

NOTE: If you need to terminate the installation, do not reboot your switch; instead, finish the installation and then issue the `request system software delete package.tgz` command, where *package.tgz* is, for example, `jinstall-host-ex-4300mp-x86-64-19.4R1.1-secure.tgz`. This is your last chance to stop the installation.

6. Reboot the switch to load the installation and start the new software:

```
user@switch> request system reboot
```

7. After the reboot has completed, log in and use the `show version` command to verify that the new version of the software is successfully installed.

```
user@switch:> show version local
Hostname: hostname
Model: ex4300-48mp
JUNOS OS Kernel 64-bit [20191115.14c2ad5_builder_stable_11]
JUNOS OS libs [20191115.14c2ad5_builder_stable_11]
JUNOS OS runtime [20191115.14c2ad5_builder_stable_11]
```

```

JUNOS OS time zone information [20191115.14c2ad5_builder_stable_11]
JUNOS OS libs compat32 [20191115.14c2ad5_builder_stable_11]
JUNOS OS 32-bit compatibility [20191115.14c2ad5_builder_stable_11]
JUNOS py extensions2 [20191119.064603_builder_junos_194_r1]
JUNOS py extensions [20191119.064603_builder_junos_194_r1]
JUNOS py base2 [20191119.064603_builder_junos_194_r1]
JUNOS py base [20191119.064603_builder_junos_194_r1]
JUNOS OS vmguest [20191115.14c2ad5_builder_stable_11]
JUNOS OS crypto [20191115.14c2ad5_builder_stable_11]
JUNOS network stack and utilities [20191119.064603_builder_junos_194_r1]
JUNOS libs [20191119.064603_builder_junos_194_r1]
JUNOS libs compat32 [20191119.064603_builder_junos_194_r1]
JUNOS runtime [20191119.064603_builder_junos_194_r1]
JUNOS na telemetry [19.4R1.1]
JUNOS Web Management Platform Package [20191119.064603_builder_junos_194_r1]
JUNOS qfx runtime [20191119.064603_builder_junos_194_r1]
JUNOS common platform support [20191119.064603_builder_junos_194_r1]
JUNOS qfx platform support [20191119.064603_builder_junos_194_r1]
JUNOS Openconfig [19.4R1.1]
JUNOS dcp network modules [20191119.064603_builder_junos_194_r1]
JUNOS modules [20191119.064603_builder_junos_194_r1]
JUNOS qfx modules [20191119.064603_builder_junos_194_r1]
JUNOS qfx Data Plane Crypto Support [20191119.064603_builder_junos_194_r1]
JUNOS daemons [20191119.064603_builder_junos_194_r1]
JUNOS qfx daemons [20191119.064603_builder_junos_194_r1]
JUNOS Services URL Filter package [20191119.064603_builder_junos_194_r1]
JUNOS Services TLB Service PIC package [20191119.064603_builder_junos_194_r1]
JUNOS Services Telemetry [20191119.064603_builder_junos_194_r1]
JUNOS Services TCP-LOG [20191119.064603_builder_junos_194_r1]
JUNOS Services SSL [20191119.064603_builder_junos_194_r1]
JUNOS Services SOFTWARE [20191119.064603_builder_junos_194_r1]
JUNOS Services Stateful Firewall [20191119.064603_builder_junos_194_r1]
JUNOS Services RTCOM [20191119.064603_builder_junos_194_r1]
JUNOS Services RPM [20191119.064603_builder_junos_194_r1]
JUNOS Services PCEF package [20191119.064603_builder_junos_194_r1]
JUNOS Services NAT [20191119.064603_builder_junos_194_r1]
JUNOS Services Mobile Subscriber Service Container package
[20191119.064603_builder_junos_194_r1]
JUNOS Services MobileNext Software package [20191119.064603_builder_junos_194_r1]
JUNOS Services Logging Report Framework package
[20191119.064603_builder_junos_194_r1]
JUNOS Services LL-PDF Container package [20191119.064603_builder_junos_194_r1]
JUNOS Services Jflow Container package [20191119.064603_builder_junos_194_r1]
JUNOS Services Deep Packet Inspection package

```

```

[20191119.064603_builder_junos_194_r1]
JUNOS Services IPSec [20191119.064603_builder_junos_194_r1]
JUNOS Services IDS [20191119.064603_builder_junos_194_r1]
JUNOS IDP Services [20191119.064603_builder_junos_194_r1]
JUNOS Services HTTP Content Management package
[20191119.064603_builder_junos_194_r1]
JUNOS Services Crypto [20191119.064603_builder_junos_194_r1]
JUNOS Services Captive Portal and Content Delivery Container package
[20191119.064603_builder_junos_194_r1]
JUNOS Services COS [20191119.064603_builder_junos_194_r1]
JUNOS AppId Services [20191119.064603_builder_junos_194_r1]
JUNOS Services Application Level Gateways [20191119.064603_builder_junos_194_r1]
JUNOS Services AACL Container package [20191119.064603_builder_junos_194_r1]
JUNOS SDN Software Suite [20191119.064603_builder_junos_194_r1]
JUNOS Extension Toolkit [20191119.064603_builder_junos_194_r1]
JUNOS Phone-home [20191119.064603_builder_junos_194_r1]
JUNOS Packet Forwarding Engine Support (DC-PFE)
[20191119.064603_builder_junos_194_r1]
JUNOS Packet Forwarding Engine Support (M/T Common)
[20191119.064603_builder_junos_194_r1]
JUNOS Juniper Malware Removal Tool (JMRT)
[1.0.0+20191119.064603_builder_junos_194_r1]
JUNOS J-Insight [20191119.064603_builder_junos_194_r1]
JUNOS jfirmware [20191119.064603_builder_junos_194_r1]
JUNOS Online Documentation [20191119.064603_builder_junos_194_r1]
JUNOS jail runtime [20191115.14c2ad5_builder_stable_11]
JUNOS FIPS mode utilities [20191119.064603_builder_junos_194_r1]
JUNOS Host Software [3.14.52-rt50-WR7.0.0.9_ovp:3.1.0]
JUNOS Host ex-4300mp control-plane package [19.4R1.1]
JUNOS Host ex-4300mp platform package [19.4R1.1]
JUNOS Host ex-4300mp data-plane package [19.4R1.1]
JUNOS Host ex-4300mp base package [19.4R1.1]

```

RELATED DOCUMENTATION

[Troubleshooting Software Installation](#)

[Understanding Software Installation on EX Series Switches](#)

Understanding Zeroization to Clear System Data for FIPS Mode

IN THIS SECTION

- [Why Zeroize? | 32](#)
- [When to Zeroize? | 33](#)

Zeroization completely erases all configuration information on the Routing Engines, including all plain-text passwords, secrets, and private keys for SSH, local encryption, local authentication.

The Crypto Officer initiates the zeroization process by entering the [request system zeroize](#) operational command from the CLI. Use of this command is restricted to the Crypto Officer.



CAUTION: Perform system zeroization with care. After the zeroization process is complete, no data is left on the Routing Engine. The switch is returned to the factory default state, without any configured users or configuration files.

Zeroization can be time-consuming. Although all configurations are removed in a few seconds, the zeroization process goes on to overwrite all media, which can take considerable time depending on the size of the media.

Why Zeroize?

Your switch is not considered a valid FIPS cryptographic module until all critical security parameters (CSPs) have been entered—or reentered—while the switch is in FIPS mode.

BEST PRACTICE: For FIPS 140-2 compliance, you must zeroize the system to remove sensitive information before disabling FIPS mode on the switch.

When to Zeroize?

As Crypto Officer, perform zeroization in the following situations:

- **Before enabling FIPS mode of operation:** To prepare your switch for operation as a FIPS cryptographic module, perform zeroization before enabling FIPS mode.
- **Before disabling FIPS mode of operation:** To begin repurposing your switch for non-FIPS mode of operation, perform zeroization on the switch.

NOTE: Juniper Networks does not support installing non-FIPS software in a FIPS environment, but doing so might be necessary in certain test environments. Be sure to zeroize the system first.

RELATED DOCUMENTATION

[Zeroizing the System | 33](#)

[Enabling FIPS Mode | 34](#)

Zeroizing the System

To zeroize your switch:



CAUTION: Perform system zeroization with care. After the zeroization process is complete, no data is left on the Routing Engine. The switch is returned to the factory default state, without any configured users or configuration files.

1. Login to the switch with crypto-officer credentials using console connection, and enter

```
crypto-officer@switch> request system zeroize
warning: System will be rebooted and may not boot without configuration
Erase all data, including configuration and log files? [yes,no] (no)
```

2. To initiate the zeroization process, type **yes** at the prompt:

```
warning: System will be rebooted and may not boot without configuration
Erase all data, including configuration and log files? [yes,no] (no)
yes
warning: ipsec-key-management subsystem not running - not needed by configuration.
warning: zeroizing localre
```

The entire operation can take considerable time depending on the size of the media, but all critical security parameters (CSPs) are removed within a few seconds. The physical environment must remain secure until the zeroization process is complete.

RELATED DOCUMENTATION

[Enabling FIPS Mode | 34](#)

[Understanding Zeroization to Clear System Data for FIPS Mode | 32](#)

Enabling FIPS Mode

FIPS mode is not automatically enabled when you install Junos OS on the switch.

As Crypto Officer, you must explicitly enable FIPS mode on the switch by setting the FIPS level to 1 (one), the FIPS 140-2 level at which EX Series switches are certified. A switch on which FIPS mode is not enabled has a FIPS level of 0 (zero).

NOTE: To transition to FIPS mode, passwords must be encrypted with a FIPS-compliant hash algorithm. The encryption format must be SHA-256 or SHA-512. Passwords that do not meet this requirement, such as passwords that are hashed with MD5, must be reconfigured or removed from the configuration before FIPS mode can be enabled.

1. Zeroize the switch to delete all CSPs before entering FIPS mode. See [“Understanding Zeroization to Clear System Data for FIPS Mode” on page 32](#).
2. After the switch comes up in *Amnesiac mode*, login using username **root** and password (**blank**).

```
login: root
Password:
```

```

--- JUNOS 19.4R1.1 Kernel 64-bit  JNPR-11.0-20191115.14c2ad5_buil
root@:~ # cli
root>

```

3. Configure root authentication with password at least 10 characters or more.

```

root@switch> edit
Entering configuration mode
[edit]
root@switch#
[edit]
root@switch# set system root-authentication plain-text-password
New password:
Retype new password:
root@switch# commit
configuration check succeeds
commit complete

```

4. Load configuration onto switch and commit new configuration.
5. Configure Crypto Officer and login with Crypto Officer credentials.
6. Configure chassis boundary fips by running the **set system fips level 1** command followed by the **commit** command.

NOTE: The device might display the following warning to delete older CSPs in loaded configuration- **Encrypted-password must be re-configured to use FIPS compliant hash**

7. After deleting and reconfiguring the CSPs, commit is successful and the switch needs reboot to enter FIPS mode.

```

[edit]
crypto-officer@switch# commit
configuration check succeeds
[edit]
'system'
warning: reboot is required to transition to FIPS level 1
commit complete
[edit]

```

```
crypto-officer@switch# run request system reboot
```

8. After rebooting the switch, FIPS self-tests will run and switch enters FIPS mode.

```
crypto-officer@switch:fips>
```

NOTE: Use “local” keyword for operational commands in FIPS mode. For example, **show version local**, and **show system uptime local**.

Configuring Crypto Officer and FIPS User Identification and Access

IN THIS SECTION

- [Configuring Crypto Officer Login Access | 36](#)
- [Configuring FIPS User Login Access | 38](#)

Crypto Officer perform all configuration tasks for Junos OS in FIPS mode and issue all Junos OS in FIPS mode statements and commands. Crypto Officer and FIPS user configurations must follow Junos OS in FIPS mode guidelines.

Configuring Crypto Officer Login Access

Junos OS in FIPS mode offers a finer granularity of user permissions than those mandated by FIPS 140-2.

For FIPS 140-2 compliance, any FIPS user with the **secret**, **security**, **maintenance**, and **control** permission bits set is a Crypto Officer. In most cases the **super-user** class suffices for the Crypto Officer.

To configure login access for a Crypto Officer:

1. Log in to the switch with the root password if you have not already done so, and enter configuration mode:

```
root@switch> configure
  Entering configuration mode
[edit]
root@switch#
```

2. Name the user “crypto-officer” and assign the Crypto Officer a user ID (for example, **6400**) and a class (for example, **super-user**). When you assign the class, you assign the permissions—for example, **secret**, **security**, **maintenance**, and **control**.

For a list of permissions, see [Understanding Junos OS Access Privilege Levels](#).

```
[edit]
root@switch# set system login user crypto-officer uid 6400 class super-user
```

3. Following the guidelines in “[Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode](#)” on [page 26](#), assign the Crypto Officer a plain-text password for login authentication. Set the password by typing a password after the prompts **New password** and **Retype new password**.

```
[edit]
root@switch# set system login user crypto-officer class super-user authentication plain-text-password
```

4. Optionally, display the configuration:

```
[edit]
root@switch# edit system
[edit system]
root@switch# show
login {
  user crypto-officer {
    uid 6400;
    authentication {
      encrypted-password "<cipher-text>"; ## SECRET-DATA
    }
    class super-user;
  }
}
```

5. If you are finished configuring the switch, commit the configuration and exit:

```
[edit]
root@switch# commit
commit complete
root@switch# exit
root@switch> exit
```

Configuring FIPS User Login Access

A **fips-user** is defined as any FIPS user that does not have the **secret**, **security**, **maintenance**, and **control** permission bits set. In most cases the read-only class suffices for the FIPS User.

As the Crypto Officer you set up FIPS users.

To configure login access for a FIPS user:

1. Log in to the switch with your Crypto Officer password if you have not already done so, and enter configuration mode:

```
crypto-officer@switch> configure
  Entering configuration mode
[edit]
crypto-officer@switch:fips#
```

2. Give the user a username, assign the FIPS user a user ID (for example, **6401**) and a class (for example **read-only**).

For a list of permissions, see [Understanding Junos OS Access Privilege Levels](#).

```
[edit]
crypto-officer@switch# set system login user fips-user1 uid 6401 class read-only
```

3. Following the guidelines in [“Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode” on page 26](#), assign the FIPS a plain-text password for login authentication. Set the password by typing a password after the prompts **New password** and **Retype new password**.

```
[edit]
crypto-officer@switch# set system login user fips-user1 read-only authentication plain-text-password
```

4. Optionally, display the configuration:

```
[edit]
crypto-officer@switch# edit system
[edit system]
crypto-officer@switch# show
login {
  user fips-user1 {
    uid 6401;
    authentication {
      encrypted-password "<cipher-text>"; ## SECRET-DATA
    }
    read-only;
  }
}
```

5. If you are finished configuring the switch, commit the configuration and exit:

```
[edit]
crypto-officer@switch# commit
crypto-officer@switch> exit
```

RELATED DOCUMENTATION

[Understanding Roles and Services for Junos OS in FIPS Mode](#) | 19

3

CHAPTER

Performing Self-Tests on a Device

Understanding FIPS Self-Tests | 41

Understanding FIPS Self-Tests

The cryptographic module enforces security rules to ensure that a device running the Juniper Networks Junos operating system (Junos OS) in FIPS mode of operation meets the security requirements of FIPS 140-2 Level 1. To validate the output of cryptographic algorithms approved for FIPS and test the integrity of some system modules, the device performs the following series of known answer test (KAT) self-tests:

- **md_kats**—KAT for libmd and libc
- **openssl_kats**—KAT for OpenSSL cryptographic implementation
- **kernel_kats**—KAT for kernel cryptographic routines

The KAT self-tests are performed automatically at startup. Conditional self-tests are also performed automatically to verify digitally signed software packages, generated random numbers, RSA and ECDSA key pairs, and manually entered keys.

If the KATs are completed successfully, the system log (syslog) file is updated to display the tests that were executed.

If the device fails a KAT, the device writes the details to a system log file, enters FIPS error state (panic), and reboots.

The **file show /var/log/messages** command displays the system log.

For EX4300-48MP devices:

```
mgd: Running FIPS Self-tests
mgd: Testing kernel KATS:
mgd:   NIST 800-90 HMAC DRBG Known Answer Test:      Passed
mgd:   DES3-CBC Known Answer Test:                    Passed
mgd:   HMAC-SHA1 Known Answer Test:                    Passed
mgd:   HMAC-SHA2-256 Known Answer Test:                 Passed
mgd:   SHA-2-384 Known Answer Test:                     Passed
mgd:   SHA-2-512 Known Answer Test:                     Passed
mgd:   AES128-CMAC Known Answer Test:                   Passed
mgd:   AES-CBC Known Answer Test:                       Passed
mgd: Testing MACSec KATS:
mgd:   AES128-CMAC Known Answer Test:                   Passed
mgd:   AES256-CMAC Known Answer Test:                   Passed
mgd:   AES-ECB Known Answer Test:                       Passed
mgd:   AES-KEYWRAP Known Answer Test:                   Passed
mgd:   KBKDF Known Answer Test:                         Passed
mgd: Testing libmd KATS:
mgd:   HMAC-SHA1 Known Answer Test:                     Passed
```

```

mgd:   HMAC-SHA2-256 Known Answer Test:           Passed
mgd:   SHA-2-512 Known Answer Test:               Passed
mgd: Testing OpenSSL KATS:
mgd:   NIST 800-90 HMAC DRBG Known Answer Test:    Passed
mgd:   FIPS ECDSA Known Answer Test:               Passed
mgd:   FIPS ECDH Known Answer Test:               Passed
mgd:   FIPS RSA Known Answer Test:                 Passed
mgd:   DES3-CBC Known Answer Test:                 Passed
mgd:   HMAC-SHA1 Known Answer Test:                Passed
mgd:   HMAC-SHA2-224 Known Answer Test:            Passed
mgd:   HMAC-SHA2-256 Known Answer Test:            Passed
mgd:   HMAC-SHA2-384 Known Answer Test:            Passed
mgd:   HMAC-SHA2-512 Known Answer Test:            Passed
mgd:   AES-CBC Known Answer Test:                  Passed
mgd:   AES-GCM Known Answer Test:                  Passed
mgd:   ECDSA-SIGN Known Answer Test:               Passed
mgd:   KDF-IKE-V1 Known Answer Test:               Passed
mgd:   KDF-SSH-SHA256 Known Answer Test:           Passed
mgd:   KAS-ECC-EPHEM-UNIFIED-NOKC Known Answer Test: Passed
mgd:   KAS-FFC-EPHEM-NOKC Known Answer Test:       Passed
mgd: Testing QuickSec 7.0 KATS:
mgd:   NIST 800-90 HMAC DRBG Known Answer Test:    Passed
mgd:   DES3-CBC Known Answer Test:                  Passed
mgd:   HMAC-SHA1 Known Answer Test:                 Passed
mgd:   HMAC-SHA2-224 Known Answer Test:             Passed
mgd:   HMAC-SHA2-256 Known Answer Test:             Passed
mgd:   HMAC-SHA2-384 Known Answer Test:             Passed
mgd:   HMAC-SHA2-512 Known Answer Test:             Passed
mgd:   AES-CBC Known Answer Test:                   Passed
mgd:   AES-GCM Known Answer Test:                   Passed
mgd:   SSH-RSA-ENC Known Answer Test:               Passed
mgd:   SSH-RSA-SIGN Known Answer Test:              Passed
mgd:   SSH-ECDSA-SIGN Known Answer Test:            Passed
mgd:   KDF-IKE-V1 Known Answer Test:                Passed
mgd:   KDF-IKE-V2 Known Answer Test:                Passed
mgd: Testing QuickSec KATS:
mgd:   NIST 800-90 HMAC DRBG Known Answer Test:    Passed
mgd:   DES3-CBC Known Answer Test:                  Passed
mgd:   HMAC-SHA1 Known Answer Test:                 Passed
mgd:   HMAC-SHA2-224 Known Answer Test:             Passed
mgd:   HMAC-SHA2-256 Known Answer Test:             Passed
mgd:   HMAC-SHA2-384 Known Answer Test:             Passed
mgd:   HMAC-SHA2-512 Known Answer Test:             Passed
mgd:   AES-CBC Known Answer Test:                   Passed

```

```

mgd:    AES-GCM Known Answer Test:                Passed
mgd:    SSH-RSA-ENC Known Answer Test:              Passed
mgd:    SSH-RSA-SIGN Known Answer Test:              Passed
mgd:    KDF-IKE-V1 Known Answer Test:                Passed
mgd:    KDF-IKE-V2 Known Answer Test:                Passed
mgd: Testing SSH IPsec KATS:
mgd:    NIST 800-90 HMAC DRBG Known Answer Test:      Passed
mgd:    DES3-CBC Known Answer Test:                  Passed
mgd:    HMAC-SHA1 Known Answer Test:                 Passed
mgd:    HMAC-SHA2-256 Known Answer Test:              Passed
mgd:    AES-CBC Known Answer Test:                   Passed
mgd:    SSH-RSA-ENC Known Answer Test:                Passed
mgd:    SSH-RSA-SIGN Known Answer Test:                Passed
mgd:    KDF-IKE-V1 Known Answer Test:                 Passed
mgd: Testing file integrity:
mgd:    File integrity Known Answer Test:              Passed
mgd: Testing crypto integrity:
mgd:    Crypto integrity Known Answer Test:            Passed
mgd: Expect an everiexec: no fingerprint for file='/sbin/kats/cannot-exec' fsid=216
    fileid=49356 gen=1 uid=0 pid=7351
xec Authentication error...
mgd: /sbin/kats/run-tests: /sbin/kats/cannot-exec: Authentication error
mgd: FIPS Self-tests Passed

```

4

CHAPTER

Operational Commands

[request system zeroize](#) | 45

request system zeroize

Syntax

request system zeroize

Release Information

Command introduced in Junos OS Release 18.1 for EX Series switches.

Description

Erase and replace with zeros all user-created data from Routing Engines.

Options

none—Zeroize all Routing Engines in Junos OS in FIPS mode. You must confirm the request by typing **yes** to proceed. This command is restricted to Crypto Officer because the **maintenance** permission bit is one of the permission bits, along with **secret** and **control**, that distinguishes Crypto Officer from other FIPS users.

Required Privilege Level

maintenance

RELATED DOCUMENTATION

[Understanding Zeroization to Clear System Data for FIPS Mode | 32](#)

[Zeroizing the System | 33](#)

List of Sample Output

[request system zeroize on page 45](#)

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system zeroize

```
security-administrator@switch:fips> request system zeroize
```

```
warning: System will be rebooted and may not boot without configuration
Erase all data, including configuration and log files? [yes,no] (no) yes
```

```
warning: ipsec-key-management subsystem not running - not needed by configuration.  
warning: zeroizing localre
```