Junos® OS

FIPS Evaluated Configuration Guide for MX240, MX480, MX960, MX2010, MX2020, EX9204, EX9208, and EX9214 Devices

Release
17.3R2

Modified: 2019-05-10

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

Junos® OS FIPS Evaluated Configuration Guide for MX240, MX480, MX960, MX2010, MX2020, EX9204, EX9208, and EX9214 Devices
17.3R2

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

List of Tables

About the Documentation

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 viii 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 viii 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`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	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*

Table 2: Text and Syntax Conventions (continued)

Convention	Description	Examples
Text like this	Represents names of configuration statements, commands, files, and directories; 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)	Encloses 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**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [*community-ids*]**

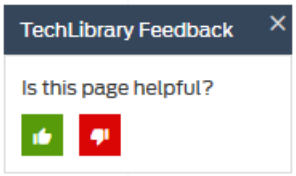
Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• 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/.

CHAPTER 1

Junos OS in FIPS Mode of Operation for MX and EX Series Devices

Understanding Junos OS in FIPS Mode

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, the Juniper Networks RE-1800 Routing Engine on Juniper Networks MX Series 3D Universal Edge Routers or EX Series Ethernet Switches running the Juniper Networks Junos operating system (Junos OS) in *FIPS mode* comply with the FIPS 140-2 Level 1 standard.

About the Cryptographic Boundary on Your Router or Switch

FIPS 140-2 compliance requires a defined *cryptographic boundary* around each *cryptographic module* on a router or 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 form.

CAUTION: **Virtual Chassis features are not supported in FIPS mode—they have not been tested by Juniper Networks. 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 *nonmodifiable 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 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.

For specific configuration limitations and restrictions, see *Understanding Configuration Limitations and Restrictions on Junos OS in FIPS Mode*.

Validated Version of Junos OS in FIPS Mode

To determine whether a Junos OS release is NIST-validated, see the compliance page on the Juniper Networks Web site (https://apps.juniper.net/compliance).

Related Documentation

- Identifying Secure Delivery on page 14

Identifying Secure 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 an appliance 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, 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 in 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 FIPS Mode Terminology and Supported Cryptographic Algorithms

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

- FIPS Terminology on page 15
- Supported Cryptographic Algorithms on page 16

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 26

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. MX Series routers or EX Series Ethernet switches are certified at FIPS 140-2 Level 1.

Crypto Officer—Person with appropriate permissions who is responsible for securely enabling, configuring, monitoring, and maintaining Junos OS in FIPS mode on a router or switch. For details, see "Understanding Roles and Services for Junos OS in FIPS Mode" on page 24.

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.**

Hashing—A message authentication method that applies a cryptographic technique iteratively to a message of arbitrary length and produces a hash *message digest* or *signature* of fixed length that is appended to the message when sent.

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 39.

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 router or switch before its operation as a FIPS cryptographic module—or in preparation for repurposing the router or switches 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 18.

Supported Cryptographic Algorithms

Table 3 on page 17 summarizes the high level protocol algorithm support.

Table 3: Protocols Allowed in FIPS Mode

Protocol	Key Exchange	Authentication	Cipher	Integrity
SSHv2	• ECDH-sha2-nistp256 • ECDH-sha2-nistp384 • ECDH-sha2-nistp521	Host (module): • ECDSA P-256 Client (user): • ECDSA P-256 • ECDSA P-384 • ECDSA P-521	• 3 Key Triple-DES CBC • AES CTR 128 • AES CTR 192 • AES CTR 256 • AES CBC 128 • AES CBC 192 • AES CBC 256	• 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.

BEST PRACTICE: **For FIPS 140-2 compliance, use only FIPS-approved cryptographic algorithms in Junos OS in FIPS mode.**

The following cryptographic algorithms are supported in FIPS mode. Symmetric methods use the same key for encryption and decryption, while asymmetric methods (preferred) 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, and 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 level, in bits. ECDSA using the P-256 curve can be configured under OpenSSH.

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

For Junos OS in FIPS mode, HMAC uses the iterated cryptographic hash function SHA-1 (designated as HMAC-SHA1) along with a secret key.

RSA—Algorithm for public key cryptography that is based on the presumed difficulty of factoring large integers of up to 2048 bits. The RSA algorithm involves three steps: key generation, encryption, and decryption. SSHv2 requires the asymmetric algorithm RSA-2048 with 2,048 bits (617 decimal digits), the largest of the RSA integers. The RSA algorithm is used in the validation of Juniper Networks signed binaries and is also available and used with the **ssh** command.

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 on page 39
- Understanding Zeroization to Clear System Data for FIPS Mode on page 18
- *Understanding Requirements for Secure Communication Between Routing Engines in FIPS Mode*

Understanding Zeroization to Clear System Data for FIPS Mode

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, and IPsec.

The Crypto Officer initiates the zeroization process by entering the **request system zeroize** operational command from the CLI after enabling FIPS mode.

CAUTION: **Perform system zeroization with care. After the zeroization process is complete, no data is left on the Routing Engine. The router or 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? on page 18
- When to Zeroize? on page 19

Why Zeroize?

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

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

When to Zeroize?

As Crypto Officer, perform zeroization in the following situations:

- **Before FIPS operation.** To prepare your router or switch for operation as a FIPS cryptographic module, perform zeroization before enabling FIPS mode.
- **Before non-FIPS operation.** To begin repurposing your router or switch for non-FIPS operation, perform zeroize before disabling FIPS mode.

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 on page 31
- Disabling FIPS Mode on page 49

Understanding FIPS Error States and System Panic

A router or switch running Junos OS in FIPS mode has certain operational restrictions such as the ability to load only integrity-checked software files and use only FIPS-approved cryptographic algorithms. To ensure correct operation, the router or switch performs a series of FIPS self-tests.

The router or switch performs additional tests as needed—for example, to ensure that randomly generated numbers are truly random and to verify manually entered keys (passwords).

If it fails a test, the router or switch enters a FIPS error state known as *system panic*.

When a low-level cryptographic function cannot complete for lack of memory or another resource, a memory allocation error occurs. This error does not result in system panic.

FIPS errors that occur early in the boot cycle can prevent the system from successfully starting up. For this reason, keep alternate boot media up to date.

For details, see:

- FIPS System Panic on page 20
- Memory Allocation Error on page 20
- Error Recovery from Alternate Boot Media on page 21

FIPS System Panic

If a router or switch fails a FIPS self-test, the router or switch enters a FIPS error state known as *system panic*. The panic condition halts all cryptographic processing and stops all data output from the router or switch. To clear the FIPS error, the router or switch reboots, runs the FIPS self-tests, and if it passes all the tests, returns to normal operation.

If the router or switch fails a self-test during a reboot from panic mode, the system stops booting and attempts to reboot. If the reboot is unsuccessful, the router or switch attempts again to reboot, this time from available boot media.

During a system panic, only status messages are displayed on the console. For example, a FIPS error is logged as shown in the following example:

```
panic: pid 5090 (fips-error), uid 0, FIPS error 5: cannot verify certificate
PackageCA
```

The reboot after panic displays the following error message on the console:

```
savecore: reboot after panic: pid 5090 (fips-error), uid 0, FIPS error 5: cannot
 verify certificate PackageCA
```

The following error states create a system panic:

NOTE: These errors have only an extremely small chance of occurring.

- The router or switch failed a known answer test (KAT).
- The random number is not random.
- Signature generation failed.
- Signature verification failed.
- Certificate verification failed.
- Encryption or decryption failed.
- An environment error occurred.
- An error occurred in a pair-wise conditional test.

Memory Allocation Error

A FIPS memory allocation error occurs when a low-level cryptographic function cannot finish processing for lack of memory or of another resource. This error causes the affected process to be terminated, but does not result in system panic.

FIPS memory failures are logged as follows:

```
Apr 15 23:08:15 shmoo /kernel: pid 6374 (fips-error), uid 0, FIPS error 9: RSA
verify memory allocation failed
```

Terminating the process clears the error so that the process can be run again.

Error Recovery from Alternate Boot Media

A Juniper Networks router or switch running Junos OS in FIPS mode performs KAT self-tests at startup. If the router or switch fails a KAT, the boot process stops and the router or switch attempts to reboot. If the reboot is unsuccessful, the router or switch attempts again to reboot, this time from available boot media.

If the alternate media are not functional, the router or switch might not be able to start up at all. In that case, the Crypto Officer must insert the removable boot media so that the system can boot normally and install Junos OS.

For this reason, be sure to keep the alternate media on the router or switch in a functional state by running the **request system snapshot recovery** command after enabling FIPS mode.

CHAPTER 2

Configuring Roles and Authentication Methods

Downloading and Installing Junos OS Software Packages (FIPS Mode)

MX Series routers or EX Series Ethernt switches can provide the security defined by Federal Information Processing Standards (FIPS) 140-2 Level 1. To operate in Junos OS in FIPS mode, the router or switch must have the following software packages installed:

- Junos FIPS mode, Release 17.3R2

To install the Junos software packages, perform the following tasks:

1. Download the Junos OS package and the Junos-FIPS software package from https://support.juniper.net/support/downloads/.
2. Connect locally to the active Routing Engine console port on the router or switch.
3. Copy Junos OS to the Routing Engine.
4. Upgrade the router or switch to Junos OS in FIPS mode by using the **request system software add reboot junos-install-mx-x86-64-17.3R2.tgz** command for MX Series routers and **request system software add reboot junos-install-ex92xx-x86-64-17.3R2.tgz** for EX Series Ethernet switces. For more details about adding system software, see the *Junos Installation and Configuration Guide*.

Related Documentation

- *Understanding the Operational Environment for Junos OS in FIPS Mode*

Understanding Roles and Services for Junos OS in FIPS Mode

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 (operator, administrative user, and so on) must fall into one of the two categories: Crypto Officer or FIPS user. For this reason, user authentication in FIPS mode is role-based rather than identity-based.

In addition to their FIPS roles, both user types can perform normal tasks on the router or switch as individual user configuration allows.

Crypto Officer and FIPS user configurations must follow the guidelines for Junos OS in FIPS mode.

For details, see:

- Crypto Officer Role and Responsibilities on page 24
- FIPS User Role and Responsibilities on page 25
- What Is Expected of All FIPS Users on page 25

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 router or switch. The Crypto Officer securely installs Junos OS on the router or switch, enables FIPS mode, establishes keys and passwords for other users and software modules, and initializes the router or switch before network connection.

BEST PRACTICE: **We recommend that the Crypto Officer administer the system in a secure manner by keeping passwords secure and checking audit files.**

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.
- 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 and data on (zeroize) the router or 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 Officers 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 users can view configuration on the router or switch and perform other tasks that are not specific to FIPS mode. FIPS user can view status output but cannot reboot or zeroize the device.

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 routers or switches and documentation in a secure area.
- Deploy routers or 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 on page 31
- *Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms*

Understanding the Operational Environment for Junos OS in FIPS Mode

A Juniper Networks router or switch running the Juniper Networks 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 router or switch in non-FIPS mode:

Hardware Environment for Junos OS in FIPS Mode

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

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

A Juniper Networks router or switch running Junos OS in FIPS mode forms a special type of nonmodifiable operational environment. To achieve this environment on the router or switch, the system prevents the execution of any binary file that was not part of the certified Junos OS in FIPS mode distribution. When a router or switch is in FIPS mode, it can run only Junos OS.

FIPS mode on MX Series routers and EX Series Ethernet switches is available in Junos OS Release 17.3R2 and later. The Junos OS in FIPS mode software environment is established after the Crypto Officer successfully enables FIPS mode on a router or switch. The Junos OS Release 17.3R2 image that includes FIPS mode is available on the Juniper Networks website and can be installed on a functioning router or switch.

For FIPS 140-2 compliance, we recommend that you delete all user-created files and data from (that is, *zeroize*) 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
- rsh
- telnet

- tftp
- xnm-clear-text

Attempts to configure these services, or load configurations with these services configured, result in a configuration syntax error.

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). The default password format must be changed to SHA256, or SHA512. 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.

For strict compliance, do not examine core and crash dump information on the local console in Junos OS in FIPS mode because some CSPs might be shown in plain text.

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 router or switch or Routing Engine as a cryptographic module.

Table 4 on page 27 lists CSPs on routers running Junos OS.

Table 4: Critical Security Parameters

CSP	Description	Zeroize	Use
SSH-2 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.
SSH-2 session key	Session key used with SSH-2 and as a Diffie-Hellman private key. Encryption: 3DES, AES-128, AES-192, AES-256. MACs: HMAC-SHA-1, HMAC-SHA-2-256, HMAC-SHA2-512 Key exchange: ECDH-sha2-nistp256, ECDH-sha2-nistp384, and ECDH-sha2-nistp521.	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.

Table 4: Critical Security Parameters (continued)

CSP	Description	Zeroize	Use
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 randon 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. However, as the Crypto Officer, you can enter user authentication data in plain text.

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

Local passwords are hashed with the SHA256 or SHA512 algorithm. 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 FIPS Mode Terminology and Supported Cryptographic Algorithms on page 15
- Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode on page 29
- Understanding Zeroization to Clear System Data for FIPS Mode on page 18
- *Understanding Configuration Limitations and Restrictions on Junos OS in FIPS Mode*

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. For a list of supported cryptographic algorithms (ciphers), see "Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms" on page 15.
- **Password encryption.** To change the default encryption method from MD5 to SHA256, or 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 (**r00t**) 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 FIPS Mode Terminology and Supported Cryptographic Algorithms on page 15
- Understanding the Operational Environment for Junos OS in FIPS Mode on page 26

Understanding Remote Access for Junos OS in FIPS Mode

When the router or switch is in Junos OS in FIPS mode, only SSH is available as a remote access service. To secure the information sent on administrative connections, use SSHv2 for CLI configuration. For SSH configuration information, see the *Junos OS System Basics Configuration Guide*.

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

The Ethernet management (**MGMT**) port on the router or switch is disabled by default. To use the MGMT port, you must enable the **fxp0** interface and assign it an IP address if you have not already done so. For more information, see the *Junos OS System Basics Configuration Guide*.

Related Documentation

- *Understanding Configuration Limitations and Restrictions on Junos OS in FIPS Mode*

Zeroizing the System

The **request system zeroize** command is a standard Junos OS operational mode command that you can use to revert a router or switch to the factory-default configuration. The operation unlinks all user-created data files, including customized configuration and log files, from their directories. The router or switch then reboots and reverts to the factory-default configuration. Your device is not considered a valid cryptographic module until all critical security parameters (CSPs) have been entered while the device is running the Junos OS in FIPS mode.

BEST PRACTICE: You must zeroize the system to remove all plain-text passwords, secret data, and private keys and CSPs, when no longer required.

The Crypto Officer runs the **request system zeroize** command to remove all user-created files from a device and replace the user data with zeros. This command completely erases all configuration information on the Routing Engines, including all rollback configuration files and plain-text passwords, secret data, and private keys and CSPs for SSH, local encryption, local authentication, IPsec, and SNMP.

To zeroize your device:

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

1. From the CLI, enter:

```
admin@device> 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:

```
  Erase all data, including configuration and log files?   [yes, no] (no)
yes
  re1:
  --------------------------------------------------------------------------
  warning: zeroizing re1
  ...
  Rebooting after scrubbing memory...
  ...
```

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

Establishing Root Password Access (FIPS Mode)

When Junos OS is installed on a router or switch and the router or switch is powered on, it is ready to be configured. Initially, you log in as the user **root** with no password. When you log in as **root**, your SSH connection is enabled by default.

As Crypto Officer, you must establish a root password conforming to the FIPS password requirements in "Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode" on page 29. When you enable FIPS mode in Junos OS on the router or switch, you cannot configure passwords unless they meet this standard.

After you log in, configure the root (superuser) password to be used to access the router or switch as follows:

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

```
% cli
  – JUNOS 17.3-20170807.0 built 2017-08-07 05:14:27 UTC
root@host:fips> configure
  Entering configuration mode
  [edit]
  root@host:fips#
```

2. To set the password format, include the **format** statement at the **[edit system password]** hierarchy level.

```
  [edit]
  root@host:fips# set system password format (sha256 | sha512)
```

3. Configure a temporary root password so that you can commit the configuration changes.

4. Commit the configuration changes.

5. Reset the root password to meet FIPS requirements.

6. Change the password format to a FIPS-compliant hash algorithm:

   NOTE: When establishing root password access after zeroization, the password format must be changed from the default of **md5**. MD5 is not a FIPS-compliant hash algorithm.

   a. Configure the FIPS-compliant hash algorithm for plain-text passwords by including the **format** statement at the **[edit system login]** hierarchy level and selecting **sha256**, or **sha512**:

      ```
      [edit]
      root@host:fips# set system login format (sha256 | sha512)
      ```

   b. Configure a temporary root password to be able to commit the password format change.

   c. Commit the configuration:

      ```
      [edit]
      root@host:fips# commit
        commit complete
      ```

7. Configure the root password by including the **root-authentication** statement at the **[edit system]** hierarchy level and selecting one of the password options.

   - To configure a plain-text password, select the **plain-text-password** option. Enter and confirm the password at the prompts.

     ```
     [edit]
     root@host:fips# set system root-authentication plain-text-password
     New password: type password here
     Retype new password: retype password here
     ```

     Ensure that you follow the password guidelines in "Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode" on page 29.

   - To configure public keys for SSH authentication of root logins, use the **ssh-ecdsa** option. You can configure more than one public key for SSH authentication of root logins as well as for user accounts. When a user logs in as **root**, the public keys are referenced to determine whether the private key matches any of them.

   NOTE: The system is now ready to execute the **set system fips level 1** command.

8. If you are finished configuring the router or switch, commit the configuration and exit:

```
[edit]
root@host:fips# commit
  commit complete
root@host:fips# exit
root@host:fips> exit
```

Related Documentation

- Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode on page 29
- For more information about the root password and root logins, see the *Junos OS System Basics Configuration Guide*.

Configuring Crypto Officer and FIPS User Identification and Access

Crypto Officer performs 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 Access on page 34
- Configuring FIPS User Login Access on page 35

Configuring Crypto Officer 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 router or switch with the root password if you have not already done so, and enter configuration mode:

   ```
   root@host:fips> configure
     Entering configuration mode
     [edit]
     root@host:fips#
   ```

2. Name the user **crypto-officer** and assign the Crypto Officer a user ID (for example, **6400**, which must be a unique number associated with the login account in the range of 100 through 64000) 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@host:fips# set system login user username uid value class class-name
   ```

For example:

```
[edit]
root@host:fips# 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 29, 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@host:fips# set system login user username uid value class class-name
  authentication (plain-test-password | encrypted-password)
```

For example:

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

4. Optionally, display the configuration:

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

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

```
[edit]
root@host:fips# commit
  commit complete
root@host:fips# exit
root@host:fips> exit
```

Otherwise, go on to "Configuring FIPS User Login Access" on page 35.

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.

As the Crypto Officer you set up FIPS users. FIPS users cannot be granted permissions normally reserved for the Crypto Officer—for example, permission to zeroize the system.

To configure login access for a FIPS user:

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

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

2. Give the user, a username, and assign the user a user ID (for example, 6401, which must be a unique number in the range of 1 through 64000) and a class read-only.

   For a list of permissions, see Understanding Junos OS Access Privilege Levels.

```
[edit]
root@host:fips# set system login user username uid value class class-name
```

   For example:

```
[edit]
crypto-officer@host:fips# 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 29, assign the FIPS user 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@host:fips# set system login user username uid value class class-name
  authentication (plain-text-password | encrypted-password)
```

   For example:

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

4. Optionally, display the configuration:

```
[edit]
crypto-officer@host:fips# edit system
[edit system]
crypto-officer@host:fips# show
login {
  user fips-user1 {
    uid 6401;
    authentication {
```

```
        encrypted-password "<cipher-text>"; ## SECRET-DATA
    }
    class read-only;
  }
}
```

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

```
[edit]
crypto-officer@host:fips# commit
crypto-officer@host:fips> exit
```

Otherwise, go on to *Configuring the Console Port for FIPS Mode*.

Related Documentation

- Understanding Roles and Services for Junos OS in FIPS Mode on page 24

CHAPTER 3

Configuring FIPS Self-Tests on a Device

Understanding FIPS Self-Tests

The cryptographic module enforces security rules to ensure that a router or switch running the Juniper Networks Junos operating system (Junos OS) in FIPS mode 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 router or switch performs the following series of known answer test (KAT) self-tests:

- **kernel_kats**—KAT for kernel cryptographic routines
- **md_kats**—KAT for libmd and libc
- **openssl_kats**—KAT for OpenSSL cryptographic implementation
- **quicksec_kats**—KAT for QuickSec Toolkit cryptographic implementation
- **ssh_ipsec_kats**—KAT for SSH IPsec Toolkit cryptographic implementation

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 router or switch fails a KAT, it writes the details to a system log file, enters FIPS error state (panic), and reboots the router or switch.

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

Related Documentation

- Example: Configuring FIPS Self-Tests on page 40

Example: Configuring FIPS Self-Tests

This example shows how to configure FIPS self-tests to run periodically.

Hardware and Software Requirements

- You must have administrative privileges to configure FIPS self-tests.
- The device must be running the evaluated version of Junos OS in FIPS mode software.

Overview

The FIPS self-test consists of the following suites of known answer tests (KATs):

- **kernel_kats**—KAT for kernel cryptographic routines
- **md_kats**—KAT for libmd and libc
- **quicksec_kats**—KAT for QuickSec Toolkit cryptographic implementation
- **openssl_kats**—KAT for OpenSSL cryptographic implementation
- **ssh_ipsec_kats**—KAT for SSH IPsec Toolkit cryptographic implementation

In this example, the FIPS self-test is executed at 9:00 AM in New York City, USA, every Wednesday.

NOTE: **Instead of weekly tests, you can configure monthly tests by including the month and day-of-month statements.**

When a KAT self-test fails, a log message is written to the system log messages file with details of the test failure. Then the system panics and reboots.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands into a text file, remove any line breaks, and then paste the commands into the CLI at the **[edit]** hierarchy level.

```
set system fips self-test periodic start-time 09:00
set system fips self-test periodic day-of-week 3
```

Step-by-Step Procedure

To configure the FIPS self-test:

1. Configure the FIPS self-test to execute at 9:00 AM every Wednesday.

```
[edit system fips self-test]
user@host# set periodic start-time 09:00
user@host# set periodic day-of-week 3
```

2. If you are done configuring the device, commit the configuration.

```
[edit system fips self-test]
user@host# commit
```

Results

From configuration mode, confirm your configuration by issuing the **show system** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show system
fips {
  self-test {
    periodic {
      start-time "09:00";
      day-of-week 3;
    }
  }
}
```

Verification

Confirm that the configuration is working properly.

Verifying the FIPS Self-Test

Purpose Verify that the FIPS self-test is enabled.

Action Run the FIPS self-test manually by issuing the **request system fips self-test** command.

After issuing the **request system fips self-test** command, the system log file is updated to display the KATs that are executed. To view the system log file, issue the **file show /var/log/messages** command.

For MX Series routers:

```
user@host> file show /var/log/messages
   Aug  7 21:29:43  adora kernel: mgd: Running FIPS Self-tests
   Aug  7 21:29:43  adora kernel: mgd: Testing kernel KATS:
   Aug  7 21:29:43  adora kernel: mgd:   NIST 800-90 HMAC DRBG Known Answer Test:
        Passed
   Aug  7 21:29:43  adora kernel: mgd:   DES3-CBC Known Answer Test:
          Passed
   Aug  7 21:29:43  adora kernel: mgd:   HMAC-SHA1   Known Answer Test:
```

```
          Passed
Aug  7 21:29:43  adora kernel: mgd:   HMAC-SHA2-256 Known Answer Test:
        Passed
Aug  7 21:29:43  adora kernel: mgd:   SHA-2-384 Known Answer Test:
        Passed
Aug  7 21:29:43  adora kernel: mgd:   SHA-2-512 Known Answer Test:
        Passed
Aug  7 21:29:43  adora kernel: mgd:   AES128-CMAC Known Answer Test:
        Passed
Aug  7 21:29:43  adora kernel: mgd:   AES-CBC Known Answer Test:
        Passed
Aug  7 21:29:43  adora kernel: mgd: Testing MacSec KATS:
Aug  7 21:29:43  adora kernel: mgd:   AES128-CMAC Known Answer Test:
        Passed
Aug  7 21:29:43  adora kernel: mgd:   AES256-CMAC Known Answer Test:
        Passed
Aug  7 21:29:43  adora kernel: mgd:   AES-KEYWRAP Known Answer Test:
        Passed
Aug  7 21:29:43  adora kernel: mgd: Testing libmd KATS:
Aug  7 21:29:43  adora kernel: mgd:   HMAC-SHA1 Known Answer Test:
        Passed
Aug  7 21:29:43  adora kernel: mgd:   HMAC-SHA2-256 Known Answer Test:
        Passed
Aug  7 21:29:43  adora kernel: mgd:   SHA-2-512 Known Answer Test:
        Passed
Aug  7 21:29:43  adora kernel: mgd: Testing OpenSSL KATS:
Aug  7 21:29:43  adora kernel: mgd:   FIPS RNG Known Answer Test:
        Passed
Aug  7 21:29:43  adora kernel: mgd:   NIST 800-90 HMAC DRBG Known Answer Test:
      Passed
Aug  7 21:29:43  adora kernel: mgd:   FIPS DSA Known Answer Test:
        Passed
Aug  7 21:29:43  adora kernel: mgd:   FIPS ECDSA Known Answer Test:
        Passed
Aug  7 21:29:43  adora kernel: mgd:   FIPS ECDH Known Answer Test:
        Passed
Aug  7 21:29:43  adora kernel: mgd:   FIPS RSA Known Answer Test:
        Passed
Aug  7 21:29:43  adora kernel: mgd:   DES3-CBC Known Answer Test:
        Passed
Aug  7 21:29:43  adora kernel: mgd:   HMAC-SHA1 Known Answer Test:
        Passed
Aug  7 21:29:43  adora kernel: mgd:   HMAC-SHA2-224 Known Answer Test:
        Passed
Aug  7 21:29:43  adora kernel: mgd:   HMAC-SHA2-256 Known Answer Test:
        Passed
Aug  7 21:29:43  adora kernel: mgd:   HMAC-SHA2-384 Known Answer Test:
        Passed
Aug  7 21:29:43  adora kernel: mgd:   HMAC-SHA2-512 Known Answer Test:
        Passed
Aug  7 21:29:43  adora kernel: mgd:   AES-CBC Known Answer Test:
        Passed
Aug  7 21:29:43  adora kernel: mgd:   AES-GCM Known Answer Test:
        Passed
Aug  7 21:29:43  adora kernel: mgd:   ECDSA-SIGN Known Answer Test:
        Passed
Aug  7 21:29:43  adora kernel: mgd:   KDF-IKE-V1 Known Answer Test:
        Passed
Aug  7 21:29:43  adora kernel: mgd:   KDF-SSH-SHA256 Known Answer Test:
        Passed
```

```
    Aug  7 21:29:43  adora kernel: mgd: Testing QuickSec KATS:
   Aug  7 21:29:43  adora kernel: mgd:   NIST 800-90 HMAC DRBG Known Answer Test:
         Passed
    Aug  7 21:29:43  adora kernel: mgd:   DES3-CBC Known Answer Test:
           Passed
    Aug  7 21:29:43  adora kernel: mgd:   HMAC-SHA1 Known Answer Test:
           Passed
    Aug  7 21:29:43  adora kernel: mgd:   HMAC-SHA2-224 Known Answer Test:
           Passed
    Aug  7 21:29:43  adora kernel: mgd:   HMAC-SHA2-256 Known Answer Test:
           Passed
    Aug  7 21:29:43  adora kernel: mgd:   HMAC-SHA2-384 Known Answer Test:
           Passed
    Aug  7 21:29:43  adora kernel: veriexec: no signatures for device.
file='/sbin/kats/cannot-exec' fsid=197 fileid=51404 gen=1 uid=0 pid=3226
    Aug  7 21:29:43  adora kernel: mgd:   HMAC-SHA2-512 Known Answer Test:
           Passed
    Aug  7 21:29:43  adora kernel: mgd:   AES-CBC Known Answer Test:
           Passed
    Aug  7 21:29:43  adora kernel: mgd:   AES-GCM Known Answer Test:
           Passed
    Aug  7 21:29:43  adora kernel: mgd:   SSH-RSA-ENC Known Answer Test:
           Passed
    Aug  7 21:29:43  adora kernel: mgd:   SSH-RSA-SIGN Known Answer Test:
           Passed
    Aug  7 21:29:43  adora kernel: mgd:   KDF-IKE-V1 Known Answer Test:
           Passed
    Aug  7 21:29:43  adora kernel: mgd:   KDF-IKE-V2 Known Answer Test:
           Passed
    Aug  7 21:29:43  adora kernel: mgd: Testing SSH IPsec KATS:
   Aug  7 21:29:43  adora kernel: mgd:   NIST 800-90 HMAC DRBG Known Answer Test:
         Passed
    Aug  7 21:29:43  adora kernel: mgd:   DES3-CBC Known Answer Test:
           Passed
    Aug  7 21:29:43  adora kernel: mgd:   HMAC-SHA1 Known Answer Test:
           Passed
    Aug  7 21:29:43  adora kernel: mgd:   HMAC-SHA2-256 Known Answer Test:
           Passed
    Aug  7 21:29:43  adora kernel: mgd:   AES-CBC Known Answer Test:
           Passed
    Aug  7 21:29:43  adora kernel: mgd:   SSH-RSA-ENC Known Answer Test:
           Passed
    Aug  7 21:29:43  adora kernel: mgd:   SSH-RSA-SIGN Known Answer Test:
           Passed
    Aug  7 21:29:43  adora kernel: mgd:   KDF-IKE-V1 Known Answer Test:
           Passed
    Aug  7 21:29:43  adora kernel: mgd:   File integrity Known Answer Test:
           Passed
    Aug  7 21:29:43  adora kernel: mgd:   Crypto integrity Known Answer Test:
           Passed
    Aug  7 21:29:43  adora kernel: mgd: /sbin/kats/run-tests:
/sbin/kats/cannot-exec: Authentication error
    Aug  7 21:29:43  adora kernel: mgd: FIPS Self-tests Passed
```

For EX Series Ethernet switches:

```
user@host> file show /var/log/messages
```

```
   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:    verieхe               c: no si   Passed
mgd: gnaturesTesting MacSec K forATS:
mgd:   AES device.128-CMAC Known A filnswer Test:     e='/sbin/kats
 Pa/cannot-execssed
mgd:   AES' fsid=2256-CMAC Known A08 fileid=5140nswer Test:     4 gen
   Pa=1 uid=0ssed
mgd:   AES pid=4695
-KEYWRAP 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:   FIPS RNG Known Answer Test:                      Passed
mgd:   NIST 800-90 HMAC DRBG Known Answer Test:         Passed
mgd:   FIPS DSA 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: 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 exec Authentication error...
mgd: /sbin/kats/run-tests: /sbin/kats/cannot-exec: Authentication error
mgd: FIPS Self-tests Passed
mgd: commit complete
```

Meaning The system log file displays the date and the time at which the KATs were executed and their status.

CHAPTER 4

Configuring Junos OS in FIPS Mode of Operation

Enabling FIPS mode

You, as Crypto Officer, can enable and configure Junos OS in FIPS mode on your router or switch.

Before you begin enabling and configuring FIPS mode on the router or switch:

- Verify the secure delivery of your router or switch. See "Identifying Secure Delivery" on page 14.

To enable and configure Junos OS in FIPS mode, perform the following tasks. Follow the links for instructions.

1. Connect to console port and zeroize the device to delete all CSPs before entering FIPS mode.

2. After the device comes up in 'Amnesiac mode', login using username **root** and password **""** (blank).

```
FreeBSD/amd64 (Amnesiac) (ttyu0)
login: root
  --- JUNOS 17.3R2 Kernel 64-bit  JNPR-10.3-20171116.170330_fbsd-
  At least one package installed on this device has limited support.
  Run 'file show /etc/notices/unsupported.txt' for details.
root@:~ #
```

3. Configure root authentication.

```
root> edit
  Entering configuration mode
  [edit]
  root# set system root-authentication plain-text-password
  New password:
```

```
  Retype new password:
  [edit]
  root# commit
  commit complete
```

4. Load configuration onto device and commit new configuration.

5. Configure Crypto Officer authentication and login using Crypto Officer credentials.

6. Install fips-mode package needed for Routing Engine KATS.

```
crypto-officer@hostname> request system software add optional://fips-mode.tgz
  Verified fips-mode signed by PackageDevelopmentEc_2017 method ECDSA256+SHA256
```

7. Configure fips level 1 and commit.

```
crypto-officer@hostname>edit
  Entering configuration mode
[edit]
crypto-officer@hostname# set system fips level 1
```

Device might display *Encrypted-password must be re-configured to use FIPS compliant hash* warning to delete older CSP in loaded configuration.

8. After deleting and reconfiguring CSPs, commit will go through and device needs reboot to enter FIPS mode.

```
[edit]
crypto-officer@hostname# commit
  Generating RSA key /etc/ssh/fips_ssh_host_key
  Generating ECDSA key /etc/ssh/fips_ssh_host_ecdsa_key
  [edit]
  system
  reboot is required to transition to FIPS level 1
  commit complete
```

9. After rebooting the device, FIPS self-tests will run and device enters FIPS mode.

```
crypto-officer@hostname>
```

After you as the Crypto Officer complete Junos OS in FIPS mode configuration, you can connect the router or switch to the network and proceed with normal configuration.

Related Documentation

- Understanding the Operational Environment for Junos OS in FIPS Mode on page 26

Disabling FIPS Mode

As Crypto Officer, you might need to disable FIPS mode on your router or switch to return it to non-FIPS operation.

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

To disable FIPS mode in Junos OS:

1. Log in to the router or switch with your Crypto Officer password if you have not already done so:

```
crypto-officer@hostname:fips> request system zeroize
```

2. The device will display below warning messages. Type in “yes” to proceed with zeroization of device.

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

re0:
--------------------------------------------------------------------------
warning: zeroizing re0
```

3. Once zeroize is done, router will reboot with “Factory-default” setting (without any configuration).

```
  – JUNOS 17.3-20170807.0 built 2017-08-07 05:14:27 UTC
root@host:fips> configure
  Entering configuration mode
  [edit]
  root@host:fips#
```

CHAPTER 5

Operational Commands for Junos OS in FIPS Mode

- request system zeroize

request system zeroize

Syntax

```
request system zeroize
<local>
```

Release Information

Command introduced before Junos OS Release 9.0.
Command introduced in Junos OS Release 12.2 for MX Series routers.

Description

Remove all configuration information on the Routing Engines and reset all key values. The command removes all data files, including customized configuration and log files, by unlinking the files from their directories. The command removes all user-created files from the system including all plain-text passwords, secrets, and private keys for SSH, local encryption, local authentication, IPsec, RADIUS, TACACS+, and SNMP.

This command reboots the device and sets it to the factory default configuration. After the reboot, you cannot access the device through the management Ethernet interface. Log in through the console as **root** and start the Junos OS CLI by typing **cli** at the prompt.

NOTE: If you configure the **commit synchronize** statement at the **[edit system]** hierarchy level and issue a **commit** in the master Routing Engine, the master configuration is automatically synchronized with the backup. However, if the backup Routing Engine is down when you issue the **commit**, the Junos OS displays a warning and commits the candidate configuration in the master Routing Engine. When the backup Routing Engine comes up, its configuration will automatically be synchronized with the master. A newly inserted backup Routing Engine automatically synchronizes its configuration with the master Routing Engine configuration.

Required Privilege Level

maintenance

List of Sample Output

request system zeroize on page 52

Sample Output

request system zeroize

```
user@host> 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.
error: Could not connect to re1 : Invalid argument
error: Couldn't connect to re re1
warning: zeroizing re0
```

```
Waiting (max 60 seconds) for system process `vnlru' to stop...done
Waiting (max 60 seconds) for system process `bufdaemon' to stop...done
Waiting (max 60 seconds) for system process `syncer' to stop...
Syncing disks, vnodes remaining...0 0 0 0 done
All buffers synced.
Uptime: 25m19s
besw0: 4 Broadcom SDK kernel threads killed
Khelp module "jsocket" can't unload until its refcount drops from 21 to 0.

Version 2.00.1201. Copyright (C) 2009 American Megatrends, Inc.
KONTRON RE2027 Firmware Version 1.18
........
```