

# Junos<sup>®</sup> OS

---

## FIPS Evaluated Configuration Guide for MX204 and EX9251 Devices

Published  
2020-06-17

Release  
19.2R1

Juniper Networks, Inc.  
1133 Innovation Way  
Sunnyvale, California 94089  
USA  
408-745-2000  
[www.juniper.net](http://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<sup>®</sup> OS FIPS Evaluated Configuration Guide for MX204 and EX9251 Devices*

19.2R1

Copyright © 2020 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

Supported Platforms | 11

About the Cryptographic Boundary on Your Device | 11

How FIPS Mode Differs from Non-FIPS Mode | 12

Validated Version of Junos OS in FIPS Mode | 12

### Understanding FIPS Terminology and Supported Cryptographic Algorithms | 13

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 | 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 | 21

Software Environment for Junos OS in FIPS Mode | 21

Critical Security Parameters | 23

Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode | 25

Downloading Software Packages from Juniper Networks | 26

Installing Software on MX204 or EX9251 devices with Single Routing Engine | 27

Understanding Zeroization to Clear System Data for FIPS Mode | 30

Why Zeroize? | 31

When to Zeroize? | 31

Zeroizing the System | 32

Enabling FIPS Mode | 33

Configuring Crypto Officer and FIPS User Identification and Access | 35

Configuring Crypto Officer Access | 35

Configuring FIPS User Login Access | 37

### 3

## Performing Self-Tests on a Device

Understanding FIPS Self-Tests | 41

Example: Configuring FIPS Self-Tests | 41

### 4

## Operational Commands

`request vmhost zeroize` | 48

# 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 MX204 and EX9251 devices 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
<b>Bold text like this</b>	Represents text that you type.	To enter configuration mode, type the <b>configure</b> command:  user@host> <b>configure</b>
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> <b>show chassis alarms</b>  No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> <li>Introduces or emphasizes important new terms.</li> <li>Identifies guide names.</li> <li>Identifies RFC and Internet draft titles.</li> </ul>	<ul style="list-style-type: none"> <li>A policy <i>term</i> is a named structure that defines match conditions and actions.</li> <li><i>Junos OS CLI User Guide</i></li> <li>RFC 1997, <i>BGP Communities Attribute</i></li> </ul>

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@# <b>set system domain-name</b> <i>domain-name</i>
<b>Text like this</b>	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> <li>To configure a stub area, include the <b>stub</b> statement at the [edit <b>protocols ospf area area-id</b>] hierarchy level.</li> <li>The console port is labeled <b>CONSOLE</b>.</li> </ul>
< > (angle brackets)	Encloses optional keywords or variables.	<b>stub</b> <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.	<b>broadcast   multicast</b>  ( <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.	<b>rsvp { # Required for dynamic MPLS only</b>
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	<b>community name members [ <i>community-ids</i> ]</b>
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
<b>Bold text like this</b>	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> <li>In the Logical Interfaces box, select <b>All Interfaces</b>.</li> <li>To cancel the configuration, click <b>Cancel</b>.</li> </ul>
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select <b>Protocols&gt;Ospf</b> .

## 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](mailto: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 Terminology and Supported Cryptographic Algorithms | 13

Identifying Secure Product Delivery | 16

Understanding Management Interfaces | 17

---

# Understanding Junos OS in FIPS Mode

## IN THIS SECTION

- [Supported Platforms | 11](#)
- [About the Cryptographic Boundary on Your Device | 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. The 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.

Operating MX Series routers or EX Series Ethernet Switches in a FIPS 140-2 Level 1 environment requires enabling and configuring FIPS mode from the Junos OS command-line interface (CLI).

The *Crypto Officer* enables FIPS mode in Junos OS Release 19.2R1 and sets up keys and passwords for the system and other *FIPS users*.

## Supported Platforms

For the features described in this document, the following platforms are evaluated for FIPS certification:

- [MX204 Series Routers](#).
- [EX9251 Series Switches](#).

## About the Cryptographic Boundary on Your Device

FIPS 140-2 compliance requires a defined *cryptographic boundary* around each *cryptographic module* on a device. 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. Do not configure a Virtual Chassis in FIPS mode.

## How FIPS Mode Differs from Non-FIPS Mode

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.

## Validated Version of Junos OS in FIPS Mode

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

### RELATED DOCUMENTATION

Identifying Secure Product Delivery | 16

# Understanding FIPS Terminology and Supported Cryptographic Algorithms

## IN THIS SECTION

- Terminology | 13
- Supported Cryptographic Algorithms | 14

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

## 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. MX devices 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 device. For details, see [“Understanding Roles and Services for Junos OS in FIPS” 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 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 device before its operation as a FIPS cryptographic module or in preparation for repurposing the device for non-FIPS operation. The Crypto Officer can zeroize the system with a CLI operational command.

## Supported Cryptographic Algorithms

[Table 3 on page 14](#) summarizes the high level protocol algorithm support.

**Table 3: Protocols Allowed in FIPS Mode**

Protocol	Key Exchange	Authentication	Cipher	Integrity
SSHv2	<ul style="list-style-type: none"> <li>dh-group14-sha1</li> <li>ECDH-sha2-nistp256</li> <li>ECDH-sha2-nistp384</li> <li>ECDH-sha2-nistp521</li> </ul>	Host (module): <ul style="list-style-type: none"> <li>ECDSA P-256</li> <li>SSH-RSA</li> </ul> Client (user): <ul style="list-style-type: none"> <li>ECDSA P-256</li> <li>ECDSA P-384</li> <li>ECDSA P-521</li> <li>SSH-RSA</li> </ul>	<ul style="list-style-type: none"> <li>3 Key Triple-DES CBC</li> <li>AES CTR 128</li> <li>AES CTR 192</li> <li>AES CTR 256</li> <li>AES CBC 128</li> <li>AES CBC 192</li> <li>AES CBC 256</li> </ul>	<ul style="list-style-type: none"> <li>HMAC-SHA-1</li> <li>HMAC-SHA-256</li> <li>HMAC-SHA-512</li> </ul>

**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 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.

**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, P-384, and P-521 curves 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 functions SHA-1, SHA-256, and SHA-512 along with a secret key.

**SHA-256 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, 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).

**NOTE:** 3DES is supported only in FIPS.

## RELATED DOCUMENTATION

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

[Understanding Zeroization to Clear System Data for FIPS Mode | 30](#)

# 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://support.juniper.net/support/> 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 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 | 19

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

Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode | 25

Downloading Software Packages from Juniper Networks | 26

Installing Software on MX204 or EX9251 devices with Single Routing Engine | 27

Understanding Zeroization to Clear System Data for FIPS Mode | 30

Zeroizing the System | 32

Enabling FIPS Mode | 33

Configuring Crypto Officer and FIPS User Identification and Access | 35

---

# Understanding Roles and Services for Junos OS in FIPS

## 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 (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.

Crypto Officer performs 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 device. The Crypto Officer securely installs Junos OS on the device, enables FIPS mode, establishes keys and passwords for other users and software modules, and initializes the device 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. The length of the password should be atleast 10 characters.
- Reset user passwords with FIPS-approved algorithms.
- Examine log and audit files for events of interest.
- Erase user-generated files, keys, and data by zeroizing the device.

## 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.

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 devices and documentation in a secure area.
- Deploy devices 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 | 32](#)

# Understanding the Operational Environment for Junos OS in FIPS Mode

## IN THIS SECTION

- [Hardware Environment for Junos OS in FIPS Mode | 21](#)
- [Software Environment for Junos OS in FIPS Mode | 21](#)
- [Critical Security Parameters | 23](#)

A Juniper Networks device 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 device in non-FIPS mode:

## Hardware Environment for Junos OS in FIPS Mode

Junos OS in FIPS mode establishes a cryptographic boundary in the device that no critical security parameters (CSPs) can cross using plain text. Each hardware component of the device 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 device running Junos OS in FIPS mode forms a special type of nonmodifiable operational environment. To achieve this environment on the device, the system prevents the execution of any binary

file that was not part of the certified Junos OS in FIPS mode distribution. When a device is in FIPS mode, it can run only Junos OS.

FIPS mode on MX204 Series routers and EX9251 Series switches is available in Junos OS Release 19.2R1 and later. The Junos OS in FIPS mode software environment is established after the Crypto Officer successfully enables FIPS mode on a device. The Junos OS Release 19.2R1 image that includes FIPS mode is available on the Juniper Networks website and can be installed on a functioning device.

For FIPS 140-2 compliance, we recommend that you delete all user-created files and data by *zeroizing* the device 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 SSH 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 device to a network until the Crypto Officer completes configuration from the local console connection.

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 device or Routing Engine as a cryptographic module.

Table 4 on page 23 lists CSPs on devices running Junos OS.

**Table 4: Critical Security Parameters**

CSP	Description	Zeroize	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.
SSHv2 session keys	Session key used with SSHv2 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: dh-group14-sha1, 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: SHA256, SHA512.	Zeroize command.	Used to authenticate a user to the cryptographic module.
Crypto Officer authentication key	Hash of the Crypto Officer's password: SHA256, SHA512.	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.

Table 4: Critical Security Parameters (*continued*)

CSP	Description	Zeroize	Use
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 device 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 Password Specifications and Guidelines for Junos OS in FIPS Mode | 25](#)

[Understanding Zeroization to Clear System Data for FIPS Mode | 30](#)



# 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 (**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 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 from the Juniper Networks website:

- Junos OS for MX and EX Series devices, Release 19.2R1

**NOTE:** For MX204 download, **junos-vmhost-install-mx-x86-64-19.2R1.tgz**.

For EX9251 download, **junos-vmhost-install-ex92xx-x86-64-19.2R1.tgz**.

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://userregistration.juniper.net/entitlement/setupAccountInfo.do>.

To download software packages from Juniper Networks:

1. Using a Web browser, follow the links to the download URL on the Juniper Networks webpage.  
<https://support.juniper.net/support/downloads/>
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. Download the software. See [Downloading Software](#)

## RELATED DOCUMENTATION

[Installation and Upgrade Guide](#)

## Installing Software on MX204 or EX9251 devices with Single Routing Engine

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

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

1. Download the software package as described in [“Downloading Software Packages from Juniper Networks” on page 26](#).
2. If you have not already done so, connect to the console port on the device from your management device, and log in to the Junos OS CLI.
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 device. 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 MX device:

```
user@hostname> request vmhost software add <package>
```

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

- For a software package in a local directory on the device, 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, `junos-vmhost-install-mx-x86-64-19.2R1.tgz`.
  - `ftp://hostname/pathname/package.tgz`
  - `http://hostname/pathname/package.tgz`

6. Reboot the device to load the installation:

```
user@hostname> request vmhost 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@hostname> show version
Hostname: hostname
Model: mx204
Junos: 19.2R1
JUNOS OS Kernel 64-bit [20190322.180549_fbsd-builder_stable_11]
JUNOS OS libs [20190322.180549_fbsd-builder_stable_11]
JUNOS OS runtime [20190322.180549_fbsd-builder_stable_11]
JUNOS OS time zone information [20190322.180549_fbsd-builder_stable_11]
JUNOS network stack and utilities [20190403.122029_builder_release_192_throttle]
JUNOS libs [20190403.122029_builder_release_192_throttle]
JUNOS OS libs compat32 [20190322.180549_fbsd-builder_stable_11]
JUNOS OS 32-bit compatibility [20190322.180549_fbsd-builder_stable_11]
JUNOS libs compat32 [20190403.122029_builder_release_192_throttle]
JUNOS runtime [20190403.122029_builder_release_192_throttle]
Junos vmguest package [20190403.122029_builder_release_192_throttle]
JUNOS sflow mx [20190403.122029_builder_release_192_throttle]
JUNOS py extensions [20190403.122029_builder_release_192_throttle]
JUNOS py base [20190403.122029_builder_release_192_throttle]
JUNOS OS vmguest [20190322.180549_fbsd-builder_stable_11]
JUNOS OS crypto [20190322.180549_fbsd-builder_stable_11]
JUNOS na telemetry [19.2-20190403.0]
JUNOS Security Intelligence [20190403.122029_builder_release_192_throttle]
JUNOS mx libs compat32 [20190403.122029_builder_release_192_throttle]
JUNOS mx runtime [20190403.122029_builder_release_192_throttle]
JUNOS common platform support [20190403.122029_builder_release_192_throttle]
JUNOS Openconfig [19.2-20190403.0]
JUNOS mtx network modules [20190403.122029_builder_release_192_throttle]
JUNOS modules [20190403.122029_builder_release_192_throttle]
JUNOS mx modules [20190403.122029_builder_release_192_throttle]
JUNOS mx libs [20190403.122029_builder_release_192_throttle]
JUNOS SQL Sync Daemon [20190403.122029_builder_release_192_throttle]
JUNOS mtx Data Plane Crypto Support [20190403.122029_builder_release_192_throttle]
JUNOS daemons [20190403.122029_builder_release_192_throttle]
JUNOS mx daemons [20190403.122029_builder_release_192_throttle]
JUNOS -MX appidd application-identification daemon
[20190403.122029_builder_release_192_throttle]
JUNOS Services URL Filter package [20190403.122029_builder_release_192_throttle]
JUNOS Services TLB Service PIC package
```

```

[20190403.122029_builder_release_192_throttle]
JUNOS Services Telemetry [20190403.122029_builder_release_192_throttle]
JUNOS Services TCP-LOG [20190403.122029_builder_release_192_throttle]
JUNOS Services SSL [20190403.122029_builder_release_192_throttle]
JUNOS Services SOFTWARE [20190403.122029_builder_release_192_throttle]
JUNOS Services Stateful Firewall [20190403.122029_builder_release_192_throttle]
JUNOS Services RTCOM [20190403.122029_builder_release_192_throttle]
JUNOS Services RPM [20190403.122029_builder_release_192_throttle]
JUNOS Services PCEF package [20190403.122029_builder_release_192_throttle]
JUNOS Services NAT [20190403.122029_builder_release_192_throttle]
JUNOS Services Mobile Subscriber Service Container package
[20190403.122029_builder_release_192_throttle]
JUNOS Services MobileNext Software package
[20190403.122029_builder_release_192_throttle]
JUNOS Services Logging Report Framework package
[20190403.122029_builder_release_192_throttle]
JUNOS Services LL-PDF Container package
[20190403.122029_builder_release_192_throttle]
JUNOS Services Jflow Container package
[20190403.122029_builder_release_192_throttle]
JUNOS Services Deep Packet Inspection package
[20190403.122029_builder_release_192_throttle]
JUNOS Services IPSec [20190403.122029_builder_release_192_throttle]
JUNOS Services IDS [20190403.122029_builder_release_192_throttle]
JUNOS IDP Services [20190403.122029_builder_release_192_throttle]
JUNOS Services HTTP Content Management package
[20190403.122029_builder_release_192_throttle]
JUNOS Services Flowd MS-MPC Software package
[20190403.122029_builder_release_192_throttle]
JUNOS Services Crypto [20190403.122029_builder_release_192_throttle]
JUNOS Services Captive Portal and Content Delivery Container package
[20190403.122029_builder_release_192_throttle]
JUNOS Services COS [20190403.122029_builder_release_192_throttle]
JUNOS AppId Services [20190403.122029_builder_release_192_throttle]
JUNOS Services Application Level Gateways
[20190403.122029_builder_release_192_throttle]
JUNOS Services ACL Container package
[20190403.122029_builder_release_192_throttle]
JUNOS SDN Software Suite [20190403.122029_builder_release_192_throttle]
JUNOS Extension Toolkit [20190403.122029_builder_release_192_throttle]
JUNOS Packet Forwarding Engine Support (wrlinux9)
[20190403.122029_builder_release_192_throttle]
JUNOS Packet Forwarding Engine Support (MX/EX92XX Common)
[20190403.122029_builder_release_192_throttle]

```

```
JUNOS Packet Forwarding Engine Support (M/T Common)
[20190403.122029_builder_release_192_throttle]
JUNOS Packet Forwarding Engine Support (MX Common)
[20190403.122029_builder_release_192_throttle]
JUNOS Juniper Malware Removal Tool (JMRT)
[1.0.0+20190403.122029_builder_release_192_throttle]
JUNOS J-Insight [20190403.122029_builder_release_192_throttle]
JUNOS jfirmware [20190403.122029_builder_release_192_throttle]
JUNOS Online Documentation [20190403.122029_builder_release_192_throttle]
JUNOS jail runtime [20190322.180549_fbsd-builder_stable_11]
```

## 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? | 31](#)
- [When to Zeroize? | 31](#)

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.

On MX204 and EX9521 devices, Crypto Officer initiates the zeroization process by entering the **request vmhost zeroize** operational command.



**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.

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

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

## When to Zeroize?

As Crypto Officer, perform zeroization in the following situations:

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

**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](#) | 32

# Zeroizing the System

To zeroize your device, follow the below procedure:

1. Connect to device with Crypto Officer credentials using console and from the CLI, enter

```
crypto-officer@hostname> request vmhost zeroize
VMHost Zeroization : Erase all data, including configuration and log files ?
[yes,no] (no) yes
```

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

```
Erase all data, including configuration and log files?  [yes, no] (no)
yes
warning: Vmhost will reboot and may not boot without configuration
warning: Proceeding with vmhost zeroize
Zeroize secondary internal disk ...
Proceeding with zeroize on secondary disk
Mounting device in preparation for zeroize...
Cleaning up target disk for zeroize ...
Zeroize done on target disk.
Zeroize of secondary disk completed
Zeroize primary internal disk ...
Proceeding with zeroize on primary disk
/etc/ssh/ssh_host_ecdsa_key
/etc/ssh/ssh_host_ecdsa_key.pub
/etc/ssh/ssh_host_dsa_key
/etc/ssh/ssh_host_rsa_key
/etc/ssh/ssh_host_rsa_key.pub
/etc/ssh/ssh_host_dsa_key.pub
Mounting device in preparation for zeroize...
Cleaning up target disk for zeroize ...
Zeroize done on target disk.
Zeroize of primary disk completed
Zeroize done
warning: Proceeding with vmhost reboot
Initiating vmhost reboot...
```

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 | 33](#)[Understanding Zeroization to Clear System Data for FIPS Mode | 30](#)

## Enabling FIPS Mode

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 25](#). When you enable FIPS mode in Junos OS on the device, you cannot configure passwords unless they meet this standard.

Local passwords are encrypted with the secure hash algorithm SHA256 or SHA512. 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.

To enable FIPS mode in Junos OS on the device:

1. Zeroize the device to delete all CSPs before entering FIPS mode. Refer to [“Understanding Zeroization to Clear System Data for FIPS Mode” on page 30](#) section for details.
2. After the device comes up in 'Amnesiac mode', login using username **root** and password "" (blank).

```
FreeBSD/amd64 (Amnesiac) (ttyu0)
login: root
--- JUNOS 19.2-20180131.0 Kernel 64-bit  JNPR-11.0-20180123.155949_fbsd-
root@:~ # cli
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. Configure Crypto Officer and login with Crypto Officer credentials.
5. The **fips-mode** and **jpfe-fips** are optional packages needed for enabling FIPS. These packages are part of Junos OS software. To enable these packages, use the following commands:

```
crypto-officer@hostname> request system software add optional://fips-mode
Verified fips-mode signed by PackageDevelopmentEc_2019 method ECDSA256+SHA256
```

```
crypto-officer@hostname> request system software add optional://jpfe-fips
Verified jpfe-fips signed by PackageDevelopmentEc_2019 method ECDSA256+SHA256
```

6. Configure chassis boundary fips by setting **set system fips chassis level 1** and **commit**. Device might display the **Encrypted-password must be re-configured to use FIPS compliant hash** warning to delete older CSP in loaded configuration.
7. 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 RSA2 key /etc/ssh/fips_ssh_host_rsa_key
Generating ECDSA key /etc/ssh/fips_ssh_host_ecdsa_key
[edit]
system
reboot is required to transition to FIPS level 1
commit complete
[edit]
crypto-officer@hostname# run request vmhost reboot
```

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

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

## RELATED DOCUMENTATION

[Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode](#) | 25

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

### IN THIS SECTION

- [Configuring Crypto Officer Access | 35](#)
- [Configuring FIPS User Login Access | 37](#)

Crypto Officers enables FIPS mode on device and 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

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 device with the root password if you have not already done so, and enter configuration mode:

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

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@hostname# set system login user username uid value class class-name
```

For example:

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

- Following the guidelines in “[Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode](#)” on page 25, 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@hostname# set system login user username class class-name authentication (plain-test-password |
    encrypted-password)
```

For example:

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

- Optionally, display the configuration:

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

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

```
[edit]
root@hostname# commit
commit complete
root@hostname# exit
Exiting configuration mode
root@hostname>
```

Otherwise, go on to [“Configuring FIPS User Login Access” on page 37](#).

## 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 device with your Crypto Officer password if you have not already done so, and enter configuration mode:

```
crypto-officer@hostname:fips> edit
Entering configuration mode
[edit]
crypto-officer@hostname: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. When you assign the class, you assign the permissions—for example, **clear**, **network**, **resetview**, and **view-configuration**.

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

```
[edit]
crypto-officer@hostname:fips# set system login user username uid value class read-only
```

For example:

```
[edit]
```

```
crypto-officer@hostname:fips# set system login user fips-user1 uid 6401 class read-only
```

- Following the guidelines in [“Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode” on page 25](#). 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]
crypto-officer@hostname:fips# set system login user username class read-only authentication
    (plain-text-password | encrypted-password)
```

For example:

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

- Optionally, display the configuration:

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

- If you are finished configuring the device, commit the configuration and exit:

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

## RELATED DOCUMENTATION

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

# 3

CHAPTER

## Performing Self-Tests on a Device

---

Understanding FIPS Self-Tests | 41

Example: Configuring FIPS Self-Tests | 41

---



# Understanding FIPS Self-Tests

The cryptographic module enforces security rules to ensure that 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 device 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

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 there is KAT failure, 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.

## Example: Configuring FIPS Self-Tests

### IN THIS SECTION

- [Hardware and Software Requirements | 42](#)
- [Overview | 42](#)
- [Configuration | 42](#)
- [Verification | 43](#)

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
- **openssl\_kats**—KAT for OpenSSL 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 and login to the device with crypto officer credentials:

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

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

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

```
[edit system fips self-test]
crypto-officer@hostname:fips# 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.

```
crypto-officer@hostname:fips# 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 or by rebooting the device.

After issuing the **request system fips self-test** command or after rebooting the device, 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.

**Cannot-exec** is an unsigned package and **/sbin/kats/run-tests: /sbin/kats/cannot-exec: Authentication error** is an expected message when the device in FIPS mode tries to install this unsigned package as part of FIPS self-tests.

For MX204 and EX9251 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-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 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 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 signatures for device. file='/sbin/kats/cannot-exec'
      fsid=209 fileid=51404 gen=1 uid=0 pid=4220:

```

```
xec Authentication error...  
mgd:    /sbin/kats/run-tests:/sbin/kats/cannot-exec: Authentication error  
mgd:    FIPS Self-tests Passed
```

# 4

CHAPTER

## Operational Commands

---

[request vmhost zeroize](#) | 48

---

# request vmhost zeroize

## Syntax

```
request vmhost zeroize
```

## Release Information

Command introduced in Junos OS Release 15.1F3 for the MX240, MX480, and MX960 devices.

## Description

Remove all configuration information on the Routing Engines and reset all key values. If the device has dual Routing Engines, the command is broadcast to both Routing Engines on the device. 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 the root user and start the Junos OS CLI by typing **cli** at the prompt.

## Required Privilege Level

maintenance

## List of Sample Output

[request vmhost zeroize on page 48](#)

## Sample Output

### request vmhost zeroize

```
user@host> request vmhost zeroize
```

```
VMHost Zeroization : Erase all data, including configuration and log files ?
[yes,no] (no) yes

re0:
-----
warning: Vmhost will reboot and may not boot without configuration
warning: Proceeding with vmhost zeroize
```



```
Zeroize secondary internal disk ...
Proceeding with zeroize on secondary disk
Mounting device in preparation for zeroize...
Cleaning up target disk for zeroize ...
Zeroize done on target disk.
Zeroize of secondary disk completed
Zeroize primary internal disk ...
Proceeding with zeroize on primary disk
/etc/ssh/ssh_host_ecdsa_key.pub
/etc/ssh/ssh_host_rsa_key
/etc/ssh/ssh_host_dsa_key.pub
/etc/ssh/ssh_host_rsa_key.pub
/etc/ssh/ssh_host_ecdsa_key
/etc/ssh/ssh_host_dsa_key
Mounting device in preparation for zeroize...
Cleaning up target disk for zeroize ...
Zeroize done on target disk.
Zeroize of primary disk completed
Zeroize done
```