



Junos[®] OS

FIPS Evaluated Configuration Guide for EX4600, QFX5100, and QFX5200 Devices

Release

18.1R1



Modified: 2019-08-07

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

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

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

Junos® OS FIPS Evaluated Configuration Guide for EX4600, QFX5100, and QFX5200 Devices

18.1R1

Copyright © 2019 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 | vii |
| | Documentation and Release Notes | vii |
| | Documentation Conventions | vii |
| | Documentation Feedback | ix |
| | Requesting Technical Support | x |
| | Self-Help Online Tools and Resources | x |
| | Creating a Service Request with JTAC | xi |
| Chapter 1 | Overview | 13 |
| | Understanding Junos OS in FIPS Mode | 13 |
| | About the Cryptographic Boundary on Your EX and QFX Series Switch | 13 |
| | How FIPS Mode Differs from Non-FIPS Mode | 14 |
| | Validated Version of Junos OS in FIPS Mode | 14 |
| | Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms | 15 |
| | FIPS Terminology | 15 |
| | Supported Cryptographic Algorithms | 16 |
| | Identifying Secure Product Delivery | 18 |
| | Understanding Management Interfaces | 19 |
| | Authentication Methods in FIPS Mode of Operation | 19 |
| | Username and Password Authentication over the Console and SSH | 19 |
| | Username and Public Key Authentication over SSH | 20 |
| Chapter 2 | Configuring Roles and Authentication Methods | 21 |
| | Understanding Roles and Services for Junos OS in FIPS Mode | 21 |
| | Crypto Officer Role and Responsibilities | 22 |
| | FIPS User Role and Responsibilities | 22 |
| | What Is Expected of All FIPS Users | 22 |
| | Understanding the Operational Environment for Junos OS in FIPS Mode | 23 |
| | Hardware Environment for Junos OS in FIPS Mode | 23 |
| | Software Environment for Junos OS in FIPS Mode | 24 |
| | Critical Security Parameters | 24 |
| | Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode | 26 |
| | Downloading Software Packages from Juniper Networks | 27 |
| | Installing Software on EX and QFX Series devices with a Single Routing Engine | 28 |

| | | |
|------------------|--|-----------|
| | Understanding Zeroization to Clear System Data for FIPS Mode | 30 |
| | Why Zeroize? | 31 |
| | When to Zeroize? | 31 |
| | Zeroizing the System | 32 |
| | Establishing Root Password Access | 33 |
| | Enabling FIPS Mode | 34 |
| | Configuring Crypto Officer and FIPS User Identification and Access | 39 |
| | Configuring Crypto Officer Login Access | 39 |
| | Configuring FIPS User Login Access | 40 |
| Chapter 3 | Performing Self-Tests on a Device | 43 |
| | Understanding FIPS Self-Tests | 43 |
| | Performing Power-On Self-Tests on the Device | 43 |
| Chapter 4 | Configuring SSH and Console Connection | 47 |
| | Configuring a System Login Message and Announcement | 47 |
| | Configuring SSH on the Evaluated Configuration | 48 |
| | Limiting the Number of User Login Attempts for SSH Sessions | 49 |
| Chapter 5 | Configuration Statements | 51 |
| | fips (FIPS) | 51 |
| | level (FIPS) | 52 |
| Chapter 6 | Operational Commands | 53 |
| | request system zeroize (FIPS) | 54 |

List of Tables

| | | |
|------------------|---|------------|
| | About the Documentation | vii |
| | Table 1: Notice Icons | viii |
| | Table 2: Text and Syntax Conventions | viii |
| Chapter 1 | Overview | 13 |
| | Table 3: Cryptographic Boundaries on FIPS-Certified EX and QFX Series Switches | 14 |
| Chapter 2 | Configuring Roles and Authentication Methods | 21 |
| | Table 4: Critical Security Parameters | 25 |

About the Documentation

- [Documentation and Release Notes on page vii](#)
- [Documentation Conventions on page vii](#)
- [Documentation Feedback on page ix](#)
- [Requesting Technical Support on page x](#)

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 |
| <i>Italic text like this</i> | <ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. | <ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i> |
| <i>Italic text like this</i> | Represents variables (options for which you substitute a value) in commands or configuration statements. | Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i> |

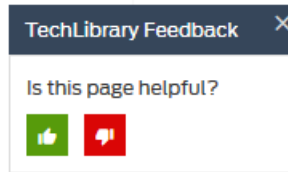
Table 2: Text and Syntax Conventions (continued)

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

Documentation Feedback

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

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



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

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>

- Join and participate in the Juniper Networks Community Forum:
<https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net>

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

Creating a Service Request with JTAC

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

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

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

CHAPTER 1

Overview

- [Understanding Junos OS in FIPS Mode on page 13](#)
- [Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms on page 15](#)
- [Identifying Secure Product Delivery on page 18](#)
- [Understanding Management Interfaces on page 19](#)
- [Authentication Methods in FIPS Mode of Operation on page 19](#)

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, Juniper Networks EX4600, QFX5100, and QFX5200 Series switches running the Juniper Networks Junos operating system (Junos OS) in *FIPS mode* comply with the FIPS 140-2 Level 1 standard.

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

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

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

- [About the Cryptographic Boundary on Your EX and QFX Series Switch on page 13](#)
- [How FIPS Mode Differs from Non-FIPS Mode on page 14](#)
- [Validated Version of Junos OS in FIPS Mode on page 14](#)

About the Cryptographic Boundary on Your EX and QFX Series Switch

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

For the Juniper Networks EX and QFX Series switches that are certified at FIPS-140-2 Level 1, the cryptographic boundary of the module is determined by the chassis type. For a list of FIPS-certified switches and the cryptographic boundary of each switch, see [Table 3 on page 14](#).

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

| Switch | Chassis Type | Cryptographic Boundary |
|----------------|--|------------------------|
| EX4600 switch | Fixed configuration with two expansion modules | Switch case |
| QFX5100 switch | Fixed configuration with two expansion modules | Switch case |
| QFX5200 switch | Fixed configuration | Switch case |



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

How FIPS Mode Differs from Non-FIPS Mode

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

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

Validated Version of Junos OS in FIPS Mode

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

Related Documentation

- [Identifying Secure Product Delivery on page 18](#)

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 23](#).

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

Crypto Officer—Person with appropriate permissions who is responsible for securely enabling, configuring, monitoring, and maintaining Junos OS in FIPS mode on a switch. For details, see [“Understanding Roles and Services for Junos OS in FIPS Mode” on page 21](#).

ESP—Encapsulating Security Payload (ESP) protocol. The part of the IPsec protocol that guarantees the confidentiality of packets through encryption. The protocol ensures that if an ESP packet is successfully decrypted, and no other party knows the secret key the peers share, the packet was not wiretapped in transit.

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

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



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

KATs—Known answer tests. System self-tests that validate the output of cryptographic algorithms approved for FIPS and test the integrity of some Junos OS modules. For details, see [“Understanding FIPS Self-Tests” on page 43](#).

SA—Security association (SA). A connection between hosts that allows them to communicate securely by defining, for example, how they exchange private keys. As Crypto Officer, you must manually configure an internal SA on switches running Junos OS in FIPS mode. All values, including the keys, must be statically specified in the configuration. On switches with more than one Routing Engine, the configuration must match on both ends of the connection between the Routing Engines. For communication to take place, each Routing Engine must have the same configured options, which need no negotiation and do not expire. .

SPI—Security parameter index (SPI). A numeric identifier used with the destination address and security protocol in IPsec to identify an SA. Because you manually configure the SA for Junos OS in FIPS mode, the SPI must be entered as a parameter rather than derived randomly.

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

Zeroization—Erasure of all CSPs and other user-created data on a switch before its operation as a FIPS cryptographic module—or in preparation for repurposing the switch for non-FIPS operation. The Crypto Officer can zeroize the system with a CLI operational command. For details, see [“Understanding Zeroization to Clear System Data for FIPS Mode” on page 30](#).

Supported Cryptographic Algorithms

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 use different keys for encryption and decryption.

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

Diffie-Hellman—A method of key exchange across a nonsecure environment (such as the Internet). The Diffie-Hellman algorithm negotiates a session key without sending the key itself across the network by allowing each party to pick a partial key

independently and send part of that key to the other. Each side then calculates a common key value. This is a symmetrical method—keys are typically used only for a short time, discarded, and regenerated.

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

ECDSA—Elliptic Curve Digital Signature Algorithm. A variant of the Digital Signature Algorithm (DSA) that uses cryptography based on the algebraic structure of elliptic curves over finite fields. The bit size of the elliptic curve determines the difficulty of decrypting the key. The public key believed to be needed for ECDSA is about twice the size of the security level, in bits. ECDSA uses the P-256, P-384, and P-521 curves that 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, SHA-384, and SHA-512—Secure hash algorithms (SHA) belonging to the SHA-2 standard defined in FIPS PUB 180-2. Developed by NIST, SHA-256 produces a 256-bit hash digest, SHA-384 produces a 384-bit hash digest, and SHA-512 produces a 512-bit hash digest.

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

- Related Documentation**
- [Understanding FIPS Self-Tests on page 43](#)
 - [Understanding Zeroization to Clear System Data for FIPS Mode on page 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 rear panel of a device is configured as RS-232 data terminal equipment (DTE). You can use the command-line interface (CLI) over this port to configure the device from a terminal.
- **Remote Management Protocols**—The device can be remotely managed over any Ethernet interface. SSHv2 is the only permitted remote management protocol that can be used in the evaluated configuration. The remote management protocols J-Web and Telnet are not available for use on the device.

Authentication Methods in FIPS Mode of Operation

The Juniper Networks Junos operating system (Junos OS) running in FIPS mode of operation allows a wide range of capabilities for users, and authentication is identity-based. The following types of identity-based authentication are supported in the FIPS mode of operation:

- [Username and Password Authentication over the Console and SSH on page 19](#)
- [Username and Public Key Authentication over SSH on page 20](#)

Username and Password Authentication over the Console and SSH

In this authentication method, the user is requested to enter the username and password. The device enforces the user to enter a minimum of 10-characters password that is chosen from the 96 human-readable ASCII characters.



NOTE: The maximum password length is 20 characters.

In this method, the device enforces a timed access mechanism—for example, first two failed attempts to enter the correct password (assuming 0 time to process), no timed access is enforced. When the user enters the password for the third time, the module enforces a 5-second delay. Each failed attempt thereafter results in an additional 5-second delay above the previous failed attempt. For example, if the fourth failed attempt is a 10-second delay, then the fifth failed attempt is a 15-second delay, the sixth failed attempt is a 20-second delay, and the seventh failed attempt is a 25-second delay.

Therefore, this leads to a maximum of seven possible attempts in a 1-minute period for each getty active terminal. So, the best approach for the attacker would be to disconnect after 4 failed attempts, and wait for a new getty to be spawned. This would allow the attacker to perform roughly 9.6 attempts per minute (576 attempts per hour or 60 minutes). This would be rounded off to 9 attempts per minute, because there is no such thing as 0.6 attempts. Thus the probability of a successful random attempt is $1/96^{10}$, which is less than 1/1 million. The probability of a success with multiple consecutive attempts in a 1-minute period is $9/(96^{10})$, which is less than 1/100,000.

Username and Public Key Authentication over SSH

With SSH public-key authentication, the user provides the username and proves ownership of the private key corresponding to the public key stored on the server. The device supports ECDSA (P-256, P-384, and P-521) and RSA (2048-bit or higher since our RSA implementation is FIPS 186-4 compliant). The probability of a success with multiple consecutive attempts in a 1-minute period is $5.6e7/(2^{112})$.

- Related Documentation**
- [Configuring SSH on the Evaluated Configuration on page 48](#)

CHAPTER 2

Configuring Roles and Authentication Methods

- [Understanding Roles and Services for Junos OS in FIPS Mode on page 21](#)
- [Understanding the Operational Environment for Junos OS in FIPS Mode on page 23](#)
- [Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode on page 26](#)
- [Downloading Software Packages from Juniper Networks on page 27](#)
- [Installing Software on EX and QFX Series devices with a Single Routing Engine on page 28](#)
- [Understanding Zeroization to Clear System Data for FIPS Mode on page 30](#)
- [Zeroizing the System on page 32](#)
- [Establishing Root Password Access on page 33](#)
- [Enabling FIPS Mode on page 34](#)
- [Configuring Crypto Officer and FIPS User Identification and Access on page 39](#)

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

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

For details, see:

- [Crypto Officer Role and Responsibilities on page 22](#)
- [FIPS User Role and Responsibilities on page 22](#)
- [What Is Expected of All FIPS Users on page 22](#)

Crypto Officer Role and Responsibilities

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



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

The permissions that distinguish the Crypto Officer from other FIPS users are **secret**, **security**, **maintenance**, and **control**. For FIPS compliance, assign the Crypto Officer to a login class that contains all of these permissions. A user with the Junos OS maintenance permission can read files containing critical security parameters (CSPs).



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

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

- Set the initial root password.
- 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 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 configure networking features on the switch and perform other tasks that are not specific to FIPS mode. FIPS users who are not Crypto Officers can view status output.

What Is Expected of All FIPS Users

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

All FIPS users must:

- Keep all passwords confidential.
- Store switches and documentation in a secure area.
- Deploy switches in secure areas.
- Check audit files periodically.
- Conform to all other FIPS 140-2 security rules.
- Follow these guidelines:
 - Users are trusted.
 - Users abide by all security guidelines.
 - Users do not deliberately compromise security.
 - Users behave responsibly at all times.

**Related
Documentation**

- [Zeroizing the System on page 32](#)
- [Configuring Crypto Officer and FIPS User Identification and Access on page 39](#)

Understanding the Operational Environment for Junos OS in FIPS Mode

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

- [Hardware Environment for Junos OS in FIPS Mode on page 23](#)
- [Software Environment for Junos OS in FIPS Mode on page 24](#)
- [Critical Security Parameters on page 24](#)

Hardware Environment for Junos OS in FIPS Mode

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

For more information about the cryptographic boundary on your switch, see [“Understanding Junos OS in FIPS Mode” on page 13](#).

Communications involving CSPs between these secure environments must take place using encryption.



BEST PRACTICE: If a seal is tampered with, the cryptographic module is considered to be compromised. To restore the module, we recommend that

you apply new tamper-evident seals, zeroize the system, and set up new passwords and CSPs.

.....

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

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

FIPS mode on EX and QFX Series switches are available starting with Junos OS Release 18.1R1. The Junos OS in FIPS mode software environment is established after the Crypto Officer successfully enables FIPS mode on EX and QFX Series switches. The Junos OS Release 18.1R1 image that includes FIPS package is available on the Juniper Networks website and can be installed on EX and QFX Series switches. See [“Downloading Software Packages from Juniper Networks” on page 27](#) for more information on image names.

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



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

.....

Critical Security Parameters

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

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

[Table 4 on page 25](#) lists CSPs on switches running Junos OS.

Table 4: Critical Security Parameters

| CSP | Description | Zeroization Method | Use |
|-----------------------------------|--|---|--|
| SSH-2 private host key | ECDSA key used to identify the host, generated the first time SSH is configured. 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-256. MACs: HMAC-SHA-1, HMAC SHA-256, HMAC SHA-512. Key exchange: DH Group exchange ($2048 \leq \text{key} \leq 8192$), ECDH: 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. |
| Crypto Officer authentication key | Hash of the Crypto Officer's password: SHA-256, SHA-512. | Zeroize command. | Used to authenticate the Crypto Officer to the cryptographic module. |
| HMAC DRBG seed | Seed for deterministic random bit generator (DRBG). | Seed is not stored by the cryptographic module. | Used for seeding DRBG. |
| HMAC DRBG V value | The value (V) of output block length (outlen) in bits, which is updated each time another outlen bits of output are produced. | Power cycle. | A critical value of the internal state of DRBG. |
| HMAC DRBG key value | The current value of the outlen-bit key, which is updated at least once each time that the DRBG mechanism generates pseudorandom bits. | Power cycle. | A critical value of the internal state of DRBG. |
| NDRNG entropy | Used as entropy input string to the HMAC DRBG. | Power cycle. | A critical value of the internal state of DRBG. |

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



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

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

- Related Documentation**
- [Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode on page 26](#)
 - [Understanding Zeroization to Clear System Data for FIPS Mode on page 30](#)

Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode

Ensure that the switch is in FIPS mode before you configure the Crypto Officer or any users. 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 example, 20 characters for SHA-1 authentication.

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

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

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

- Words that might be found in or exist as a permuted form in a system files such as `/etc/passwd`.
- The hostname of the system (always a first guess).
- Any word or phrase that appears in a dictionary or other well-known source, including dictionaries and thesauruses in languages other than English; works by classical or

popular writers; or common words and phrases from sports, sayings, movies or television shows.

- Permutations on any of the above—for example, a dictionary word with letters replaced with digits (**root**) or with digits added to the end.
- Any machine-generated password. Algorithms reduce the search space of password-guessing programs and so must not be used.

Related Documentation

- [Understanding the Operational Environment for Junos OS in FIPS Mode on page 23](#)

Downloading Software Packages from Juniper Networks

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

- Junos OS for EX and QFX Series switches, Release 18.1R1

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>.



NOTE: For EX4600, QFX5100, and QFX5200, FIPS is supported only on non-flex image. You have to upgrade to the non-flex image to enable FIPS mode. Also, the Junos OS Release 18.1R1 image `jinstall-host-qfx-5e-x86-64-18.1R1.9-secure-signed.tgz` that includes FIPS package is available on the Juniper Networks website and the same image can be installed on EX4600, QFX5100, and QFX5200 switches.

To download software packages from Juniper Networks:

1. Using a Web browser, follow the links to the download URL on the Juniper Networks webpage.
 - To download the software image, click the <https://support.juniper.net/support/downloads/> link.
2. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. Select the software package that you want to download. You can select software that supports a specific platform or technology:

- For Junos OS package, ensure that the name contains the correct switch name and the Junos OS release that is FIPS-certified on the switches.

The software image name for EX4600, QFX5100, and QFX5200 is
jinstall-host-qfx-5e-x86-64-18.1R1.9-secure-signed.tgz.

4. Download the software to a local host or to an internal software distribution site.
5. Install the Junos OS. See [“Installing Software on EX and QFX Series devices with a Single Routing Engine”](#) on page 28.

**Related
Documentation**

- [Installing Software on EX and QFX Series devices with a Single Routing Engine](#) on page 28

Installing Software on EX and QFX Series devices with a Single Routing Engine

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

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

1. Download the software package as described in [“Downloading Software Packages from Juniper Networks”](#) on page 27.
2. If you have not already done so, connect to the console port on the switch from your management device, and log in to the Junos OS CLI. (For instructions, see [Performing the Initial Software Configuration for QFX5200 Switches](#) for QFX5200, [Configuring a QFX5100 Device](#) for QFX5100, and [Configuring an EX4600 Switch](#) for EX4600.
3. (Optional) Back up the current software configuration to a second storage option. See the [Junos OS Installation and Upgrade Guide](#) for instructions on performing this task.
4. (Optional) Copy the software package to the switch. We recommend that you use FTP to copy the file to the **/var/tmp/** directory.

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

5. Install the new package on the switch:

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

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

- For a software package in a local directory on the switch, use **/var/tmp/package.tgz**.
- For a software package on a remote server, use one of the following paths, replacing **package** with the software package name—for example,
jinstall-host-qfx-5e-x86-64-18.1R1.9-secure-signed.tgz.

- `ftp://hostname/pathname/package.tgz`
- `http://hostname/pathname/package.tgz`



NOTE: If you need to terminate the installation, do not reboot your switch; instead, finish the installation and then issue the `request system software delete package.tgz` command, where `package.tgz` is, for example, `jinstall-host-qfx-5e-x86-64-18.1R1.9-secure-signed.tgz`. This is your last chance to stop the installation.

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

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

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

```
user@switch:> show version
localre:
-----
Hostname: switch
Model: ex4600-40f
Junos: 18.1R1.9
JUNOS OS Kernel 64-bit [20180308.0604c57_builder_stable_11]
JUNOS OS libs [20180308.0604c57_builder_stable_11]
JUNOS OS runtime [20180308.0604c57_builder_stable_11]
JUNOS OS time zone information [20180308.0604c57_builder_stable_11]
JUNOS OS libs compat32 [20180308.0604c57_builder_stable_11]
JUNOS OS 32-bit compatibility [20180308.0604c57_builder_stable_11]
JUNOS py extensions [20180323.181821_builder_junos_181_r1]
JUNOS py base [20180323.181821_builder_junos_181_r1]
JUNOS OS vmguest [20180308.0604c57_builder_stable_11]
JUNOS OS crypto [20180308.0604c57_builder_stable_11]
JUNOS network stack and utilities [20180323.181821_builder_junos_181_r1]
JUNOS libs [20180323.181821_builder_junos_181_r1]
JUNOS libs compat32 [20180323.181821_builder_junos_181_r1]
JUNOS runtime [20180323.181821_builder_junos_181_r1]
JUNOS Web Management Platform Package [20180323.181821_builder_junos_181_r1]
JUNOS qfx runtime [20180323.181821_builder_junos_181_r1]
JUNOS common platform support [20180323.181821_builder_junos_181_r1]
JUNOS qfx platform support [20180323.181821_builder_junos_181_r1]
JUNOS dcp network modules [20180323.181821_builder_junos_181_r1]
JUNOS modules [20180323.181821_builder_junos_181_r1]
JUNOS qfx modules [20180323.181821_builder_junos_181_r1]
JUNOS qfx Data Plane Crypto Support [20180323.181821_builder_junos_181_r1]
JUNOS daemons [20180323.181821_builder_junos_181_r1]
JUNOS qfx daemons [20180323.181821_builder_junos_181_r1]
JUNOS Services URL Filter package [20180323.181821_builder_junos_181_r1]
JUNOS Services TLB Service PIC package [20180323.181821_builder_junos_181_r1]
JUNOS Services Telemetry [20180323.181821_builder_junos_181_r1]
JUNOS Services SSL [20180323.181821_builder_junos_181_r1]
JUNOS Services SOFTWIRE [20180323.181821_builder_junos_181_r1]
JUNOS Services Stateful Firewall [20180323.181821_builder_junos_181_r1]
```

```
JUNOS Services RPM [20180323.181821_builder_junos_181_r1]
JUNOS Services PCEF package [20180323.181821_builder_junos_181_r1]
JUNOS Services NAT [20180323.181821_builder_junos_181_r1]
JUNOS Services Mobile Subscriber Service Container package
[20180323.181821_builder_junos_181_r1]
JUNOS Services MobileNext Software package
[20180323.181821_builder_junos_181_r1]
JUNOS Services Logging Report Framework package
[20180323.181821_builder_junos_181_r1]
JUNOS Services LL-PDF Container package
[20180323.181821_builder_junos_181_r1]
JUNOS Services Jflow Container package [20180323.181821_builder_junos_181_r1]
JUNOS Services Deep Packet Inspection package
[20180323.181821_builder_junos_181_r1]
JUNOS Services IPSec [20180323.181821_builder_junos_181_r1]
JUNOS Services IDS [20180323.181821_builder_junos_181_r1]
JUNOS IDP Services [20180323.181821_builder_junos_181_r1]
JUNOS Services HTTP Content Management package
[20180323.181821_builder_junos_181_r1]
JUNOS Services Crypto [20180323.181821_builder_junos_181_r1]
JUNOS Services Captive Portal and Content Delivery Container package
[20180323.181821_builder_junos_181_r1]
JUNOS Services COS [20180323.181821_builder_junos_181_r1]
JUNOS AppId Services [20180323.181821_builder_junos_181_r1]
JUNOS Services Application Level Gateways
[20180323.181821_builder_junos_181_r1]
JUNOS Services ACL Container package [20180323.181821_builder_junos_181_r1]
JUNOS SDN Software Suite [20180323.181821_builder_junos_181_r1]
JUNOS Extension Toolkit [20180323.181821_builder_junos_181_r1]
JUNOS Packet Forwarding Engine Support (DC-PFE)
[20180323.181821_builder_junos_181_r1]
JUNOS Packet Forwarding Engine Support (M/T Common)
[20180323.181821_builder_junos_181_r1]
JUNOS jfirmware [20180323.181821_builder_junos_181_r1]
JUNOS Online Documentation [20180323.181821_builder_junos_181_r1]
JUNOS jail runtime [20180308.0604c57_builder_stable_11]
JUNOS FIPS mode utilities [20180323.181821_builder_junos_181_r1]
JUNOS Host Software [3.14.52-rt50-WR7.0.0.9_ovp:3.0.8]
JUNOS Host qfx-5e host-control package [18.1R1.9]
JUNOS Host qfx-5e host-platform package [18.1R1.9]
JUNOS Host qfx-5e control-plane package [18.1R1.9]
JUNOS Host qfx-5e platform package [18.1R1.9]
JUNOS Host qfx-5e base package [18.1R1.9]
JUNOS Host qfx-5e data-plane package [18.1R1.9]
```

- Related Documentation**
- [Troubleshooting Software Installation](#)
 - [Understanding Software Installation on EX Series Switches](#)

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 \(FIPS\)](#) operational command from the CLI after enabling FIPS mode. Use of this command is restricted to the Crypto Officer.



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

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

- [Why Zeroize? on page 31](#)
- [When to Zeroize? on page 31](#)

Why Zeroize?

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



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

When to Zeroize?

As Crypto Officer, perform zeroization in the following situations:

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



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

- **When a tamper-evident seal is disturbed.** If the seal on secure port has been tampered with, the system is considered to be compromised. After applying new tamper-evident seals to the appropriate locations, zeroize the system and set up new passwords and CSPs.

Related Documentation

- [Zeroizing the System on page 32](#)
- [Enabling FIPS Mode on page 34](#)

Zeroizing the System

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

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

As Crypto Officer, you run the **request system zeroize** command to remove all user-created files from a switch 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, secrets, and private keys for SSH, local encryption, local authentication, and IPsec.

To zeroize your switch:



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

1. From the CLI, enter

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

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

```
Erase all data, including configuration and log files? [yes, no] (no)
yes
re0:
-----
warning: zeroizing re0
...
Rebooting after scrubbing memory...
...
```

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 on page 34](#)
- [Understanding Zeroization to Clear System Data for FIPS Mode on page 30](#)

Establishing Root Password Access

When Junos OS is installed on a switch and the switch is powered on, it is ready to be configured. Initially, you log in as the user **root** with no password.

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

Local passwords are encrypted with the secure hash algorithm SHA-1, SHA-256 or SHA-512. Password recovery is not possible in Junos OS in FIPS mode. Junos OS in FIPS mode cannot boot into single-user mode without the correct root password.

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

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

```
% cli
- JUNOS 18.1-20171129.0 built 2017-11-29 04:12:22 UTC
root@switch> configure
  Entering configuration mode
  [edit]
root@switch#
```

2. Change the password format to 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@switch# set system login password format ( sha256 | sha512)
```

3. 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@switch# 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 26](#).

- To configure public keys for SSH authentication of root logins, use the **ssh-eccdsa** option. You can configure more than one public key for SSH authentication of root

logins and 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.

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

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

Related Documentation • [Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode on page 26](#)

Enabling FIPS Mode

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

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



NOTE: To transition to FIPS mode, passwords must be encrypted with a FIPS-compliant hash algorithm. The encryption format must be SHA-1 or higher. Passwords that do not meet this requirement, such as passwords that are hashed with MD5, must be reconfigured or removed from the configuration before FIPS mode can be enabled.

To enable FIPS mode in Junos OS on the switch:

1. Enter configuration mode:

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

2. Enable FIPS mode on the switch by setting the FIPS level to 1, and verify the level:

```
[edit]
root@switch# set system fips level 1

[edit]
root@switch# show system
fips {
  level 1;
}
```

3. Commit the configuration:



NOTE: If the switch terminal displays error messages about the presence of critical security parameters (CSPs), delete those CSPs, and then commit the configuration.

```
root@switch# commit
configuration check succeeds
[edit]
'system'
  reboot is required to transition to FIPS level 1
commit complete
```

4. Reboot the switch:

```
[edit]
root@switch# run request system reboot
Reboot the system ? [yes,no] (no) yes
```

During the reboot, the switch runs Known Answer Tests (KATS). It returns a login prompt:

```
Verified manifest signed by PackageDevelopmentEc_2018 method ECDSA256+SHA256
cp: /var/host/junos-defaults.conf: No such file or directory
mount_cd9660: /dev/gpt/junos: Invalid argument
ifconfig: devop error: Device not configured
  bcmsdk_5_9_x kldKLD bcmsdk_5_9_x.ko: depends on acb - not available or
version mismatch
linker_load_file: Unsupported file type
kldload: an error occurred while loading the module. Please check dmesg(8)
for more details.
Junosprocfs mounted on /junosproc.
@ 1529397024 [2018-06-19 08:30:24 UTC] mgd start
Creating initial configuration: ...
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:   NIST 800-90 HMAC DRBG Known Answer Test:      Passed
mgd:   FIPS ECDSA Known Answer Test:                 Passed
```

```

mgd: FIPS ECDH Known Answer Test: Passed
mgd: FIPS RSA Known Answer Test: Passed
mgd: DES3-CBC Known Answer Test: Passed
mgd: HMAC-SHA1 Known Answer Test: Passed
mgd: HMAC-SHA2-224 Known Answer Test: Passed
mgd: HMAC-SHA2-256 Known Answer Test: Passed
mgd: HMAC-SHA2-384 Known Answer Test: Passed
mgd: HMAC-SHA2-512 Known Answer Test: Passed
mgd: AES-CBC Known Answer Test: Passed
mgd: AES-GCM Known Answer Test: Passed
mgd: ECDSA-SIGN Known Answer Test: Passed
mgd: KDF-IKE-V1 Known Answer Test: Passed
mgd: KDF-SSH-SHA256 Known Answer Test: Passed
mgd: KAS-ECC-EPHEM-UNIFIED-NOKC Known Answer Test: Passed
mgd: KAS-FFC-EPHEM-NOKC Known Answer Test: Passed
mgd: Testing QuickSec 7.0 KATS:
mgd: NIST 800-90 HMAC DRBG Known Answer Test: Passed
mgd: DES3-CBC Known Answer Test: Passed
mgd: HMAC-SHA1 Known Answer Test: Passed
mgd: HMAC-SHA2-224 Known Answer Test: Passed
mgd: HMAC-SHA2-256 Known Answer Test: Passed
mgd: HMAC-SHA2-384 Known Answer Test: Passed
mgd: HMAC-SHA2-512 Known Answer Test: Passed
mgd: AES-CBC Known Answer Test: Passed
mgd: AES-GCM Known Answer Test: Passed
mgd: SSH-RSA-ENC Known Answer Test: Passed
mgd: SSH-RSA-SIGN Known Answer Test: Passed
mgd: SSH-ECDSA-SIGN Known Answer Test: Passed
mgd: KDF-IKE-V1 Known Answer Test: Passed
mgd: KDF-IKE-V2 Known Answer Test: Passed
mgd: Testing QuickSec KATS:
mgd: NIST 800-90 HMAC DRBG Known Answer Test: Passed
mgd: DES3-CBC Known Answer Test: Passed
mgd: HMAC-SHA1 Known Answer Test: Passed
mgd: HMAC-SHA2-224 Known Answer Test: Passed
mgd: HMAC-SHA2-256 Known Answer Test: Passed
mgd: HMAC-SHA2-384 Known Answer Test: Passed
mgd: HMAC-SHA2-512 Known Answer Test: Passed
mgd: AES-CBC Known Answer Test: Passed
mgd: AES-GCM Known Answer Test: Passed
mgd: SSH-RSA-ENC Known Answer Test: Passed
mgd: SSH-RSA-SIGN Known Answer Test: Passed
mgd: KDF-IKE-V1 Known Answer Test: Passed
mgd: KDF-IKE-V2 Known Answer Test: Passed
mgd: Testing SSH IPsec KATS:
mgd: NIST 800-90 HMAC DRBG Known Answer Test: Passed
mgd: DES3-CBC Known Answer Test: Passed
mgd: HMAC-SHA1 Known Answer Test: Passed
mgd: HMAC-SHA2-256 Known Answer Test: Passed
mgd: AES-CBC Known Answer Test: Passed
mgd: SSH-RSA-ENC Known Answer Test: Passed
mgd: SSH-RSA-SIGN Known Answer Test: Passed
mgd: KDF-IKE-V1 Known Answer Test: Passed
mgd: Testing file integrity:
mgd: File integrity Known Answer Test: Passed
mgd: Testing crypto integrity:
mgd: Crypto integrity Known Answer Test: Passed
mgd: Expect an exec Authentication error...
verirexec: no fingerprint for file='/sbin/kats/cannot-exec' fsid=197
fileid=51404 gen=1 uid=0 pid=4119

```

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

Log in to the switch. The CLI displays a banner that is followed by a prompt that includes “:fips”:

```
--- JUNOS 18.1R1-20170816 built 2014-12-29 04:12:22 UTC
root@switch:fips>
```

5. Reboot the switch again to restore the HMAC-DRBG as an active random adapter:

```
[edit]
root@switch# run request system reboot
Reboot the system ? [yes,no] (no) yes
```

During the reboot, the switch runs Known Answer Tests (KATS) as shown in the step 4. It returns a login prompt:

```
--- JUNOS 18.1R1-20170816 built 2014-12-29 04:12:22 UTC
root@switch:fips>
```

6. After the reboot has completed, log in and use the **show version local** command to verify.

```
user@switch:fips> show version local
Hostname: switch
Model: ex4600-40f
Junos: 18.1R1.9
JUNOS OS Kernel 64-bit [20180308.0604c57_builder_stable_11]
JUNOS OS libs [20180308.0604c57_builder_stable_11]
JUNOS OS runtime [20180308.0604c57_builder_stable_11]
JUNOS OS time zone information [20180308.0604c57_builder_stable_11]
JUNOS OS libs compat32 [20180308.0604c57_builder_stable_11]
JUNOS OS 32-bit compatibility [20180308.0604c57_builder_stable_11]
JUNOS py extensions [20180323.181821_builder_junos_181_r1]
JUNOS py base [20180323.181821_builder_junos_181_r1]
JUNOS OS vmguest [20180308.0604c57_builder_stable_11]
JUNOS OS crypto [20180308.0604c57_builder_stable_11]
JUNOS network stack and utilities [20180323.181821_builder_junos_181_r1]
JUNOS libs [20180323.181821_builder_junos_181_r1]
JUNOS libs compat32 [20180323.181821_builder_junos_181_r1]
JUNOS runtime [20180323.181821_builder_junos_181_r1]
JUNOS Web Management Platform Package [20180323.181821_builder_junos_181_r1]
JUNOS qfx runtime [20180323.181821_builder_junos_181_r1]
JUNOS common platform support [20180323.181821_builder_junos_181_r1]
JUNOS qfx platform support [20180323.181821_builder_junos_181_r1]
JUNOS dcp network modules [20180323.181821_builder_junos_181_r1]
JUNOS modules [20180323.181821_builder_junos_181_r1]
JUNOS qfx modules [20180323.181821_builder_junos_181_r1]
JUNOS qfx Data Plane Crypto Support [20180323.181821_builder_junos_181_r1]
JUNOS daemons [20180323.181821_builder_junos_181_r1]
JUNOS qfx daemons [20180323.181821_builder_junos_181_r1]
JUNOS Services URL Filter package [20180323.181821_builder_junos_181_r1]
JUNOS Services TLB Service PIC package [20180323.181821_builder_junos_181_r1]
JUNOS Services Telemetry [20180323.181821_builder_junos_181_r1]
```

JUNOS Services SSL [20180323.181821_builder_junos_181_r1]
JUNOS Services SOFTWARE [20180323.181821_builder_junos_181_r1]
JUNOS Services Stateful Firewall [20180323.181821_builder_junos_181_r1]
JUNOS Services RPM [20180323.181821_builder_junos_181_r1]
JUNOS Services PCEF package [20180323.181821_builder_junos_181_r1]
JUNOS Services NAT [20180323.181821_builder_junos_181_r1]
JUNOS Services Mobile Subscriber Service Container package
[20180323.181821_builder_junos_181_r1]
JUNOS Services MobileNext Software package
[20180323.181821_builder_junos_181_r1]
JUNOS Services Logging Report Framework package
[20180323.181821_builder_junos_181_r1]
JUNOS Services LL-PDF Container package
[20180323.181821_builder_junos_181_r1]
JUNOS Services Jflow Container package [20180323.181821_builder_junos_181_r1]
JUNOS Services Deep Packet Inspection package
[20180323.181821_builder_junos_181_r1]
JUNOS Services IPSec [20180323.181821_builder_junos_181_r1]
JUNOS Services IDS [20180323.181821_builder_junos_181_r1]
JUNOS IDP Services [20180323.181821_builder_junos_181_r1]
JUNOS Services HTTP Content Management package
[20180323.181821_builder_junos_181_r1]
JUNOS Services Crypto [20180323.181821_builder_junos_181_r1]
JUNOS Services Captive Portal and Content Delivery Container package
[20180323.181821_builder_junos_181_r1]
JUNOS Services COS [20180323.181821_builder_junos_181_r1]
JUNOS AppId Services [20180323.181821_builder_junos_181_r1]
JUNOS Services Application Level Gateways
[20180323.181821_builder_junos_181_r1]
JUNOS Services ACL Container package [20180323.181821_builder_junos_181_r1]
JUNOS SDN Software Suite [20180323.181821_builder_junos_181_r1]
JUNOS Extension Toolkit [20180323.181821_builder_junos_181_r1]
JUNOS Packet Forwarding Engine Support (DC-PFE)
[20180323.181821_builder_junos_181_r1]
JUNOS Packet Forwarding Engine Support (M/T Common)
[20180323.181821_builder_junos_181_r1]
JUNOS jfirmware [20180323.181821_builder_junos_181_r1]
JUNOS Online Documentation [20180323.181821_builder_junos_181_r1]
JUNOS jail runtime [20180308.0604c57_builder_stable_11]
JUNOS FIPS mode utilities [20180323.181821_builder_junos_181_r1]
JUNOS Host Software [3.14.52-rt50-WR7.0.0.9_ovp:3.0.8]
JUNOS Host qfx-5e host-control package [18.1R1.9] JUNOS Host qfx-5e
host-platform package [18.1R1.9] JUNOS Host qfx-5e control-plane package
[18.1R1.9] JUNOS Host qfx-5e platform package [18.1R1.9] JUNOS Host qfx-5e
base package [18.1R1.9] JUNOS Host qfx-5e data-plane package [18.1R1.9]



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

Configuring Crypto Officer and FIPS User Identification and Access

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

- [Configuring Crypto Officer Login Access on page 39](#)
- [Configuring FIPS User Login Access on page 40](#)

Configuring Crypto Officer Login Access

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

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

To configure login access for a Crypto Officer:

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

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

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

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

```
[edit]
root@switch: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 26, assign the Crypto Officer a plain-text password for login authentication. Set the password by typing a password after the prompts **New password** and **Retype new password**.

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

4. Optionally, display the configuration:

```
[edit]
```

```
root@switch:fips# edit system
[edit system]
root@switch: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 switch, commit the configuration and exit:

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

Configuring FIPS User Login Access

A **fips-user** is defined as any FIPS user that does not have the **secret**, **security**, **maintenance**, and **control** permission bits set.

As the Crypto Officer you set up FIPS users.

To configure login access for a FIPS user:

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

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

2. Give the user a username, assign the FIPS user a user ID (for example, **6401**) and a class (for example, **read-only**). When you assign the class, you assign the permissions—for example, **clear**, **configure**, **network**, **resetview**, and **view-configuration**.

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

```
[edit]
crypto-officer@switch: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 26, assign the FIPS a plain-text password for login

authentication. Set the password by typing a password after the prompts **New password** and **Retype new password**.

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

4. Optionally, display the configuration:

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

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

```
[edit]
crypto-officer@switch:fips# commit
crypto-officer@switch: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 21](#)

CHAPTER 3

Performing Self-Tests on a Device

- [Understanding FIPS Self-Tests on page 43](#)

Understanding FIPS Self-Tests

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

- **md_kats**—KAT for libmd and libc
- **quicksec_7_0_kats**—KAT for Quicksec_7_0 Toolkit cryptographic implementation
- **openssl_kats**—KAT for OpenSSL cryptographic implementation
- **kernel_kats**—KAT for kernel cryptographic routines

The KAT self-tests are performed automatically at startup and reboot, regardless of whether FIPS mode of operation is enabled on the device. Conditional self-tests are also performed automatically to verify digitally signed software packages, generated random numbers, RSA and DSA key pairs, and manually entered keys.

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

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

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

Performing Power-On Self-Tests on the Device

Each time the cryptographic module is powered on, the module tests that the cryptographic algorithms still operate correctly and that sensitive data has not been damaged.

The module displays the following status output while running the power-on self-tests:

```
Verified manifest signed by PackageDevelopmentEc_2018 method ECDSA256+SHA256
cp: /var/host/junos-defaults.conf: No such file or directory
mount_cd9660: /dev/gpt/junos: Invalid argument
ifconfig: devop error: Device not configured bcmsdk_5_9_x kldKLD bcmsdk_5_9_x.ko:
  depends on acb - not available or version mismatch
linker_load_file: Unsupported file type
kldload: an error occurred while loading the module. Please check dmesg(8) for
more details.
Junosprocfs mounted on /junosproc.
@ 1529397024 [2018-06-19 08:30:24 UTC] mgd start Creating initial configuration:
...
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:   NIST 800-90 HMAC DRBG Known Answer Test:      Passed
mgd:   FIPS ECDSA Known Answer Test:                 Passed
mgd:   FIPS ECDH Known Answer Test:                  Passed
mgd:   FIPS RSA Known Answer Test:                   Passed
mgd:   DES3-CBC Known Answer Test:                   Passed
mgd:   HMAC-SHA1 Known Answer Test:                  Passed
mgd:   HMAC-SHA2-224 Known Answer Test:               Passed
mgd:   HMAC-SHA2-256 Known Answer Test:               Passed
mgd:   HMAC-SHA2-384 Known Answer Test:               Passed
mgd:   HMAC-SHA2-512 Known Answer Test:               Passed
mgd:   AES-CBC Known Answer Test:                   Passed
mgd:   AES-GCM Known Answer Test:                   Passed
mgd:   ECDSA-SIGN Known Answer Test:                 Passed
mgd:   KDF-IKE-V1 Known Answer Test:                 Passed
mgd:   KDF-SSH-SHA256 Known Answer Test:              Passed
mgd:   KAS-ECC-EPHEM-UNIFIED-NOKC Known Answer Test: Passed
mgd:   KAS-FFC-EPHEM-NOKC Known Answer Test:         Passed
mgd: Testing QuickSec 7.0 KATS:
mgd:   NIST 800-90 HMAC DRBG Known Answer Test:      Passed
mgd:   DES3-CBC Known Answer Test:                   Passed
mgd:   HMAC-SHA1 Known Answer Test:                  Passed
mgd:   HMAC-SHA2-224 Known Answer Test:               Passed
mgd:   HMAC-SHA2-256 Known Answer Test:               Passed
mgd:   HMAC-SHA2-384 Known Answer Test:               Passed
mgd:   HMAC-SHA2-512 Known Answer Test:               Passed
mgd:   AES-CBC Known Answer Test:                   Passed
mgd:   AES-GCM Known Answer Test:                   Passed
mgd:   SSH-RSA-ENC Known Answer Test:                Passed
```

```

mgd: SSH-RSA-SIGN Known Answer Test: Passed
mgd: SSH-ECDSA-SIGN Known Answer Test: Passed
mgd: KDF-IKE-V1 Known Answer Test: Passed
mgd: KDF-IKE-V2 Known Answer Test: Passed
mgd: Testing QuickSec KATS:
mgd: NIST 800-90 HMAC DRBG Known Answer Test: Passed
mgd: DES3-CBC Known Answer Test: Passed
mgd: HMAC-SHA1 Known Answer Test: Passed
mgd: HMAC-SHA2-224 Known Answer Test: Passed
mgd: HMAC-SHA2-256 Known Answer Test: Passed
mgd: HMAC-SHA2-384 Known Answer Test: Passed
mgd: HMAC-SHA2-512 Known Answer Test: Passed
mgd: AES-CBC Known Answer Test: Passed
mgd: AES-GCM Known Answer Test: Passed
mgd: SSH-RSA-ENC Known Answer Test: Passed
mgd: SSH-RSA-SIGN Known Answer Test: Passed
mgd: KDF-IKE-V1 Known Answer Test: Passed
mgd: KDF-IKE-V2 Known Answer Test: Passed
mgd: Testing SSH IPsec KATS:
mgd: NIST 800-90 HMAC DRBG Known Answer Test: Passed
mgd: DES3-CBC Known Answer Test: Passed
mgd: HMAC-SHA1 Known Answer Test: Passed
mgd: HMAC-SHA2-256 Known Answer Test: Passed
mgd: AES-CBC Known Answer Test: Passed
mgd: SSH-RSA-ENC Known Answer Test: Passed
mgd: SSH-RSA-SIGN Known Answer Test: Passed
mgd: KDF-IKE-V1 Known Answer Test: Passed
mgd: Testing file integrity:
mgd: File integrity Known Answer Test: Passed
mgd: Testing crypto integrity:
mgd: Crypto integrity Known Answer Test: Passed
mgd: Expect an exec Authentication error...
verexec: no fingerprint for file='/sbin/kats/cannot-exec' fsid=197 fileid=51404
gen=1 uid=0 pid=4119
mgd: /sbin/kats/run-tests: /sbin/kats/cannot-exec: Authentication error
mgd: FIPS Self-tests Passed

```



NOTE: The module implements cryptographic libraries and algorithms that are not utilized in the approved mode of operation.

CHAPTER 4

Configuring SSH and Console Connection

- [Configuring a System Login Message and Announcement on page 47](#)
- [Configuring SSH on the Evaluated Configuration on page 48](#)
- [Limiting the Number of User Login Attempts for SSH Sessions on page 49](#)

Configuring a System Login Message and Announcement

A login message appears before the user logs in and announcement appears after the user logs in. By default, no login message or announcement is displayed on the device.

To configure a system login message, use the following command:

```
[edit]
user@host# set system login message login-message-banner-text
```

To configure system announcement, use the following command:

```
[edit]
user@host# set system login announcement system-announcement-text
```



NOTE:

- If the message text contains any spaces, enclose it in quotation marks.
 - You can format the message using the following special characters:
 - \n—New line
 - \t—Horizontal tab
 - \'—Single quotation mark
 - \"—Double quotation mark
 - \\—Backslash
-

Related Documentation

- [Configuring SSH on the Evaluated Configuration on page 48](#)

Configuring SSH on the Evaluated Configuration

SSH is an allowed remote management interface in the evaluated configuration. This topic describes how to configure SSH on the device.

- Before you begin, log in with your root account on the device running Junos OS Release 18.1R1 and edit the configuration.

To configure SSH on the device:

1. Specify the permissible SSH host-key algorithms for the system services.

```
[edit ]
root@host# set system services ssh hostkey-algorithm ssh-ecdsa
root@host# set system services ssh hostkey-algorithm no-ssh-dss
root@host# set system services ssh hostkey-algorithm ssh-rsa
```

2. Specify the SSH key-exchange for Diffie-Hellman keys for the system services.

```
[edit ]
root@host#set system services ssh key-exchange dh-group14-sha1
root@host#set system services ssh key-exchange ecdh-sha2-nistp256
root@host#set system services ssh key-exchange ecdh-sha2-nistp384
root@host#set system services ssh key-exchange ecdh-sha2-nistp521
```

3. Specify all the permissible message authentication code algorithms for SSHv2.

```
[edit ]
root@host#set system services ssh macs hmac-sha1
root@host#set system services ssh macs hmac-sha2-256
root@host#set system services ssh macs hmac-sha2-512
```

4. Specify the ciphers allowed for protocol version 2.

```
[edit ]
root@host#set system services ssh ciphers aes128-cbc
root@host#set system services ssh ciphers aes256-cbc
root@host#set system services ssh ciphers aes128-ctr
root@host#set system services ssh ciphers aes256-ctr
root@host#set system services ssh ciphers aes192-cbc
root@host#set system services ssh ciphers aes192-ctr
```

Supported SSH hostkey algorithm:

| | |
|-----------|------------------------------------|
| ssh-ecdsa | Allow generation of ECDSA host-key |
| ssh-rsa | Allow generation of RSA host-key |

Supported SSH key-exchange algorithm:

| | |
|--------------------|---|
| dh-group14-sha1 | The RFC 4253 mandated group14 with SHA1 hash |
| ecdh-sha2-nistp256 | The EC Diffie-Hellman on nistp256 with SHA2-256 |
| ecdh-sha2-nistp384 | The EC Diffie-Hellman on nistp384 with SHA2-384 |
| ecdh-sha2-nistp521 | The EC Diffie-Hellman on nistp521 with SHA2-512 |

Supported MAC algorithm:

| | |
|---------------|---|
| hmac-sha1 | Hash-based MAC using Secure Hash Algorithm (SHA1) |
| hmac-sha2-256 | Hash-based MAC using Secure Hash Algorithm (SHA2) |
| hmac-sha2-512 | Hash-based MAC using Secure Hash Algorithm (SHA2) |

Supported SSH ciphers algorithm:

| | |
|------------|--|
| aes128-cbc | 128-bit AES with Cipher Block Chaining |
| aes128-ctr | 128-bit AES with Counter Mode |
| aes192-cbc | 192-bit AES with Cipher Block Chaining |
| aes192-ctr | 192-bit AES with Counter Mode |
| aes256-cbc | 256-bit AES with Cipher Block Chaining |
| aes256-ctr | 256-bit AES with Counter Mode |

Related Documentation

- [Limiting the Number of User Login Attempts for SSH Sessions on page 49](#)

Limiting the Number of User Login Attempts for SSH Sessions

An administrator may login remotely to a device through SSH. Administrator credentials are stored locally on the device. If the administrator presents a valid username and password, access to the Device under test (DUT) is granted. If the number of authentication attempts exceed the configured maximum, no authentication attempts are accepted for a configured time interval. When the interval expires, authentication attempts are again accepted.

You configure the amount of time the device gets locked after failed attempts. The amount of time in minutes before the user can attempt to log in to the device after being locked out due to the number of failed login attempts specified in the **tries-before-disconnect** statement. When a user fails to correctly login after the number of allowed attempts specified by the **tries-before-disconnect** statement, the user must wait the configured amount of minutes before attempting to log in to the device again. The **lockout-period** must be greater than zero. The range at which you can configure the **lockout-period** is one through 43,200 minutes.

```
[edit system login]
user@host# set retry-options lockout-period <number>
```

You can configure the device to limit the number of attempts to enter a password while logging through SSH. Using the following command, the connection.

```
[edit system login]
user@host# set retry-options tries-before-disconnect <number>
```

Here, **tries-before-disconnect** is the number of times a user can attempt to enter a password when logging in. The connection closes if a user fails to log in after the number specified. The range is from 2 through 10, and the default value is 3.

You can also configure a delay, in seconds, before a user can try to enter a password after a failed attempt.

```
[edit system login]
user@host# set retry-options backoff-threshold <number>
```

Here, **backoff-threshold** is the threshold for the number of failed login attempts before the user experiences a delay in being able to enter a password again. The range is from 1 through 3, and the default value is 2 seconds.

In addition, the device can be configured to specify the threshold for the number of failed attempts before the user experiences a delay in entering the password again.

```
[edit system login]
user@host# set retry-options backoff-factor <number>
```

Here, **backoff-factor** is the length of time, in seconds, before a user can attempt to log in after a failed attempt. The delay increases by the value specified for each subsequent attempt after the threshold. The range is from 5 through 10, and the default value is 5 seconds.

You can control user access through SSH. By configuring **ssh root-login deny**, you can ensure the root account remains active and continues to have local administrative privileges to the device even if other remote users are logged off.

```
[edit system ]
user@host# set services ssh root-login deny
```

**Related
Documentation**

- [Configuring SSH on the Evaluated Configuration on page 48](#)

CHAPTER 5

Configuration Statements

- [fips \(FIPS\) on page 51](#)
- [level \(FIPS\) on page 52](#)

fips (FIPS)

Syntax `fips {
 level level;
 }`

Hierarchy Level `[edit system]`

Release Information Statement introduced in Junos OS Release 18.1 for EX and QFX Series switches.

Description Configure Junos OS Federal Information Processing Standard (FIPS) mode features on a switch.

The remaining statements are explained separately.

Required Privilege Level `system`—To view this statement in the configuration.
 `system-control`—To add this statement to the configuration.

level (FIPS)

Syntax `level level;`

Hierarchy Level [edit system fips]

Release Information Statement introduced in Junos OS Release 18.1 for EX and QFX Series switches.

Description Set the level for the Junos OS Federal Information Processing Standards (FIPS) mode on the device. Setting the FIPS level to a value other than the default, 0 (zero), enables FIPS mode on the device.

Compared to non-FIPS mode, Junos OS in FIPS mode is a nonmodifiable operational environment with limitations.

Options *level*—FIPS level on a device, from level 1 (lowest) through level 4 (highest). At level 0 (the default), the device is in non-FIPS mode.

Range: 0 through 4



NOTE: To enable Junos OS in FIPS mode on an EX Series switch, set level to 1. Only level 1 is supported on the switches.

Required Privilege system—To view this statement in the configuration.

Level system-control—To add this statement to the configuration.

CHAPTER 6

Operational Commands

- request system zeroize (FIPS)

request system zeroize (FIPS)

| | |
|---------------------------------|---|
| Syntax | <code>request system zeroize</code> |
| Release Information | Command introduced in Junos OS Release 18.1 for EX and QFX Series switches. |
| Description | Erase and replace with zeros all user-created data from Routing Engines. |
| Options | none—Zeroize all Routing Engines in Junos OS in FIPS mode. You must confirm the request by typing yes to proceed. This command is restricted to Crypto Officers because the maintenance permission bit is one of the permission bits, along with secret and control , that distinguishes Crypto Officers from other FIPS users. |
| Required Privilege Level | maintenance |
| Related Documentation | <ul style="list-style-type: none">• Understanding Zeroization to Clear System Data for FIPS Mode on page 30• Zeroizing the System on page 32 |
| List of Sample Output | request system zeroize (FIPS) on page 54 |
| Output Fields | When you enter this command, you are provided feedback on the status of your request. |

Sample Output

request system zeroize (FIPS)

```
crypto-officer@switch:fips> request system zeroize
warning: System will be rebooted and may not boot without configuration
Erase all data, including configuration and log files? [yes, no] (no) yes
re0:
-----
warning: zeroizing re0
...
Rebooting after scrubbing memory...
...
```