



---

## Junos<sup>®</sup> OS

### Common Criteria and FIPS Evaluated Configuration Guide for MX240, MX480, MX960, MX2008, MX2010, MX2020, EX9204, EX9208, and EX9214 Series Devices

Release  
**18.1R3**



Modified: 2019-05-10

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® OS Common Criteria and FIPS Evaluated Configuration Guide for MX240, MX480, MX960, MX2008, MX2010, MX2020, EX9204, EX9208, and EX9214 Series Devices*

18.1R3

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 . . . . .	ix
	Documentation and Release Notes . . . . .	ix
	Documentation Conventions . . . . .	ix
	Documentation Feedback . . . . .	xi
	Requesting Technical Support . . . . .	xii
	Self-Help Online Tools and Resources . . . . .	xii
	Creating a Service Request with JTAC . . . . .	xiii
<b>Chapter 1</b>	<b>Overview . . . . .</b>	<b>15</b>
	Understanding the Common Criteria Evaluated Configuration . . . . .	15
	Understanding Common Criteria . . . . .	15
	Supported Platforms . . . . .	16
	Understanding Junos OS in FIPS Mode . . . . .	16
	About the Cryptographic Boundary on Your Router or Switch . . . . .	17
	How FIPS Mode Differs from Non-FIPS Mode . . . . .	17
	How Junos OS in FIPS Mode Differs from Junos-FIPS . . . . .	17
	Validated Version of Junos OS in FIPS Mode . . . . .	17
	Understanding Common Criteria and FIPS Terminology and Supported	
	Cryptographic Algorithms . . . . .	18
	Terminology . . . . .	18
	Supported Cryptographic Algorithms . . . . .	19
	Identifying Secure Product Delivery . . . . .	21
	Understanding Management Interfaces . . . . .	22
<b>Chapter 2</b>	<b>Configuring Administrative Credentials and Privileges . . . . .</b>	<b>23</b>
	Understanding the Associated Password Rules for an Authorized	
	Administrator . . . . .	23
	Configuring a Network Device Collaborative Protection Profile Authorized	
	Administrator . . . . .	25
<b>Chapter 3</b>	<b>Configuring Roles and Authentication Methods . . . . .</b>	<b>27</b>
	Understanding Roles and Services for Junos OS in Common Criteria and	
	FIPS . . . . .	27
	Crypto Officer Role and Responsibilities . . . . .	28
	FIPS User Role and Responsibilities . . . . .	29
	What Is Expected of All FIPS Users . . . . .	29
	Understanding the Operational Environment for Junos OS in FIPS Mode . . . . .	29
	Hardware Environment for Junos OS in FIPS Mode . . . . .	29
	Software Environment for Junos OS in FIPS Mode . . . . .	30
	Critical Security Parameters . . . . .	31

	Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode . . . . .	33
	Downloading Software Packages from Juniper Networks . . . . .	34
	Installing Software on a MX Series Routers and EX Series Ethernet switches with a Single Routing Engine (FIPS Mode) . . . . .	35
	Understanding Zeroization to Clear System Data for FIPS Mode . . . . .	37
	Why Zeroize? . . . . .	38
	When to Zeroize? . . . . .	38
	Zeroizing the System . . . . .	38
	Enabling FIPS Mode . . . . .	39
	Configuring Crypto Officer and FIPS User Identification and Access . . . . .	41
	Configuring Crypto Officer Access . . . . .	41
	Configuring FIPS User Login Access . . . . .	43
<b>Chapter 4</b>	<b>Configuring SSH and Console Connection . . . . .</b>	<b>45</b>
	Configuring a System Login Message and Announcement . . . . .	45
	Configuring SSH on the Evaluated Configuration for FIPS . . . . .	46
	Configuring SSH on the Evaluated Configuration for NDcPP . . . . .	47
	Limiting the Number of User Login Attempts for SSH Sessions . . . . .	49
	Configuring the time and date . . . . .	50
	Configuring the user session idle timeout . . . . .	50
	Configuring the SSH rekey values . . . . .	50
<b>Chapter 5</b>	<b>Configuring the Remote Syslog Server . . . . .</b>	<b>51</b>
	Syslog Server Configuration on a Linux System . . . . .	51
	Configuring Event Logging to a Local File . . . . .	51
	Configuring Event Logging to a Remote Server . . . . .	51
	Configuring Event Logging to a Remote Server when Initiating the Connection from the Remote Server . . . . .	52
<b>Chapter 6</b>	<b>Configuring Audit Log Options . . . . .</b>	<b>57</b>
	Configuring Audit Log Options in the Evaluated Configuration . . . . .	57
	Configuring Audit Log Options for MX240, MX480, MX960, MX2008, MX2010, MX2020, EX9204, EX9208, and EX9214 Devices . . . . .	57
	Sample Code Audits of Configuration Changes . . . . .	58
<b>Chapter 7</b>	<b>Configuring Event Logging . . . . .</b>	<b>63</b>
	Event Logging Overview . . . . .	63
	Configuring Event Logging to a Local File . . . . .	64
	Interpreting Event Messages . . . . .	64
	Logging Changes to Secret Data . . . . .	65
	Login and Logout Events Using SSH . . . . .	66
	Logging of Audit Startup . . . . .	66
<b>Chapter 8</b>	<b>Performing Self-Tests on a Device . . . . .</b>	<b>67</b>
	Understanding FIPS Self-Tests . . . . .	67
	Example: Configuring FIPS Self-Tests . . . . .	67
<b>Chapter 9</b>	<b>Operational Commands . . . . .</b>	<b>77</b>
	request system zeroize . . . . .	78
	request vmhost zeroize no-forwarding . . . . .	80

<b>Chapter 10</b>	<b>Protecting Against DoS Attacks . . . . .</b>	<b>83</b>
	Configuring Access Control Lists . . . . .	83
	Configuring Reverse Path Forwarding . . . . .	83



# List of Tables

	<b>About the Documentation</b> . . . . .	<b>ix</b>
	Table 1: Notice Icons . . . . .	x
	Table 2: Text and Syntax Conventions . . . . .	x
<b>Chapter 3</b>	<b>Configuring Roles and Authentication Methods</b> . . . . .	<b>27</b>
	Table 3: Critical Security Parameters . . . . .	31
<b>Chapter 6</b>	<b>Configuring Audit Log Options</b> . . . . .	<b>57</b>
	Table 4: Auditable Events . . . . .	60
<b>Chapter 7</b>	<b>Configuring Event Logging</b> . . . . .	<b>63</b>
	Table 5: Fields in Event Messages . . . . .	64





# About the Documentation

- Documentation and Release Notes on page ix
- Documentation Conventions on page ix
- Documentation Feedback on page xi
- Requesting Technical Support on page xii

## 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 x 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 x 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>
<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>

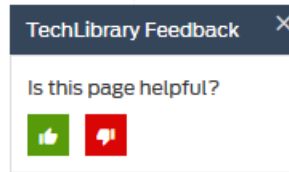
Table 2: Text and Syntax Conventions (continued)

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"><li>To configure a stub area, include the <b>stub</b> statement at the <b>[edit 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 &lt;default-metric <i>metric</i>&gt;;</b>
(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>  <b>(<i>string1</i>   <i>string2</i>   <i>string3</i>)</b>
# (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.	<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"><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/>.



## CHAPTER 1

# Overview

- Understanding the Common Criteria Evaluated Configuration on page 15
- Understanding Junos OS in FIPS Mode on page 16
- Understanding Common Criteria and FIPS Terminology and Supported Cryptographic Algorithms on page 18
- Identifying Secure Product Delivery on page 21
- Understanding Management Interfaces on page 22

## Understanding the Common Criteria Evaluated Configuration

---

This document describes the steps required to duplicate the configuration of the device running Junos OS when the device is evaluated. This is referred to as the evaluated configuration. The following list describes the standards to which the device has been evaluated:

- NDcPPv2—[https://www.commoncriteriaportal.org/files/ppfiles/PP\\_ND\\_V2.0.pdf](https://www.commoncriteriaportal.org/files/ppfiles/PP_ND_V2.0.pdf)
- FIPS—<https://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>

These documents are available at <https://www.niap-ccevs.org/Profile/PP.cfm?archived=1>.



**NOTE:** On MX240, MX480, MX960, MX2008, MX2010, MX2020, EX9204, EX9208, and EX9214 devices, Junos OS Release 18.1R1 is certified for Common Criteria with FIPS mode enabled on the devices.

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

## Understanding Common Criteria

Common Criteria for information technology is an international agreement signed by 28 countries that permits the evaluation of security products against a common set of standards. In the Common Criteria Recognition Arrangement (CCRA) at <http://www.commoncriteriaportal.org/ccra/>, the participants agree to mutually recognize evaluations of products performed in other countries. All evaluations are performed using a common methodology for information technology security evaluation.

For more information on Common Criteria, see <http://www.commoncriteriaportal.org/>.

Target of Evaluation (TOE) is a device or system subjected to evaluation based on Collaborative Protection Profile (cPP).

## Supported Platforms

For the features described in this document, the following platforms are supported:

- Routing Engine (RE-S-1800X4, RE-MX2000-1800X4, and REMX2K-1800-32G, or RE-S-X6-64G and REMX2K-X8-64G) and service PIC (MSMPC for VPNEP) have to be installed on MX240, MX480, MX960, MX2008, MX2010, and MX2020 to qualify NDcPPv2E.
- Routing Engine (EX9200-RE or EX9200-RE2) has to be installed on EX9204, EX9208, and EX9214 to qualify NDcPPv2E.

### Related Documentation

- [Identifying Secure Product Delivery on page 21](#)

## Understanding Junos OS in FIPS Mode

---

Federal Information Processing Standards (FIPS) 140-2 defines security levels for hardware and software that perform cryptographic functions. By meeting the applicable overall requirements within the FIPS standard, the Juniper Networks RE-S-1800X4, RE-MX2000-1800X4, REMX2K-1800-32G, RE-S-X6-64G, and REMX2K-X8-64G Routing Engines on Juniper Networks MX Series 3D Universal Edge Routers or EX9200-RE and EX9200-RE2 Routing Engines on 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 on the routers or switches from the Junos OS command-line interface (CLI).

The *Crypto Officer* enables FIPS mode in Junos OS Release 18.1R3 and sets up keys and passwords for the system and other *FIPS users*.



**BEST PRACTICE:** Be sure to verify the secure delivery of your router or switch and apply tamper-evident seals to its vulnerable ports.

- [About the Cryptographic Boundary on Your Router or Switch on page 17](#)
- [How FIPS Mode Differs from Non-FIPS Mode on page 17](#)
- [How Junos OS in FIPS Mode Differs from Junos-FIPS on page 17](#)
- [Validated Version of Junos OS in FIPS Mode on page 17](#)



## About the Cryptographic Boundary on Your Router or Switch

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



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

To physically secure the cryptographic module, all Juniper Networks routers or switches require a tamper-evident seal on the USB and mini-USB ports.

## 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 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.

## How Junos OS in FIPS Mode Differs from Junos-FIPS

*Junos OS in FIPS mode* is an operating mode of Junos OS that you enable from the Junos OS command-line interface (CLI). In contrast, the *Junos-FIPS image* is a separately downloadable Junos OS image available for Juniper Networks MX Series routers or EX Series Ethernet Switches.

Junos OS in FIPS mode is available only on the routers and switches that are running Junos OS Release 18.1R1 and later.

## 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 21](#)

## Understanding Common Criteria and FIPS Terminology and Supported Cryptographic Algorithms

---

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

- [Terminology on page 18](#)
- [Supported Cryptographic Algorithms on page 19](#)

### Terminology

**Common Criteria**—Common Criteria for information technology is an international agreement signed by 28 countries that permits the evaluation of security products against a common set of standards.

**Security Administrator**—For Common Criteria, user accounts in the TOE have the following attributes: user identity (user name), authentication data (password), and role (privilege). The Security Administrator is associated with the defined login class “security-admin”, which has the necessary permission set to permit the administrator to perform all tasks necessary to manage the Junos OS.

**NDcPP**—Collaborative Protection Profile for Network Devices, version 2.0, dated 05 May 2017.

**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 29](#).

**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/EX 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 Common Criteria and FIPS” on page 27](#).

**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 67](#).

**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



**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 on page 67](#)
- [Understanding Zeroization to Clear System Data for FIPS Mode on page 37](#)

---

## Identifying Secure Product Delivery

---

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

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

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

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

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

- Related Documentation**
- [Understanding the Common Criteria Evaluated Configuration on page 15](#)

## 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, and it is enabled by default on the device. The remote management protocols J-Web and Telnet are not available for use on the device.

- Related Documentation**
- [Understanding the Common Criteria Evaluated Configuration on page 15](#)

## CHAPTER 2

# Configuring Administrative Credentials and Privileges

- [Understanding the Associated Password Rules for an Authorized Administrator on page 23](#)
- [Configuring a Network Device Collaborative Protection Profile Authorized Administrator on page 25](#)

## Understanding the Associated Password Rules for an Authorized Administrator

---

The authorized administrator is associated with a defined login class, and the administrator is assigned with all permissions. Data is stored locally for fixed password authentication.



**NOTE:** We recommend that you not use control characters in passwords.

Use the following guidelines and configuration options for passwords and when selecting passwords for authorized administrator accounts. Passwords should be:

- Easy to remember so that users are not tempted to write it down.
- Changed periodically.
- Private and not shared with anyone.
- Contain a minimum of 10 characters. The minimum password length is 10 characters.

[edit]

```
administrator@host# set system login password minimum-length 10
```

- Include both alphanumeric and punctuation characters, composed of any combination of upper and lowercase letters, numbers, and special characters such as, “!”, “@”, “#”, “\$”, “%”, “^”, “&”, “\*”, “(”, and “)”. There should be at least a change in one case, one or more digits, and one or more punctuation marks.
- Contain character sets. Valid character sets include uppercase letters, lowercase letters, numbers, punctuation, and other special characters.

[edit]

```
administrator@host# set system login password change-type character-sets
```

- Contain the minimum number of character sets or character set changes. The minimum number of character sets required in plain-text passwords in Junos FIPS is 2.

```
[edit]  
administrator@host# set system login password minimum-changes 2
```



**NOTE:** The hashing algorithm for user passwords can be either SHA256 or SHA512 (SHA512 is the default hashing algorithm).

```
[edit]  
administrator@host# set system login password format sha256
```



**NOTE:** The device supports ECDSA (P-256, P-384, and P-521) and RSA (2048, 3072, and 4092 modulus bit length) key-types.

Weak passwords are:

- Words that might be found in or exist as a permuted form in a system file such as `/etc/passwd`.
- The hostname of the system (always a first guess).
- Any words appearing in a dictionary. This includes dictionaries other than English, and words found in works such as Shakespeare, Lewis Carroll, Roget's Thesaurus, and so on. This prohibition includes common words and phrases from sports, sayings, movies, and television shows.
- Permutations on any of the above. For example, a dictionary word with vowels replaced with digits (for example f00t) or with digits added to the end.
- Any machine-generated passwords. Algorithms reduce the search space of password-guessing programs and so should not be used.

Strong reusable passwords can be based on letters from a favorite phrase or word, and then concatenated with other, unrelated words, along with additional digits and punctuation.

If the limit on consecutive invalid passwords is reached, the user account becomes locked. It will automatically unlock after the configured lockout time expires, or the account can be manually unlocked using the following command:

```
administrator@host# clear system login lockout user username
```



**NOTE:** Passwords should be changed periodically.



**Related Documentation** • [Identifying Secure Product Delivery on page 21](#)

## Configuring a Network Device Collaborative Protection Profile Authorized Administrator

An account for **root** is always present in a configuration and is not intended for use in normal operation. In the evaluated configuration, the **root** account is restricted to the initial installation and configuration of the evaluated device.

An NDcPPv2 authorized administrator must have all permissions, including the ability to change the router configuration.

To configure an authorized administrator:



**NOTE:** When the **log-key-changes** configuration statement is enabled and committed (with the **commit** command in configuration mode), Junos OS logs the changes to the set of authorized SSH keys for each user (including the keys that were added or removed). Junos OS logs the differences since the last time the **log-key-changes** configuration statement was enabled. If the **log-key-changes** configuration statement was never enabled, then Junos OS logs all the authorized SSH keys.

1. Create a login class named **security-admin** with all permissions.

```
[edit]
root@host# set system login class security-admin permissions all
```

2. Configure the hashed algorithm for plain-text passwords as **sha512**.

```
[edit]
root@host# set system login password format sha512
```

3. Commit the changes.

```
[edit]
root@host# commit
```

4. Define your NDcPPv2E user authorized administrator.

```
[edit]
root@host# set system login user NDcPPv2E-user full-name
Common-Criteria-NDcPPv2E-Authorized-Administrator class security-admin
authentication encrypted-password <password>
```

5. Load an SSH key file that was previously generated using **ssh-keygen**. This command loads RSA (SSH version 2), or ECDSA (SSH version 2).

```
[edit]
root@host#set system root-authentication load-key-file url:filename
```

6. Set the log-key-changes configuration statement to log when SSH authentication keys are added or removed.

```
[edit]
root@host#set system services ssh log-key-changes
```

7. Commit the changes.

```
[edit]
root@host# commit
```



.....

**NOTE:** The root password should be reset following the change to sha256 / sha512 for the password storage format. This ensures the new password is protected using a sha256 / sha512 hash. To reset the root password, use `set system root-authentication plain-text-password password` command, and confirm the new password when prompted.

.....

**Related  
Documentation**

- [Understanding the Associated Password Rules for an Authorized Administrator on page 23](#)

## CHAPTER 3

# Configuring Roles and Authentication Methods

- [Understanding Roles and Services for Junos OS in Common Criteria and FIPS on page 27](#)
- [Understanding the Operational Environment for Junos OS in FIPS Mode on page 29](#)
- [Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode on page 33](#)
- [Downloading Software Packages from Juniper Networks on page 34](#)
- [Installing Software on a MX Series Routers and EX Series Ethernet switches with a Single Routing Engine \(FIPS Mode\) on page 35](#)
- [Understanding Zeroization to Clear System Data for FIPS Mode on page 37](#)
- [Zeroizing the System on page 38](#)
- [Enabling FIPS Mode on page 39](#)
- [Configuring Crypto Officer and FIPS User Identification and Access on page 41](#)

## Understanding Roles and Services for Junos OS in Common Criteria and FIPS

For Common Criteria, user accounts in the TOE have the following attributes: user identity (user name), authentication data (password) and role (privilege). The Security Administrator is associated with the defined login class “security-admin”, which has the necessary permission set to permit the administrator to perform all tasks necessary to manage Junos OS. Administrative users (Security Administrator) must provide unique identification and authentication data before any administrative access to the system is granted.

Security Administrator roles and responsibilities are as follows:

1. Security Administrator can administer the TOE locally and remotely.
2. Create, modify, delete administrator accounts, including configuration of authentication failure parameters.
3. Re-enable an Administrator account.
4. Responsible for the configuration and maintenance of cryptographic elements related to the establishment of secure connections to and from the evaluated product.

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 on page 28](#)
- [FIPS User Role and Responsibilities on page 29](#)
- [What Is Expected of All FIPS Users on page 29](#)

## Crypto Officer Role and Responsibilities

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



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

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



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

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

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

## FIPS User Role and Responsibilities

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

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

## What Is Expected of All FIPS Users

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

All FIPS users must:

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

### Related Documentation

- [Zeroizing the System on page 38](#)

---

## Understanding the Operational Environment for Junos OS in FIPS Mode

A Juniper Networks router or switch running the Juniper Networks Junos operating system (Junos OS) in FIPS mode forms a special type of hardware and software operational environment that is different from the environment of a router or switch in non-FIPS mode:

- [Hardware Environment for Junos OS in FIPS Mode on page 29](#)
- [Software Environment for Junos OS in FIPS Mode on page 30](#)
- [Critical Security Parameters on page 31](#)

## 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. There are two types of hardware with cryptographic boundaries in Junos OS in FIPS mode: one for each Routing Engine and one for entire chassis which

includes encryption services PIC (MS-MPC). Each component forms a separate cryptographic module. Communications involving CSPs between these secure environments must take place using encryption.

The Junos OS in FIPS mode hardware environment has limitations that apply to cryptographic boundaries. The FPC slot might have to be secured with a tamper-evident seal. For FIPS Level 1 operation, the Routing Engine must be sealed into the chassis by using tamper-evident labels. On some models, tamper-evident labels must be applied to other components as well. See the FIPS Level 1 Label Installation Instructions for details. The label kit must be ordered separately and the labels applied according to the instructions included in the kit.

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

## Software Environment for Junos OS in FIPS Mode

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

FIPS mode on MX Series routers and EX Series Ethernet switches is available in Junos OS Release 18.1R1 and later. The Junos OS in FIPS mode software environment is established after the Crypto Officer successfully enables FIPS mode on a router or switch. The Junos OS Release 18.1R1 image that includes FIPS mode is available on the Juniper Networks website and can be installed on a functioning router or switch.

For FIPS 140-2 compliance, we recommend that you delete all user-created files and data by *zeroizing* the device before enabling FIPS mode.

Operating the router or switch at FIPS Level 1 requires the use of tamper-evident labels to seal the Routing Engines into the chassis.

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 router or switch 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 router or switch or Routing Engine as a cryptographic module.

Table 3 on page 31 lists CSPs on routers running Junos OS.

**Table 3: Critical Security Parameters**

CSP	Description	Zeroization Method	Use
SSH-2 private host key	ECDSA / RSA key used to identify the host, generated the first time SSH is configured.	Zeroize command.	Used to identify the host.
SSH-2 session key	Session key used with SSH-2. and as a Diffie-Hellman private key.  Encryption: 3DES (FIPS only), AES-128, AES-192 (FIPS only), AES-256.  MACs: HMAC-SHA-1, HMAC SHA-2-256, HMAC SHA2-512.  Key exchange: ECDH-sha2-nistp256, ECDH-sha2-nistp384, and ECDH-sha2-nistp521.	Power cycle and terminate session.	Symmetric key used to encrypt data between host and client.
User authentication key	Hash of the user's password: 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.

**Table 3: Critical Security Parameters (continued)**

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



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

Local passwords are hashed with the SHA256 or SHA512 algorithm. Password recovery is not possible in Junos OS in FIPS mode. Junos OS in FIPS mode cannot boot into single-user mode without the correct root password.

**Related Documentation**

- [Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode on page 33](#)
- [Understanding Zeroization to Clear System Data for FIPS Mode on page 37](#)



## 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 on page 29](#)

---

## 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 18.1R3-S3



**NOTE:** For MX RE-S-1800X4, RE-MX2000-1800X4, and REMX2K-1800-32G download `junos-install-mx-x86-64-18.1R3.3.tgz` and for MX RE-S-X6-64G and REMX2K-X8-64G download `junos-vmhost-install-mx-x86-64-18.1R3.3.tgz`.

For EX9200-RE download `junos-install-ex92xx-x86-64-18.1R3-S3.4.tgz` and for EX9200-RE2 download `junos-vmhost-install-ex92xx-x86-64-18.1R3-S3.4.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://www.juniper.net/registration/Register.jsp>.

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://www.juniper.net/support/downloads/junos.html>
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 a MX Series Routers and EX Series Ethernet switches with a Single Routing Engine (FIPS Mode)

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

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

1. Download the software package as described in [“Downloading Software Packages from Juniper Networks” on page 34](#).
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.
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 device:

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

```
user@switch> request vmhost 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, `junos-vmhost-install-ex92xx-x86-64-18.1R1.tgz`.
  - `ftp://hostname/pathname/package.tgz`
  - `http://hostname/pathname/package.tgz`

6. Reboot the device to load the installation:

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

```
user@switch> 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. The load fails if the embedded certificates in the firmware image are not valid. If you installed the Junos FIPS mode package, verify that the FIPS mode utilities are present—as shown in the following example:

```
user@host> show version
Model: ex9204
Junos: 18.1R2-S3.3
JUNOS OS Kernel 64-bit [20180214.102357_fbsd-builder_stable_11]
JUNOS OS libs [20180214.102357_fbsd-builder_stable_11]
JUNOS OS runtime [20180214.102357_fbsd-builder_stable_11]
JUNOS OS time zone information [20180214.102357_fbsd-builder_stable_11]
JUNOS network stack and utilities [20180216.215829_builder_junos_181_r1]
JUNOS libs [20180216.215829_builder_junos_181_r1]
JUNOS OS libs compat32 [20180214.102357_fbsd-builder_stable_11]
JUNOS OS 32-bit compatibility [20180214.102357_fbsd-builder_stable_11]
JUNOS libs compat32 [20180216.215829_builder_junos_181_r1]
JUNOS runtime [20180216.215829_builder_junos_181_r1]
Junos vmguest package [20180216.215829_builder_junos_181_r1]
JUNOS sflow mx [20180216.215829_builder_junos_181_r1]
JUNOS py extensions [20180216.215829_builder_junos_181_r1]
JUNOS py base [20180216.215829_builder_junos_181_r1]
JUNOS OS vmguest [20180214.102357_fbsd-builder_stable_11]
JUNOS OS crypto [20180214.102357_fbsd-builder_stable_11]
JUNOS Web Management Platform Package [20180216.215829_builder_junos_181_r1]
JUNOS mx libs compat32 [20180216.215829_builder_junos_181_r1]
JUNOS mx runtime [20180216.215829_builder_junos_181_r1]
JUNOS common platform support [20180216.215829_builder_junos_181_r1]
JUNOS mtx network modules [20180216.215829_builder_junos_181_r1]
JUNOS modules [20180216.215829_builder_junos_181_r1]
JUNOS mx modules [20180216.215829_builder_junos_181_r1]
JUNOS mx libs [20180216.215829_builder_junos_181_r1]
JUNOS mtx Data Plane Crypto Support [20180216.215829_builder_junos_181_r1]
JUNOS daemons [20180216.215829_builder_junos_181_r1]
JUNOS mx daemons [20180216.215829_builder_junos_181_r1]
JUNOS Services URL Filter package [20180216.215829_builder_junos_181_r1]
JUNOS Services TLB Service PIC package [20180216.215829_builder_junos_181_r1]
JUNOS Services Telemetry [20180216.215829_builder_junos_181_r1]
JUNOS Services SSL [20180216.215829_builder_junos_181_r1]
JUNOS Services SOFTWARE [20180216.215829_builder_junos_181_r1]
JUNOS Services Stateful Firewall [20180216.215829_builder_junos_181_r1]
JUNOS Services RPM [20180216.215829_builder_junos_181_r1]
JUNOS Services PCEF package [20180216.215829_builder_junos_181_r1]
JUNOS Services NAT [20180216.215829_builder_junos_181_r1]
JUNOS Services Mobile Subscriber Service Container package
[20180216.215829_builder_junos_181_r1]
JUNOS Services MobileNext Software package
[20180216.215829_builder_junos_181_r1]
JUNOS Services Logging Report Framework package
[20180216.215829_builder_junos_181_r1]
JUNOS Services LL-PDF Container package
[20180216.215829_builder_junos_181_r1]
JUNOS Services Jflow Container package [20180216.215829_builder_junos_181_r1]
JUNOS Services Deep Packet Inspection package
[20180216.215829_builder_junos_181_r1]
JUNOS Services IPSec [20180216.215829_builder_junos_181_r1]
JUNOS Services IDS [20180216.215829_builder_junos_181_r1]
JUNOS IDP Services [20180216.215829_builder_junos_181_r1]
```

```

JUNOS Services HTTP Content Management package
[20180216.215829_builder_junos_181_r1]
JUNOS Services Crypto [20180216.215829_builder_junos_181_r1]
JUNOS Services Captive Portal and Content Delivery Container package
[20180216.215829_builder_junos_181_r1]
JUNOS Services COS [20180216.215829_builder_junos_181_r1]
JUNOS AppId Services [20180216.215829_builder_junos_181_r1]
JUNOS Services Application Level Gateways
[20180216.215829_builder_junos_181_r1]
JUNOS Services ACL Container package [20180216.215829_builder_junos_181_r1]
JUNOS SDN Software Suite [20180216.215829_builder_junos_181_r1]
JUNOS Extension Toolkit [20180216.215829_builder_junos_181_r1]
JUNOS jplatform ex92xx [20180216.215829_builder_junos_181_r1]
JUNOS Packet Forwarding Engine Support (wrlinux)
[20180216.215829_builder_junos_181_r1]
JUNOS Packet Forwarding Engine Support (MX/EX92XX Common)
[20180216.215829_builder_junos_181_r1]
JUNOS Packet Forwarding Engine Support (M/T Common)
[20180216.215829_builder_junos_181_r1]
JUNOS Packet Forwarding Engine Support (MX Common)
[20180216.215829_builder_junos_181_r1]
JUNOS jfirmware [20180216.215829_builder_junos_181_r1]
JUNOS Online Documentation [20180216.215829_builder_junos_181_r1]
JUNOS jail runtime [20180214.102357_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

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

The Crypto Officer initiates the zeroization process by entering the **request system zeroize** operational command for RE-S-1800X4, RE-MX2000-1800X4, and REMX2K-1800-32G, or EX9200-RE from the CLI after enabling FIPS mode. Use of this command is restricted to the Crypto Officer. (To zeroize the system *before* enabling FIPS mode, use the **request system zeroize** command to completely wipe-out older CSPs and scrub memory.)

For RE-S-X6-64G and REMX2K-X8-64G, or EX9200-RE2, Crypto Officer initiates the zeroization process by entering the **request vmhost zeroize no-forwarding** operational command.



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

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

- [Why Zeroize? on page 38](#)
- [When to Zeroize? on page 38](#)

## Why Zeroize?

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

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

## When to Zeroize?

As Crypto Officer, perform zeroization in the following situations:

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



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

**Related Documentation**

- [Zeroizing the System on page 38](#)

## Zeroizing the System

---

To zeroize your device, follow the below procedure:

1. For RE-S-1800X4, RE-MX2000-1800X4, and REMX2K-1800-32G, or EX9200-RE, 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) yes
re0:
```

For RE-S-X6-64G and REMX2K-X8-64G, or EX9200-RE2, from the CLI, enter

```
root@switch> request vmhost zeroize no-forwarding
```

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

```
re0:
```

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
...
...
```

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 39](#)
- [Understanding Zeroization to Clear System Data for FIPS Mode on page 37](#)

## Enabling FIPS Mode

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

As Crypto Officer, you must establish a root password conforming to the FIPS password requirements in [“Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode” on page 33](#). When you enable FIPS mode in Junos OS on the router or switch, 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 37](#) 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 18.1-20180131.0 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.

5. Install **fips-mode** package needed for Routing Engine KATS.

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

6. Install **jpfe-fips** package needed for MS-MPC line card KATS. (This is only for MX router having MS-MPC line card).

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

7. For MX Series devices,

- Configure chassis boundary fips by setting **set system fips chassis level 1** and **commit**.

For EX and MX devices,

- Configure fips by setting **set systems fips 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.

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

```
[edit]  
root@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
root@hostname# request system reboot
root@hostname# request vmhost reboot
```

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

```
root@hostname:fips>
```

#### Related Documentation

- [Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode on page 33](#)
- For more information about the root password and root logins, see the *Junos OS System Basics Configuration Guide*.

## Configuring Crypto Officer and FIPS User Identification and Access

Crypto 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 Access on page 41](#)
- [Configuring FIPS User Login Access on page 43](#)

### Configuring Crypto Officer Access

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

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

To configure login access for a Crypto Officer:

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

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

2. Name the user **crypto-officer** and assign the Crypto Officer a user ID (for example, **6400**, which must be a unique number associated with the login account in the range of 100 through 64000) and a class (for example, **super-user**). When you assign the class, you assign the permissions—for example, **secret**, **security**, **maintenance**, and **control**.

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

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

For example:

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

- Following the guidelines in [“Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode” on page 33](#), assign the Crypto Officer a plain-text password for login authentication. Set the password by typing a password after the prompts **New password** and **Retype new password**.

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

For example:

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

- Optionally, display the configuration:

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

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

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

Otherwise, go on to [“Configuring FIPS User Login Access” on page 43](#).

## Configuring FIPS User Login Access

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

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

To configure login access for a FIPS user:

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

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

2. Give the user, a username, and assign the user a user ID (for example, **6401**, which must be a unique number in the range of 1 through 64000) and a class. 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]
root@host:fips# set system login user username uid value class read-only
```

3. Following the guidelines in “[Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode](#)” on page 33, assign the FIPS user a plain-text password for login authentication. Set the password by typing a password after the prompts **New password** and **Retype new password**.

```
[edit]
root@host:fips# set system login user username uid value class read-only authentication
(plain-text-password | encrypted-password)
```

4. Optionally, display the configuration:

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

```
}  
}
```

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

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

**Related  
Documentation**

- [Understanding Roles and Services for Junos OS in Common Criteria and FIPS on page 27](#)

# Configuring SSH and Console Connection

- [Configuring a System Login Message and Announcement on page 45](#)
- [Configuring SSH on the Evaluated Configuration for FIPS on page 46](#)
- [Configuring SSH on the Evaluated Configuration for NDcPP on page 47](#)
- [Limiting the Number of User Login Attempts for SSH Sessions on page 49](#)

## Configuring a System Login Message and Announcement

---

A system login message appears before the user logs in and a system login 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 through console or management interface, 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

## Configuring SSH on the Evaluated Configuration for FIPS

---

SSH through remote management interface allowed in the evaluated configuration. This topic describes how to configure SSH through remote management. Note that the ciphers permitted for NDcPP are more restrictive than those for FIPS. For NDcPP conformance, use the preceding section to configure SSH.

The following algorithms that needs to be configured to validate SSH for FIPS.

To configure SSH on the DUT:

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

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

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

```
[edit]
user@host#set system services ssh key-exchange ecdh-sha2-nistp256
user@host#set system services ssh key-exchange ecdh-sha2-nistp384
user@host#set system services ssh key-exchange ecdh-sha2-nistp521
```

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

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

4. Specify the ciphers allowed for protocol version 2.

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

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 MACs 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

## Configuring SSH on the Evaluated Configuration for NDcPP

SSH through remote management interface allowed in the evaluated configuration. This topic describes how to configure SSH for remote management of TOE. The following algorithms that needs to be configured to validate SSH for NDcPP.

To configure SSH on the TOE:

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

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

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

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

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

```
[edit]
user@host#set system services ssh macs hmac-sha1
```

```
user@host#set system services ssh macs hmac-sha2-256
user@host#set system services ssh macs hmac-sha2-512
```

4. Specify the ciphers allowed for protocol version 2.

```
[edit]
user@host#set system services ssh ciphers aes128-cbc
user@host#set system services ssh ciphers aes256-cbc
user@host#set system services ssh ciphers aes128-ctr
user@host#set system services ssh ciphers aes256-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 MACs 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
aes256-cbc	256-bit AES with Cipher Block Chaining
aes256-ctr	256-bit AES with Counter Mode



## 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 remote administrator presents a valid username and password, access to the TOE is granted. If the credentials are invalid, the TOE allows the authentication to be retried after an interval that starts after 1 second and increases exponentially. 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 1 through 10, and the default value is 10.

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. Use the **backoff-factor** option to specify the length of the delay in seconds. 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 TOE even if other remote users are logged off.

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

The SSH2 protocol provides secure terminal sessions utilizing the secure encryption. The SSH2 protocol enforces running the key-exchange phase and changing the encryption and integrity keys for the session. Key exchange is done periodically, after specified seconds or after specified bytes of data have passed over the connection. You can configure thresholds for SSH rekeying, FCS\_SSHS\_EXT.1.8 and FCS\_SSHC\_EXT.1.8. The TSF ensures that within the SSH connections the same session keys are used for a threshold of no longer than one hour, and no more than one gigabyte of the transmitted data. When either of the thresholds are reached, a rekey must be performed.

## Configuring the time and date

To configure a system date and time, use the following command:

```
[edit]
user@host# set date YYYYMMDDHHMM.ss
```

## Configuring the user session idle timeout

To configure the idle timeout for a user session, use the following command:

```
[edit]
user@host# set system login idle-timeout minutes
```

## Configuring the SSH rekey values

Optionally specify the number of minutes or maximum amount of data before a rekey is forced on a session. The time limit may not be set higher than one hour, and the data limit may not be set higher than one gigabyte.

```
[edit system services ssh]
user@host# set rekey time-limit minutes
user@host# set rekey data-limit bytes
```

## CHAPTER 5

# Configuring the Remote Syslog Server

- [Syslog Server Configuration on a Linux System on page 51](#)

## Syslog Server Configuration on a Linux System

---

A secure Junos OS environment requires auditing of events and storing them in a local audit file. The recorded events are simultaneously sent to an external syslog server. A syslog server receives the syslog messages streamed from the router. The syslog server must have an SSH client with NETCONF support configured to receive the streamed syslog messages.

The NDcPP logs capture the events, few of them are listed below:

- Committed changes
- Login and logout of users
- Failure to establish an SSH session
- Establishment or termination of an SSH session
- Changes to the system time

## Configuring Event Logging to a Local File

Configure audit information to be stored in a local file on the device along with the level of detail using the "syslog" statement. The following must be used to ensure all events detailed in the NDcPP are logged and are stored in a local file named Audit\_file in the following example:

```
[edit system]
syslog {
  file Audit_file {
    any any;
  }
}
```

## Configuring Event Logging to a Remote Server

Configure the export of audit information to a secure, remote server by setting up an event trace monitor that sends event log messages by using NETCONF over SSH to the

remote system event logging server. The following procedures show the configuration needed to send system log messages to a secure external server by using NETCONF over SSH.

## Configuring Event Logging to a Remote Server when Initiating the Connection from the Remote Server

The following procedure describes the steps to configure event logging to a remote server when the SSH connection to the TOE is initiated from the remote system log server.

1. Generate an RSA public key on the remote syslog server.

```
$ ssh-keygen -b 2048 -t rsa -C 'syslog-monitor key pair' -f ~/.ssh/syslog-monitor
```

You will be prompted to enter the desired passphrase. The storage location for the **syslog-monitor** key pair is displayed.

2. On the TOE, create a class named **monitor** that has permission to trace events.

```
[edit]
user@host# set system login class monitor permissions trace
```

3. Create a user named **syslog-mon** with the class **monitor**, and with authentication that uses the **syslog-monitor** key pair from the key pair file located on the remote syslog server.

```
[edit]
user@host# set system login user syslog-mon class monitor authentication ssh-rsa
"ssh-rsa xxxxx syslog-monitor key pair"
```

4. Set up NETCONF with SSH.

```
[edit]
user@host# set system services netconf ssh
```

5. Configure syslog to log all the messages at */var/log/Audit\_file*.

```
[edit]
user@host# set system syslog file Audit_file any any
user@host# commit
```

6. On the remote system log server, start up the SSH agent. The start up is required to simplify the handling of the **syslog-monitor** key.

```
$ eval `ssh-agent`
```

7. On the remote syslog server, add the **syslog-monitor** key pair to the SSH agent.

```
$ ssh-add ~/.ssh/syslog-monitor
```

You will be prompted to enter the desired passphrase. Enter the same passphrase used in Step 1.

8. After logging in to the **external\_syslog\_server** session, establish a tunnel to the device and start NETCONF.

```
$ ssh syslog-mon@NDcPP_TOE -s netconf > test.out
```

9. After NETCONF is established, configure a system log events message stream. This RPC will cause the NETCONF service to start transmitting messages over the SSH connection that is established.

```
<rpc><get-syslog-events><stream>messages</stream></get-syslog-events></rpc>
```

10. The examples for syslog messages are listed below. Monitor the event log generated for admin actions on TOE as received on the syslog server. Examine the traffic that passes between the audit server and the TOE, observing that these data are not viewed during this transfer, and that they are successfully received by the audit server. Match the logs between local event and the remote event logged in a syslog server and record the particular software (such as name, version, and so on) used on the audit server during testing.

The following output shows test log results for syslog server.

```
host@ssh-keygen -b 2048 -t rsa -C 'syslog-monitor key pair' -f
~/.ssh/syslog-monitor
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/host/.ssh/syslog-monitor.
Your public key has been saved in /home/host/.ssh/syslog-monitor.pub.
The key fingerprint is:
ef:75:d7:68:c5:ad:8d:6f:5e:7a:7e:9b:3d:f1:4d:3f syslog-monitor key pair
The key's randomart image is:
+--[ RSA 2048 ]-----+
|
|
|
|          ..|
|      S      +|
|      .      Bo|
|      . . *.X|
|      . . o E@|
|      .      .BX|
+-----+
[host@nms5-vm-linux2 ~]$ cat /home/host/.ssh/syslog-monitor.pub
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQCrUREJUBpjwAoIgRrGy9zgt+
D2pikk3Q/Wdf8I5vr+njeqJhCx2bUAKrRbYXNILQQAzb7kLfi/8TqqL
eon4HOP2e6oCSorKdx/GrOTzLONL4fh0EyuSAk8bs5JuwWNBuokV025
```

```
gZpGFsBusGnlj6wqqJ/sjFsMmfxyCkbY+pUWb8m1/A9Yj0FT+6esw+9S
tF6Gbg+VpbYYk/Oday4z+z7tQHRFSrxj2G92ao1iVDBLJparEMbc8w
LdSUDxmgBTM2oad0mm+kreBUQjrmr6775RJn9H9YwIxK0xGm4SFnx/V14
R+lZ9RqmKH2wodIEM34K0wXEHZAzNZ01oLmaAVqT
syslog-monitor key pair
[host@nms5-vm-linux2 ~]$ eval `ssh-agent`
Agent pid 1453
[host@nms5-vm-linux2 ~]$ ssh-add ~/.ssh/syslog-monitor
Enter passphrase for /home/host/.ssh/syslog-monitor:
Identity added: /home/host/.ssh/syslog-monitor (/home/host/.ssh/syslog-monitor)
```

```
host@nms5-vm-linux2 ~]$ ssh syslog-mon@starfire -s netconf > test.out
host@nms5-vm-linux2 ~]$ cat test.out
this is NDcPP test device

<!-- No zombies were killed during the creation of this user interface --
<!-- user syslog-mon, class j-monitor --><hello>
  <capabilities>
    <capability>urn:ietf:params:xml:ns:netconf:base:1.0</capability>

  <capability>urn:ietf:params:xml:ns:netconf:capability:candidate:1.0</capability>

  <capability>urn:ietf:params:xml:ns:netconf:capability:confirmed-commit:1.0</capability>

    <capability>urn:ietf:params:xml:ns:netconf:capability:validate:1.0</capability>

  <capability>urn:ietf:params:xml:ns:netconf:capability:url:1.0?protocol=http,ftp,file</capability>

    <capability>http://xml.juniper.net/netconf/junos/1.0</capability>
    <capability>http://xml.juniper.net/dmi/system/1.0</capability>
  </capabilities>
  <session-id4129/session-id>
</hello>
]]>]]>
```

The following output shows event logs generated on the TOE that are received on the syslog server.

```
Jan 20 17:04:51 starfire sshd[4182]: error: Could not load host key:
/etc/ssh/ssh_host_dsa_key
Jan 20 17:04:51 starfire sshd[4182]: error: Could not load host key:
/etc/ssh/ssh_host_ecdsa_key
Jan 20 17:04:53 starfire sshd[4182]: Accepted password for sec-admin from
10.209.11.24 port 55571 ssh2
Jan 20 17:04:53 starfire mgd[4186]: UI_AUTH_EVENT: Authenticated user 'sec-admin'
at permission level 'j-administrator'
Jan 20 17:04:53 starfire mgd[4186]: UI_LOGIN_EVENT: User 'sec-admin' login, class
'j-administrator' [4186], ssh-connection '10.209.11.24 55571 10.209.14.92 22',
client-mode 'cli'
```

The following output shows that the local syslogs and remote syslogs received are similar.

```
Local : an 20 17:09:30 starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation
in progress: Redundancy interface management process checking new configuration
Jan 20 17:09:30 starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/rdd'
Jan 20 17:09:30 starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child
'/usr/sbin/rdd', PID 4317, status 0
Jan 20 17:09:30 starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in
progress: Dynamic flow capture service checking new configuration
Jan 20 17:09:30 starfire mgd[4186]: UI_CHILD_START: Starting child
'/usr/sbin/dfcd'
Jan 20 17:09:30 starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child
'/usr/sbin/dfcd', PID 4318, status 0
Jan 20 17:09:30 starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in
progress: Connectivity fault management process checking new configuration
Jan 20 17:09:30 starfire mgd[4186]: UI_CHILD_START: Starting child
'/usr/sbin/cfmd'
Jan 20 17:09:30 starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child
'/usr/sbin/cfmd', PID 4319, status 0
Jan 20 17:09:30 starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in
progress: Layer 2 address flooding and learning process checking new configuration
Jan 20 17:09:30 starfire mgd[4186]: UI_CHILD_START: Starting child
'/usr/sbin/l2ald'
Jan 20 17:09:30 starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child
'/usr/sbin/l2ald', PID 4320, status 0
Jan 20 17:09:30 starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in
progress: Layer 2 Control Protocol process checking new configuration
Jan 20 17:09:30 starfire mgd[4186]: UI_CHILD_START: Starting child
'/usr/sbin/l2cpd'
Jan 20 17:09:30 starfire l2cp[4321]: Initializing PNAC state machines
Jan 20 17:09:30 starfire l2cp[4321]: Initializing PNAC state machines complete
Jan 20 17:09:30 starfire l2cp[4321]: Initialized 802.1X module and state
machinesJan 20 17:09:30 starfire l2cp[4321]: Read access profile () config
Jan 20 17:09:30 starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child
'/usr/sbin/l2cpd', PID 4321, status 0
Jan 20 17:09:30 starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in
progress: Multicast Snooping process checking new configuration
Jan 20 17:09:30 starfire mgd[4186]: UI_CHILD_START: Starting child
'/usr/sbin/mcsnoopd'
Jan 20 17:09:30 starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child
'/usr/sbin/mcsnoopd', PID 4325, status 0
Jan 20 17:09:30 starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in
progress: commit wrapup...
Jan 20 17:09:30 starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in
progress: activating '/var/etc/ntp.conf'
Jan 20 17:09:30 starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in
progress: start ffp activate
Jan 20 17:09:30 starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/ffp'
Jan 20 17:09:30 starfire ffp[4326]: "dynamic-profiles": No change to
profiles.....
```

```
Remote : an 20 17:09:30 starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation
in progress: Redundancy interface management process checking new configuration
Jan 20 17:09:30 starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/rdd'
Jan 20 17:09:30 starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child
'/usr/sbin/rdd', PID 4317, status 0
Jan 20 17:09:30 starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in
progress: Dynamic flow capture service checking new configuration
```

```
Jan 20 17:09:30 starfire mgd[4186]: UI_CHILD_START: Starting child
'/usr/sbin/dfcd'
Jan 20 17:09:30 starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child
'/usr/sbin/dfcd', PID 4318, status 0
Jan 20 17:09:30 starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in
progress: Connectivity fault management process checking new configuration
Jan 20 17:09:30 starfire mgd[4186]: UI_CHILD_START: Starting child
'/usr/sbin/cfmd'
Jan 20 17:09:30 starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child
'/usr/sbin/cfmd', PID 4319, status 0
Jan 20 17:09:30 starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in
progress: Layer 2 address flooding and learning process checking new configuration
Jan 20 17:09:30 starfire mgd[4186]: UI_CHILD_START: Starting child
'/usr/sbin/l2ald'
Jan 20 17:09:30 starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child
'/usr/sbin/l2ald', PID 4320, status 0
Jan 20 17:09:30 starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in
progress: Layer 2 Control Protocol process checking new configuration
Jan 20 17:09:30 starfire mgd[4186]: UI_CHILD_START: Starting child
'/usr/sbin/l2cpd'
Jan 20 17:09:30 starfire l2cp[4321]: Initializing PNAC state machines
Jan 20 17:09:30 starfire l2cp[4321]: Initializing PNAC state machines complete
Jan 20 17:09:30 starfire l2cp[4321]: Initialized 802.1X module and state
machinesJan 20 17:09:30 starfire l2cp[4321]: Read access profile () config
Jan 20 17:09:30 starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child
'/usr/sbin/l2cpd', PID 4321, status 0
Jan 20 17:09:30 starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in
progress: Multicast Snooping process checking new configuration
Jan 20 17:09:30 starfire mgd[4186]: UI_CHILD_START: Starting child
'/usr/sbin/mcsnoopd'
Jan 20 17:09:30 starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child
'/usr/sbin/mcsnoopd', PID 4325, status 0
Jan 20 17:09:30 starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in
progress: commit wrapup...
Jan 20 17:09:30 starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in
progress: activating '/var/etc/ntp.conf'
Jan 20 17:09:30 starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in
progress: start ffp activate
Jan 20 17:09:30 starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/ffp'
Jan 20 17:09:30 starfire ffp[4326]: "dynamic-profiles": No change to profiles
.....
```



## CHAPTER 6

# Configuring Audit Log Options

- [Configuring Audit Log Options in the Evaluated Configuration on page 57](#)
- [Sample Code Audits of Configuration Changes on page 58](#)

## Configuring Audit Log Options in the Evaluated Configuration

---

The following section describes how to configure audit log options in the evaluated configuration.

- [Configuring Audit Log Options for MX240, MX480, MX960, MX2008, MX2010, MX2020, EX9204, EX9208, and EX9214 Devices on page 57](#)

### Configuring Audit Log Options for MX240, MX480, MX960, MX2008, MX2010, MX2020, EX9204, EX9208, and EX9214 Devices

To configure audit log options for MX240, MX480, MX960, MX2008, MX2010, MX2020, EX9204, EX9208, and EX9214 devices:

1. Specify the number of files to be archived in the system logging facility.

```
[edit system syslog]  
root@host#set archive files 2
```

2. Specify the file in which to log data.

```
[edit system syslog]  
root@host#set file syslog any any
```

3. Specify the size of files to be archived.

```
[edit system syslog]  
root@host#set file syslog archive size 10000000
```

4. Specify the priority and facility in messages for the system logging facility.

```
[edit system syslog]  
root@host#set file syslog explicit-priority
```

5. Log system messages in a structured format.

```
[edit system syslog]
root@host#set file syslog structured-data
```

**Related  
Documentation**

- [Sample Code Audits of Configuration Changes on page 58](#)

## Sample Code Audits of Configuration Changes

---

This sample code audits all changes to the configuration secret data and sends the logs to a file named **Audit-File**:

```
[edit system]
syslog {
  file Audit-File {
    authorization info;
    change-log info;
    interactive-commands info;
  }
}
```

This sample code expands the scope of the minimum audit to audit all changes to the configuration, not just secret data, and sends the logs to a file named **Audit-File**:

```
[edit system]
syslog {
  file Audit-File {
    any any;
    authorization info;
    change-log any;
    interactive-commands info;
    kernel info;
    pfe info;
  }
}
```

**Example: System  
Logging of  
Configuration Changes**

This example shows a sample configuration and makes changes to users and secret data. It then shows the information sent to the audit server when the secret data is added to the original configuration and committed with the **load** command.

```
[edit system]
location {
  country-code US;
  building B1;
}
...
login {
  message "UNAUTHORIZED USE OF THIS ROUTER\n\tIS STRICTLY PROHIBITED!";
  user admin {
    uid 2000;
  }
}
```

```

        class super-user;
        authentication {
            encrypted-password "$ABC123";
            # SECRET-DATA
        }
    }
}
radius-server 192.0.2.15 {
    secret "$ABC123" # SECRET-DATA
}
services {
    ssh;
}
syslog {
    user *{
        any emergency;
    }
    file messages {
        any notice;
        authorization info;
    }
    file interactive-commands {
        interactive-commands any;
    }
}
...

```

The new configuration changes the secret data configuration statements and adds a new user.

```

user@host# show | compare
[edit system login user admin authentication]
- encrypted-password "$ABC123"; # SECRET-DATA
+ encrypted-password "$ABC123"; # SECRET-DATA
[edit system login]
+ user admin2 {
+   uid 2001;
+   class operator;
+   authentication {
+     encrypted-password "$ABC123";
+     # SECRET-DATA
+   }
+ }
[edit system radius-server 192.0.2.15]
- secret "$ABC123"; # SECRET-DATA
+ secret "$ABC123"; # SECRET-DATA

```

Table 4 on page 60 shows sample for syslog auditing for NDcPPv2:

**Table 4: Auditable Events**

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
FCS_SSH_EXT.1	Failure to establish an SSH session.  Establishment/Termination of an SSH session.	Reason for failure.  Non-TOE endpoint of connection (IP address) for both successes and failures.	Identification & Authentication (FIA_UIA_EXT.1 – logging in) Large packet test.
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).	Identification & Authentication (FIA_UIA_EXT.1 – logging in)
FIA_UAU_EXT.2	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).	Identification & Authentication (FIA_UIA_EXT.1 – logging in)
FPT_STM.1	Changes to the time.	The old and new values for the time. Origin of the attempt (e.g., IP address).	Time updates (FPT_STM.1)
FPT_TUD_EXT.1	Initiation of update.	No additional information.	Proper TOE Updates (FPT_TUD_EXT.1.3)
FPT_TST_EXT.1	Indication that TSF self-test was completed.	Any additional information generated by the tests beyond “success” or “failure”.	Entered ‘request system fips self-test’ at command line.
FTA_SSL_EXT.1	Any attempts at unlocking of an interactive session.	No additional information.	Local Interactive Session Timeout Enforcement (FTA_SSL_EXT.1)
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	No additional information.	Remote Session Timeout Enforcement (FTA_SSL.3)
FTA_SSL.4	Initiation of the trusted channel. Termination of the trusted channel.  Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.	Audit Server Configuration (FAU_STG_EXT.1).
FTP_JTC.1	Used as entropy input string to the HMAC DRBG.	Power cycle.	A critical value of the internal state of DRBG.
FTP_TRP.1	Initiation of the trusted channel.  Termination of the trusted channel.  Failures of the trusted path functions.	Identification of the claimed user identity.	See audit results for FCS_SSH_EXT.1.

*Table 4: Auditable Events (continued)*

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
FTP_TRP.1	Initiation of the trusted channel.  Termination of the trusted channel.  Failures of the trusted path functions.	Identification of the claimed user identity.	See audit results for FCS_SSH_EXT.1.

**Related Documentation**

- [Configuring Audit Log Options in the Evaluated Configuration on page 57](#)



## CHAPTER 7

# Configuring Event Logging

- [Event Logging Overview on page 63](#)
- [Configuring Event Logging to a Local File on page 64](#)
- [Interpreting Event Messages on page 64](#)
- [Logging Changes to Secret Data on page 65](#)
- [Login and Logout Events Using SSH on page 66](#)
- [Logging of Audit Startup on page 66](#)

### Event Logging Overview

---

The evaluated configuration requires the auditing of configuration changes through the system log.

In addition, Junos OS can:

- Send automated responses to audit events (syslog entry creation).
- Allow authorized managers to examine audit logs.
- Send audit files to external servers.
- Allow authorized managers to return the system to a known state.

The logging for the evaluated configuration must capture the following events:

- Changes to secret key data in the configuration.
- Committed changes.
- Login/logout of users.
- System startup.
- Failure to establish an SSH session.
- Establishment/termination of an SSH session.
- Changes to the (system) time.
- Termination of a remote session by the session locking mechanism.
- Termination of an interactive session.

In addition, Juniper Networks recommends that logging also:

- Capture all changes to the configuration.
- Store logging information remotely.

**Related Documentation** • [Interpreting Event Messages on page 64](#)

---

## Configuring Event Logging to a Local File

You can configure storing of audit information to a local file with the **syslog** statement. This example stores logs in a file named **Audit-File**:

```
[edit system]
syslog {
  file Audit-File;
}
```

**Related Documentation** • [Event Logging Overview on page 63](#)

---

## Interpreting Event Messages

The following output shows a sample event message.

```
Feb 27 02:33:04 bm-a mgd[6520]: UI_LOGIN_EVENT: User 'security-officer' login, class
'j-super-user' [6520], ssh-connection '', client-mode 'cli'
Feb 27 02:33:49 bm-a mgd[6520]: UI_DBASE_LOGIN_EVENT: User 'security-officer' entering
configuration mode
Feb 27 02:38:29 bm-a mgd[6520]: UI_CMDLINE_READ_LINE: User 'security-officer',
command 'run show log Audit_log | grep LOGIN
```

[Table 5 on page 64](#) describes the fields for an event message. If the system logging utility cannot determine the value in a particular field, a hyphen ( - ) appears instead.

*Table 5: Fields in Event Messages*

Field	Description	Examples
<i>timestamp</i>	Time when the message was generated, in one of two representations: <ul style="list-style-type: none"><li>• <b>MMM-DD HH:MM:SS.MS+/-HH:MM</b>, is the month, day, hour, minute, second and millisecond in local time. The hour and minute that follows the plus sign ( + ) or minus sign ( - ) is the offset of the local time zone from Coordinated Universal Time (UTC).</li><li>• <b>YYYY-MM-DDTHH:MM:SS.MSZ</b> is the year, month, day, hour, minute, second and millisecond in UTC.</li></ul>	Feb 27 02:33:04 is the timestamp expressed as local time in the United States. 2012-02-27T09:17:15.719Z is 2:33 AM UTC on 27 Feb 2012.



Table 5: Fields in Event Messages (continued)

Field	Description	Examples
<b>hostname</b>	Name of the host that originally generated the message.	router1
<b>process</b>	Name of the Junos OS process that generated the message.	mgd
<b>processID</b>	UNIX process ID (PID) of the Junos OS process that generated the message.	4153
<b>TAG</b>	Junos OS system log message tag, which uniquely identifies the message.	UI_DBASE_LOGOUT_EVENT
<b>username</b>	Username of the user initiating the event.	"admin"
<b>message-text</b>	English-language description of the event .	set: [system radius-server 1.2.3.4 secret]

**Related Documentation**

- [Event Logging Overview on page 63](#)

## Logging Changes to Secret Data

The following are examples of audit logs of events that change the secret data. Whenever there is a change in the configuration example, the syslog event should capture the below logs:

```
Jul 24 17:43:28 router1 mgd[4163]: UI_CFG_AUDIT_SET_SECRET: User 'admin' set: [system radius-server 1.2.3.4 secret]
Jul 24 17:43:28 router1 mgd[4163]: UI_CFG_AUDIT_SET_SECRET: User 'admin' set: [system login user admin authentication encrypted-password]
Jul 24 17:43:28 router1 mgd[4163]: UI_CFG_AUDIT_SET_SECRET: User 'admin' set: [system login user admin2 authentication encrypted-password]
```

Everytime a configuration is updated or changed, the syslog should capture these logs:

```
Jul 24 18:29:09 router1 mgd[4163]: UI_CFG_AUDIT_SET_SECRET: User 'admin' replace: [system radius-server 1.2.3.4 secret]
Jul 24 18:29:09 router1 mgd[4163]: UI_CFG_AUDIT_SET_SECRET: User 'admin' replace: [system login user admin authentication encrypted-password]
Jul 24 18:29:09 router1 mgd[4163]: UI_CFG_AUDIT_SET_SECRET: User 'admin' replace: [system login user admin authentication encrypted-password]
```

For more information about configuring parameters and managing log files, see the *Junos OS System Log Messages Reference*.

**Related Documentation**

- [Interpreting Event Messages on page 64](#)

## Login and Logout Events Using SSH

---

System log messages are generated whenever a user successfully or unsuccessfully attempts SSH access. Logout events are also recorded. For example, the following logs are the result of two failed authentication attempts, then a successful one, and finally a logout:

```
Dec 20 23:17:35 bilbo sshd[16645]: Failed password for op from 172.17.58.45 port 1673 ssh2
Dec 20 23:17:42 bilbo sshd[16645]: Failed password for op from 172.17.58.45 port 1673 ssh2
Dec 20 23:17:53 bilbo sshd[16645]: Accepted password for op from 172.17.58.45 port 1673 ssh2
Dec 20 23:17:53 bilbo mgd[16648]: UI_AUTH_EVENT: Authenticated user 'op' at permission level
                        'j-operator'
Dec 20 23:17:53 bilbo mgd[16648]: UI_LOGIN_EVENT: User 'op' login, class 'j-operator' [16648]
Dec 20 23:17:56 bilbo mgd[16648]: UI_CMDLINE_READ_LINE: User 'op', command 'quit '
Dec 20 23:17:56 bilbo mgd[16648]: UI_LOGOUT_EVENT: User 'op' logout
```

**Related Documentation** • [Interpreting Event Messages on page 64](#)

## Logging of Audit Startup

---

The audit information logged includes startups of Junos OS. This in turn identifies the startup events of the audit system, which cannot be independently disabled or enabled. For example, if Junos OS is restarted, the audit log contains the following information:

```
Dec 20 23:17:35 bilbo syslogd: exiting on signal 14
Dec 20 23:17:35 bilbo syslogd: restart
Dec 20 23:17:35 bilbo syslogd /kernel: Dec 20 23:17:35 init: syslogd (PID 19128) exited with status=1
Dec 20 23:17:42 bilbo /kernel:
Dec 20 23:17:53 init: syslogd (PID 19200) started
```

**Related Documentation** • [Login and Logout Events Using SSH on page 66](#)

## CHAPTER 8

# Performing Self-Tests on a Device

- [Understanding FIPS Self-Tests on page 67](#)
- [Example: Configuring FIPS Self-Tests on page 67](#)

### 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 router or switch performs the following series of known answer test (KAT) self-tests:

- **kernel\_kats**—KAT for kernel cryptographic routines
- **md\_kats**—KAT for libmd and libc
- **openssl\_kats**—KAT for OpenSSL cryptographic implementation
- **quicksec\_kats**—KAT for QuickSec Toolkit cryptographic implementation
- **ssh\_ipsec\_kats**—KAT for SSH IPsec Toolkit cryptographic implementation

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

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

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

### Example: Configuring FIPS Self-Tests

---

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

- [Hardware and Software Requirements on page 68](#)
- [Overview on page 68](#)
- [Configuration on page 68](#)
- [Verification on page 69](#)

## Hardware and Software Requirements

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

## Overview

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

- **kernel\_kats**—KAT for kernel cryptographic routines
- **md\_kats**—KAT for libmd and libc
- **quicksec\_kats**—KAT for QuickSec Toolkit cryptographic implementation
- **openssl\_kats**—KAT for OpenSSL cryptographic implementation
- **ssh\_ipsec\_kats**—KAT for SSH IPsec Toolkit cryptographic implementation

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



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

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

## Configuration

### CLI Quick Configuration

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

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

### Step-by-Step Procedure

To configure the FIPS self-test:

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

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

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

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

## Results

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

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

## Verification

Confirm that the configuration is working properly.

### Verifying the FIPS Self-Test

**Purpose** Verify that the FIPS self-test is enabled.

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

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

For MX Series routers with RE-S-1800X4, RE-MX2000-1800X4, and REMX2K-1800-32G:

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

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

For MX Series routers with MS-MPC:

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

```

Testing jsf crypto (mpc xlp platform):
station 281, testing SAE engine no. 0 ...
station 281, testing SAE engine no. 4 ...
station 281, testing SAE engine no. 8 ...
station 281, testing SAE engine no. 1 ...
station 281, testing SAE engine no. 5 ...
station 281, testing SAE engine no. 9 ...
station 281, testing SAE engine no. 2 ...
station 281, testing SAE engine no. 6 ...
station 281, testing SAE engine no. 10 ...
station 281, testing SAE engine no. 3 ...
station 281, testing SAE engine no. 7 ...
station 281, testing SAE engine no. 11 ...
station 281, testing SAE engine no. 0 ...
station 281, testing SAE engine no. 4 ...
station 281, testing SAE engine no. 8 ...
station 281, testing SAE engine no. 1 ...
station 281, testing SAE engine no. 5 ...
station 281, testing SAE engine no. 9 ...
station 281, testing SAE engine no. 2 ...
station 281, testing SAE engine no. 6 ...
station 281, testing SAE engine no. 10 ...
station 281, testing SAE engine no. 3 ...
station 281, testing SAE engine no. 7 ...
station 281, testing SAE engine no. 11 ...
DES3-CBC Known Answer Test:
station 281, testing SAE engine no. 0 ...
station 281, testing SAE engine no. 4 ...
station 281, testing SAE engine no. 8 ...
station 281, testing SAE engine no. 1 ...
station 281, testing SAE engine no. 5 ...
station 281, testing SAE engine no. 9 ...
station 281, testing SAE engine no. 2 ...
station 281, testing SAE engine no. 6 ...
station 281, testing SAE engine no. 10 ...
station 281, testing SAE engine no. 3 ...
station 281, testing SAE engine no. 7 ...
station 281, testing SAE engine no. 11 ...
HMAC-SHA2-256 Known Answer Test:
station 281, testing SAE engine no. 0 ...
station 281, testing SAE engine no. 4 ...
station 281, testing SAE engine no. 8 ...
station 281, testing SAE engine no. 1 ...
station 281, testing SAE engine no. 5 ...
station 281, testing SAE engine no. 9 ...
station 281, testing SAE engine no. 2 ...
station 281, testing SAE engine no. 6 ...
station 281, testing SAE engine no. 10 ...
station 281, testing SAE engine no. 3 ...
station 281, testing SAE engine no. 7 ...
station 281, testing SAE engine no. 11 ...
station 281, testing SAE engine no. 0 ...
station 281, testing SAE engine no. 4 ...
station 281, testing SAE engine no. 8 ...
station 281, testing SAE engine no. 1 ...
station 281, testing SAE engine no. 5 ...
station 281, testing SAE engine no. 9 ...
station 281, testing SAE engine no. 2 ...
station 281, testing SAE engine no. 6 ...
station 281, testing SAE engine no. 10 ...

```

Passed

Passed

station 281, testing SAE engine no. 3 ...	
station 281, testing SAE engine no. 7 ...	
station 281, testing SAE engine no. 11 ...	
station 281, testing SAE engine no. 0 ...	
station 281, testing SAE engine no. 4 ...	
station 281, testing SAE engine no. 8 ...	
station 281, testing SAE engine no. 1 ...	
station 281, testing SAE engine no. 5 ...	
station 281, testing SAE engine no. 9 ...	
station 281, testing SAE engine no. 2 ...	
station 281, testing SAE engine no. 6 ...	
station 281, testing SAE engine no. 10 ...	
station 281, testing SAE engine no. 3 ...	
station 281, testing SAE engine no. 7 ...	
station 281, testing SAE engine no. 11 ...	
station 281, testing SAE engine no. 0 ...	
station 281, testing SAE engine no. 4 ...	
station 281, testing SAE engine no. 8 ...	
station 281, testing SAE engine no. 1 ...	
station 281, testing SAE engine no. 5 ...	
station 281, testing SAE engine no. 9 ...	
station 281, testing SAE engine no. 2 ...	
station 281, testing SAE engine no. 6 ...	
station 281, testing SAE engine no. 10 ...	
station 281, testing SAE engine no. 3 ...	
station 281, testing SAE engine no. 7 ...	
station 281, testing SAE engine no. 11 ...	
station 281, testing SAE engine no. 0 ...	
station 281, testing SAE engine no. 4 ...	
station 281, testing SAE engine no. 8 ...	
station 281, testing SAE engine no. 1 ...	
station 281, testing SAE engine no. 5 ...	
station 281, testing SAE engine no. 9 ...	
station 281, testing SAE engine no. 2 ...	
station 281, testing SAE engine no. 6 ...	
station 281, testing SAE engine no. 10 ...	
station 281, testing SAE engine no. 3 ...	
station 281, testing SAE engine no. 7 ...	
station 281, testing SAE engine no. 11 ...	
AES-CBC Known Answer Test:	Passed
station 281, testing SAE engine no. 0 ...	
station 281, testing SAE engine no. 4 ...	
station 281, testing SAE engine no. 8 ...	
station 281, testing SAE engine no. 1 ...	
station 281, testing SAE engine no. 5 ...	
station 281, testing SAE engine no. 9 ...	
station 281, testing SAE engine no. 2 ...	
station 281, testing SAE engine no. 6 ...	



```

station 281, testing SAE engine no. 10 ...
station 281, testing SAE engine no. 3 ...
station 281, testing SAE engine no. 7 ...
station 281, testing SAE engine no. 11 ...
station 281, testing SAE engine no. 0 ...
station 281, testing SAE engine no. 4 ...
station 281, testing SAE engine no. 8 ...
station 281, testing SAE engine no. 1 ...
station 281, testing SAE engine no. 5 ...
station 281, testing SAE engine no. 9 ...
station 281, testing SAE engine no. 2 ...
station 281, testing SAE engine no. 6 ...
station 281, testing SAE engine no. 10 ...
station 281, testing SAE engine no. 3 ...
station 281, testing SAE engine no. 7 ...
station 281, testing SAE engine no. 11 ...
station 281, testing SAE engine no. 0 ...
station 281, testing SAE engine no. 4 ...
station 281, testing SAE engine no. 8 ...
station 281, testing SAE engine no. 1 ...
station 281, testing SAE engine no. 5 ...
station 281, testing SAE engine no. 9 ...
station 281, testing SAE engine no. 2 ...
station 281, testing SAE engine no. 6 ...
station 281, testing SAE engine no. 10 ...
station 281, testing SAE engine no. 3 ...
station 281, testing SAE engine no. 7 ...
station 281, testing SAE engine no. 11 ...
station 281, testing SAE engine no. 0 ...
station 281, testing SAE engine no. 4 ...
station 281, testing SAE engine no. 8 ...
station 281, testing SAE engine no. 1 ...
station 281, testing SAE engine no. 5 ...
station 281, testing SAE engine no. 9 ...
station 281, testing SAE engine no. 2 ...
station 281, testing SAE engine no. 6 ...
station 281, testing SAE engine no. 10 ...
station 281, testing SAE engine no. 3 ...
station 281, testing SAE engine no. 7 ...
station 281, testing SAE engine no. 11 ...
station 281, testing SAE engine no. 0 ...
station 281, testing SAE engine no. 4 ...
station 281, testing SAE engine no. 8 ...
station 281, testing SAE engine no. 1 ...
station 281, testing SAE engine no. 5 ...
station 281, testing SAE engine no. 9 ...
station 281, testing SAE
ms40 (ttyd0)

```

For EX Series Ethernet switches:

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

```

mgd: Running FIPS Self-tests
mgd: Testing kernel KATS:
mgd:  NIST 800-90 HMAC DRBG Known Answer Test:      Passed
mgd:  DES3-CBC Known Answer Test:                   Passed
mgd:  HMAC-SHA1 Known Answer Test:                   Passed
mgd:  HMAC-SHA2-256 Known Answer Test:               Passed

```

mgd:	SHA-2-384 Known Answer Test:	Passed
mgd:	SHA-2-512 Known Answer Test:	Passed
mgd:	AES128-CMAC Known Answer Test:	Passed
mgd:	AES-CBC Known Answer Test:	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
```

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



## CHAPTER 9

# Operational Commands

- request system zeroize
- request vmhost zeroize no-forwarding

## request system zeroize

---

<b>Syntax</b>	<code>request system zeroize</code>
<b>Release Information</b>	<p>Command introduced before Junos OS Release 9.0.</p> <p>Command introduced in Junos OS Release 11.2 for EX Series switches.</p> <p>Command introduced in Junos OS Release 12.2 for MX Series routers.</p>
<b>Description</b>	<p>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 all 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.</p> <p>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 <b>root</b> and start the Junos OS CLI by typing <b>cli</b> at the prompt.</p>
<b>Required Privilege Level</b>	maintenance
<b>List of Sample Output</b>	<a href="#">request system zeroize on page 78</a>

### Sample Output

#### request system zeroize

```
user@host> request system zeroize

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

warning: zeroizing re0
Jul 27 22:25:53 jlaunchd: gkd-re (PID 5264) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: inet-process (PID 5267) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: periodic-packet-services (PID 5271) terminate signal
15 sent
Jul 27 22:25:53 jlaunchd: disk-monitoring (PID 5273) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: neighbor-liveness (PID 5307) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: event-processing (PID 5209) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: clksyncd-service (PID 5316) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: ethernet-link-fault-management (PID 5321) terminate
signal 15 sent
Jul 27 22:25:53 jlaunchd: subscriber-management (PID 5323) terminate signal 15
sent
Jul 27 22:25:53 jlaunchd: shm-rtssdbd (PID 5325) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: gstatd (PID 5326) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: rpcbind-service (PID 5330) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: icmd (PID 5332) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: pmcd (PID 5333) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: ftp-inet-process (PID 5334) terminate signal 15 sent
```

```
Jul 27 22:25:53 jlaunchd: process-monitor (PID 5338) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: smg-service-telemetry (PID 5340) terminate signal 15
sent
Jul 27 22:25:53 jlaunchd: application-identification (PID 5341) terminate signal
15 sent
Jul 27 22:25:53 jlaunchd: resource-management (PID 5342) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: charged (PID 5346) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: license-service (PID 5351) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: ntp (PID 6120) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: gkd-chassis (PID 6121) terminate signal 15 sent
Jul 27 22:25:53 jlaunchd: gkd-lchassis
```

```
.....
```

## request vmhost zeroize no-forwarding

---

<b>Syntax</b>	request vmhost zeroize no-forwarding
<b>Release Information</b>	<p>Command introduced in Junos OS Release 15.1F3 for the MX240, MX480, and MX960 routers.</p> <p>Command introduced in Junos OS Release 15.1F5 for the MX2010 and MX2020 routers.</p> <p>Command introduced in Junos OS Release 17.1R1 for EX9200 switches.</p>
<b>Description</b>	<p>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.</p> <p>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 <b>cli</b> at the prompt.</p>
<b>Required Privilege Level</b>	maintenance
<b>List of Sample Output</b>	<a href="#">request vmhost zeroize no-forwarding on page 80</a>

## Sample Output

### request vmhost zeroize no-forwarding

```
user@host> request vmhost zeroize no-forwarding

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
---(more)---
Waiting for PIDS: 6135.
.
Feb 16 14:59:33 jlaunchd: periodic-packet-services (PID 6181) terminate signal 15 sent
Feb 16 14:59:33 jlaunchd: smg-service (PID 6234) terminate signal 15 sent
Feb 16 14:59:33 jlaunchd: application-identification (PID 6236) terminate signal 15 sent
Feb 16 14:59:33 jlaunchd: ifstate-tracing-process (PID 6241) terminate signal 15 sent
Feb 16 14:59:33 jlaunchd: resource-management (PID 6243) terminate signal 15 sent
Feb 16 14:59:33 jlaunchd: charged (PID 6246) terminate signal 15 sent
Feb 16 14:59:33 jlaunchd: license-service (PID 6255) terminate signal 15 sent
Feb 16 14:59:33 jlaunchd: ntp (PID 6620) terminate signal 15 sent
Feb 16 14:59:33 jlaunchd: gkd-chassis (PID 6621) terminate signal 15 sent
Feb 16 14:59:33 jlaunchd: gkd-lchassis (PID 6622) terminate signal 15 sent
Feb 16 14:59:33 jlaunchd: routing (PID 6625) terminate signal 15 sent
Feb 16 14:59:33 jlaunchd: sonet-aps (PID 6626) terminate signal 15 sent
Feb 16 14:59:33 jlaunchd: remote-operations (PID 6627) terminate signal 15 sent
Feb 16 14:59:33 jlaunchd: class-of-service

```

```

.....

```



# Protecting Against DoS Attacks

- [Configuring Access Control Lists on page 83](#)
- [Configuring Reverse Path Forwarding on page 83](#)

## Configuring Access Control Lists

---

A stateless firewall filter, also known as an access control list (ACL), is a long-standing Junos feature used to define stateless packet filtering and quality of service (QoS). You can configure firewall filters to protect Ethernet switch from malicious traffic. For example, you can use the filters to restrict the local packets that pass from the switch's physical interfaces to the Routing Engine. Such filters are useful in protecting the IP services that run on the Routing Engine, such as SSH, from denial-of-service attacks.

To protect against DoS attacks such as SegmentStack, ACLs can be used to prevent untrusted hosts from establishing TCP connections with the MX/EX. SegmentStack requires an established connection to exist before the attack can be launched.

To configure ACLs, use the **rpf-check** statement, which can be included at the following hierarchy levels:

- [edit interfaces interface-name unit logical-unit-number family (inet | inet6)]
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family (inet | inet6)]

## Configuring Reverse Path Forwarding

---

Crafted sequences of TCP/IP packets may allow a remote attacker to create a denial of service (DoS) condition on routing engines (REs) running Junos OS. The attack requires a successfully established two-way TCP connection to an open port. The rate of attack traffic is lower than typical thresholds for built-in Junos OS distributed denial-of-service (DDoS) protection, so additional configuration is required to defend against these issues.

To protect against DoS attacks such as SegmentStack, unicast reverse path forwarding (RPF) should be configured. Unicast RPF helps determine the source of attacks and rejects packets from unexpected source addresses on interfaces where unicast RPF is enabled.

To configure unicast RPF,, use the **rpf-check** statement, which can be included at the following hierarchy levels:

- [edit interfaces interface-name unit logical-unit-number family (inet | inet6)]
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family (inet | inet6)]