



Junos[®] OS

Common Criteria and FIPS Evaluated Configuration Guide for QFX10002, QFX10008, and QFX10016 Series Devices

Release

18.1R1 for FIPS and 18.1R2 for Common Criteria



Modified: 2019-02-26

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

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

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

Junos® OS Common Criteria and FIPS Evaluated Configuration Guide for QFX10002, QFX10008, and QFX10016 Series Devices
18.1R1 for FIPS and 18.1R2 for Common Criteria
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
Chapter 1	Overview	15
	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 QFX Series Switch	16
	How FIPS Mode Differs from Non-FIPS Mode	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	20
	Identifying Secure Product Delivery	22
	Understanding Management Interfaces	23
Chapter 2	Configuring Roles and Authentication Methods	25
	Understanding Roles and Services for Junos OS in Common Criteria and	
	FIPS	25
	Crypto Officer Role and Responsibilities	26
	FIPS User Role and Responsibilities	27
	What Is Expected of All FIPS Users	27
	Understanding the Operational Environment for Junos OS in FIPS Mode	28
	Hardware Environment for Junos OS in FIPS Mode	28
	Software Environment for Junos OS in FIPS Mode	28
	Critical Security Parameters	29
	Understanding Password Specifications and Guidelines for Junos OS in FIPS	
	Mode	32
	Understanding Requirements for Secure Communication Between Routing	
	Engines in FIPS Mode	33
	SA Direction	33
	SPI	34
	IPsec Keys	34

	IPsec Limitations	34
	Downloading Software Packages from Juniper Networks	34
	Installing Software on a QFX Series devices with a Single Routing Engine	35
	Understanding Zeroization to Clear System Data for FIPS Mode	36
	Why Zeroize?	37
	When to Zeroize?	37
	Zeroizing the System	38
	Enabling FIPS Mode	40
	Configure FPCs in FIPS Mode	44
	Establishing Root Password Access	45
	Configuring Crypto Officer and FIPS User Identification and Access	46
	Configuring Crypto Officer Login Access	46
	Configuring FIPS User Login Access	47
Chapter 3	Configuring Administrative Credentials and Privileges	51
	Understanding the Associated Password Rules for an Authorized Administrator	51
	Authentication methods in FIPS mode of Operation	52
	Username and Password Authentication over the Console and SSH	53
	Username and Public Key Authentication over SSH	53
	Configuring a Network Device collaborative Protection Profile for an Authorized Administrator	53
Chapter 4	Configuring SSH and Console Connection	57
	Configuring a System Login Message and Announcement	57
	Configuring SSH on the Evaluated Configuration for NDcPP	58
	Configuring SSH on the Evaluated Configuration for FIPS	59
	Limiting the Number of User Login Attempts for SSH Sessions	61
Chapter 5	Configuring the Remote Syslog Server	63
	Syslog Server Configuration on a Linux System	63
	Configuring Event Logging to a Local File	63
	Configuring Event Logging to a Remote Server	63
	Configuring Event Logging to a Remote Server when Initiating the Connection from the Remote Server	64
Chapter 6	Configuring Audit Log Options	69
	Configuring Audit Log Options in the Evaluated Configuration	69
	Configuring Audit Log Options for QFX10002, QFX10008, and QFX10016 Devices	69
	Sample Code Audits of Configuration Changes	70
Chapter 7	Configuring Event Logging	75
	Event Logging Overview	75
	Configuring Event Logging to a Local File	76
	Interpreting Event Messages	76
	Logging Changes to Secret Data	77
	Login and Logout Events Using SSH	78
	Logging of Audit Startup	79

Chapter 8	Performing Self-Tests on a Device	81
	Understanding FIPS Self-Tests	81
	Performing Power-On Self-Tests on the Device	81
Chapter 9	Configuration Statements	85
	algorithm (FIPS)	86
	authentication (FIPS)	87
	direction (FIPS)	88
	fips (FIPS)	89
	internal (FIPS)	90
	ipsec (FIPS)	91
	key (FIPS)	92
	level (FIPS)	93
	manual (FIPS)	94
	protocol esp (FIPS)	94
	security (FIPS)	95
	spi (FIPS)	96
Chapter 10	Operational Commands	97
	request system zeroize	98

List of Tables

	About the Documentation	ix
	Table 1: Notice Icons	x
	Table 2: Text and Syntax Conventions	x
Chapter 1	Overview	15
	Table 3: Cryptographic Boundaries on FIPS-Certified QFX Series Switches	17
Chapter 2	Configuring Roles and Authentication Methods	25
	Table 4: Critical Security Parameters	30
Chapter 6	Configuring Audit Log Options	69
	Table 5: Auditable Events	72
Chapter 7	Configuring Event Logging	75
	Table 6: Fields in Event Messages	76

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
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>

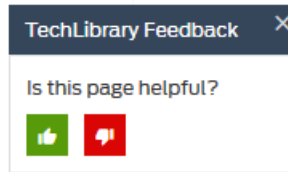
Table 2: Text and Syntax Conventions (continued)

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

Documentation Feedback

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

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



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

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service 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 22
- Understanding Management Interfaces on page 23

Understanding the Common Criteria Evaluated Configuration

This document describes the steps required to configure the device running Junos OS when the device is evaluated. This is referred to as the evaluated configuration. The device has been evaluated based on collaborative Protection Profile for Network Devices, Version 2.0, 05 May, 2017 (NDcPP Version 2.0).

This document is available at

https://www.commoncriteriaportal.org/files/ppfiles/CPD_ND_V2.0.pdf.



NOTE: On QFX10002, QFX10008, and QFX10016 devices, Junos OS Release 18.1R2 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 a system subjected to evaluation based on the Collaborative Protection Profile (cPP).

Supported Platforms

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

- The NDcPP Version 2.0 applies to QFX10002, QFX10008, and QFX10016 Series devices.

Related Documentation

- [Identifying Secure Product Delivery on page 22](#)

Understanding Junos OS in FIPS Mode

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

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

The *Crypto Officer* enables FIPS mode in Junos OS and sets up keys and passwords for the system and other *FIPS users* who can view the configuration. Both Crypto Officer and user can perform normal configuration tasks on the switch (such as modify interface types) as individual user configuration allows.

- [About the Cryptographic Boundary on Your QFX Series Switch on page 16](#)
- [How FIPS Mode Differs from Non-FIPS Mode on page 17](#)
- [Validated Version of Junos OS in FIPS Mode on page 17](#)

About the Cryptographic Boundary on Your QFX Series Switch

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

For the Juniper Networks QFX Series switches that are certified at FIPS-140-2 Level 1, the cryptographic boundary of the module is determined by the chassis type. For a list of FIPS-certified switches and the cryptographic boundary of each switch, see [Table 3 on page 17](#).

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

Switch	Chassis Type	Cryptographic Boundary
QFX10002 switch	Fixed configuration	Switch case
QFX10008 switch with any line card configuration	Modular configuration	Chassis boundary
QFX10016 switch with any line card configuration	Modular configuration	Chassis boundary

To physically secure the cryptographic module, all QFX Series switches require a tamper-evident seal on the USB. QFX10008, and QFX10016 switches require a tamper-evident seal on Four SFP+ ports located at control board.

How FIPS Mode Differs from Non-FIPS Mode

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

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

Validated Version of Junos OS in FIPS Mode

On QFX10002, QFX10008, and QFX10016 devices, Junos OS Release 18.1R1 is certified for FIPS. To determine whether a Junos OS release is NIST-validated, see the software download page on the Juniper Networks Web site (<http://www.juniper.net/>) or the National Institute of Standards and Technology site.

Related Documentation

- [Identifying Secure Product Delivery on page 22](#)

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 20](#)

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 28.

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. QFX Series switches are certified at FIPS 140-2 Level 1. For fixed-configuration switches, the cryptographic module is the switch case. For modular switches, the cryptographic module is the Routing Engine.

Crypto Officer—Person with appropriate permissions who is responsible for securely enabling, configuring, monitoring, and maintaining Junos OS in FIPS mode on a switch. For details, see “[Understanding Roles and Services for Junos OS in Common Criteria and FIPS](#)” on page 25.

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

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

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



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

IKE—The Internet Key Exchange (IKE) is part of IPsec and provides ways to securely negotiate the shared private keys that the AH and ESP portions of IPsec need to function properly. IKE employs Diffie-Hellman key-exchange methods and is optional in IPsec. (The shared keys can be entered manually at the endpoints.)

IPsec—The IP Security (IPsec) protocol. A standard way to add security to Internet communications. IPsec security association (SA) is required on the switch to enable internal communication between the Routing Engine and PFE.

An IPsec SA is required for fixed-configuration switches running Junos OS in FIPS mode because the Routing Engine communicates with system processes through logical connections; therefore, the switch requires an internal, manual IPsec SA to protect those logical communications when the switch is running in FIPS mode. By default design, the switch has some innate characteristics of a master switch in a Virtual Chassis, and this use of logical communications is one such characteristic. In a multimember Virtual Chassis, the master switch's Routing Engine would send control messages to the Routing Engines of the other member switches by using those built-in logical communications. Do not configure a Virtual Chassis in FIPS mode. Note, however, that the IPsec SA is required on your single switch to protect the built-in logical connections.

KATs—Known answer tests. System self-tests that validate the output of cryptographic algorithms approved for FIPS and test the integrity of some Junos OS modules. For details, see [“Understanding FIPS Self-Tests” on page 81](#).

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

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

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

Zeroization—Erasure of all CSPs and other user-created data on a switch before its operation as a FIPS cryptographic module—or in preparation for repurposing the switch for non-FIPS operation. The Crypto Officer can zeroize the system with a CLI operational command. For details, see [“Understanding Zeroization to Clear System Data for FIPS Mode” on page 36](#).

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.

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

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

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

the size of the security level, in bits. ECDSA using the P-256, P-384, P-521 curves that can be configured under OpenSSH.

HMAC—Defined as “Keyed-Hashing for Message Authentication” in RFC 2104, HMAC combines hashing algorithms with cryptographic keys for message authentication. For Junos OS in FIPS mode, HMAC uses the iterated cryptographic hash functions SHA-1, SHA-256, and SHA-512 along with a secret key.

SHA-256 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.

AES-CMAC—AES-CMAC provides stronger assurance of data integrity than a checksum or an error-detecting code. The verification of a checksum or an error-detecting code detects only accidental modifications of the data, while CMAC is designed to detect intentional, unauthorized modifications of the data, as well as accidental modifications.

- Related Documentation**
- [Understanding FIPS Self-Tests on page 81](#)
 - [Understanding Zeroization to Clear System Data for FIPS Mode on page 36](#)

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

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

CHAPTER 2

Configuring Roles and Authentication Methods

- [Understanding Roles and Services for Junos OS in Common Criteria and FIPS on page 25](#)
- [Understanding the Operational Environment for Junos OS in FIPS Mode on page 28](#)
- [Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode on page 32](#)
- [Understanding Requirements for Secure Communication Between Routing Engines in FIPS Mode on page 33](#)
- [Downloading Software Packages from Juniper Networks on page 34](#)
- [Installing Software on a QFX Series devices with a Single Routing Engine on page 35](#)
- [Understanding Zeroization to Clear System Data for FIPS Mode on page 36](#)
- [Zeroizing the System on page 38](#)
- [Enabling FIPS Mode on page 40](#)
- [Configure FPCs in FIPS Mode on page 44](#)
- [Establishing Root Password Access on page 45](#)
- [Configuring Crypto Officer and FIPS User Identification and Access on page 46](#)

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 allow the administrator to perform all tasks necessary to manage the 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, and 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 (read-only, administrative user, and so on) must fall into one of the two categories: Crypto Officer or FIPS user.

In addition to their FIPS roles, both Crypto Officer and user can perform normal configuration tasks on the switch as individual user configuration allows.

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

For details, see:

- [Crypto Officer Role and Responsibilities on page 26](#)
- [FIPS User Role and Responsibilities on page 27](#)
- [What Is Expected of All FIPS Users on page 27](#)

Crypto Officer Role and Responsibilities

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



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

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



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

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

- Set the initial root password.
- Reset user passwords for FIPS-approved algorithms during upgrades from Junos OS.
- Examine log and audit files for events of interest.
- Erase user-generated files and data on (zeroize) the switch.

FIPS User Role and Responsibilities

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

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

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

What Is Expected of All FIPS Users

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

All FIPS users must:

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

Related Documentation

- [Zeroizing the System on page 38](#)
- [Configuring Crypto Officer and FIPS User Identification and Access on page 46](#)

Understanding the Operational Environment for Junos OS in FIPS Mode

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

- [Hardware Environment for Junos OS in FIPS Mode on page 28](#)
- [Software Environment for Junos OS in FIPS Mode on page 28](#)
- [Critical Security Parameters on page 29](#)

Hardware Environment for Junos OS in FIPS Mode

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

For more information about the cryptographic boundary on your switch, see [“Understanding Junos OS in FIPS Mode” on page 16](#).

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



BEST PRACTICE: If a seal is tampered with, the cryptographic module is considered to be compromised. To restore the module, we recommend that you apply new tamper-evident seals, zeroize the system, and set up new passwords and CSPs.

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

Software Environment for Junos OS in FIPS Mode

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

FIPS mode on QFX Series switches are available starting with Junos OS Release 18.1R1. The Junos OS in FIPS mode software environment is established after the Crypto Officer successfully enables FIPS mode on QFX Series switch. The Junos OS Release 18.1R1 image that includes FIPS mode is available on the Juniper Networks website and can be installed on QFX Series switches.

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



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

Critical Security Parameters

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

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

Table 4 on page 30 lists CSPs on switches running Junos OS.

Table 4: Critical Security Parameters

CSP	Description	Zeroization method	Use
SSH-2 private host key	ECDSA key used to identify the host, generated the first time SSH is configured. RSA key used to identify the host, generated the first time SSH is configured.	Zeroize command.	Used to identify the host.
SSH-2 session key	Session encryption key(client to server and server to client), Session authentication keys (client to server and server to client), DH/ECDH shared secret, DH/ECDH private key. Encryption: 3DES (FIPS only), AES-128, AES-256. MACs: HMAC-SHA-1, HMAC SHA-256, HMAC SHA-512. Key exchange: DH Group exchange ($2048 \leq \text{key} \leq 8192$), ECDH: ECDH-sha2-nistp25, ECDH-sha2-nistp38, and ECDH-sha2-nistp521.	Power cycle and terminate session.	Symmetric key used to encrypt data between host and client.
User authentication key	Hash of the user's password: SHA-256, SHA-512.	Zeroize command.	Used to authenticate a user to the cryptographic module.
Crypto Officer authentication key	Hash of the Crypto Officer's password: SHA-256, SHA-512.	Zeroize command.	Used to authenticate the Crypto Officer to the cryptographic module.
RE-to-RE authentication key	HMAC key (manual IPsec SA): HMAC-SHA256-128, HMAC-SHA-256).	Zeroize/explicitly delete command.	Used to authenticate the RE-to-RE IPsec connection.
RE-to-RE encryption key	TDES/AES key (manual IPsec SA).	Zeroize/explicitly delete command.	Used in IPsec connection between REs.
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. During initial configuration, you can also enter the IP Security (IPsec) keys for communication between internal Routing Engines or for logical communications between the Routing Engine and system processes in plain text on the console port (under manual key entry rules).



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

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

**Related
Documentation**

- [Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode on page 32](#)
- [Understanding Zeroization to Clear System Data for FIPS Mode on page 36](#)

Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode

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

- **Length.** Passwords must contain between 10 and 20 characters.
- **Character set requirements.** Passwords must contain at least three of the following five defined character sets:
 - Uppercase letters
 - Lowercase letters
 - Digits
 - Punctuation marks
 - Keyboard characters not included in the other four sets—such as the percent sign (%) and the ampersand (&)
- **Authentication requirements.** All passwords and keys used to authenticate peers must contain at least 10 characters, and in some cases the number of characters must match the digest size—for example, 20 characters for SHA-1 authentication.

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

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

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

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

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

**Related
Documentation**

- [Understanding the Operational Environment for Junos OS in FIPS Mode on page 28](#)

Understanding Requirements for Secure Communication Between Routing Engines in FIPS Mode

The internal IPsec SA provides a secure way to mutually authenticate and encrypt communications between Routing Engines.

The cryptographic boundary on a modular switch is the Routing Engine. For this reason, QFX10008, and QFX10016 switches with dual (redundant) Routing Engines require an internal, manual IP Security (IPsec) security association (SA) configured on each Routing Engine for the Routing Engines to communicate with each other. The Crypto Officer must use the console of each Routing Engine to configure the IPsec SA. Only four parameters are required: SA direction, security parameter index (SPI), a key value for authentication, and a key value for encryption. The SAs must be identical. All values, including the keys, must be statically specified in the configuration and must match on both ends of the connection. For communication to take place, each Routing Engine must have the same configured options.

For details, see:

- [SA Direction on page 33](#)
- [SPI on page 34](#)
- [IPsec Keys on page 34](#)
- [IPsec Limitations on page 34](#)

SA Direction

The internal, manual IPsec security association (SA) established by you, the Crypto Officer, on a Routing Engine can have the same SPI, authentication key, and encryption key for inbound and outbound communication, or one set of values for the inbound tunnel and another set for the outbound tunnel:

- Bidirectional—Apply the same SA values in both directions between Routing Engines.
- Inbound—Apply the SA values only to the inbound IPsec tunnel.
- Outbound—Apply the SA values only to the outbound IPsec tunnel.

If you do not configure the SA to be bidirectional, you must configure two unidirectional IPsec tunnels, one in each direction.



NOTE: We do not recommend the use of unidirectional IPsec tunnels.

SPI

The security parameter index (SPI) is an arbitrary value between 256 and 16639 that uniquely identifies the SA to use at the receiving Routing Engine. The sending Routing Engine uses the SPI to identify and select the SA it uses to secure every packet. The receiving Routing Engine uses the SPI to identify and select the encryption algorithm and key it uses to decrypt packets.

IPsec Keys

The internal, manual IPsec SA established by you, the Crypto Officer, on a Routing Engine requires an authentication key, as well as an encryption key. For this type of SA, we recommend you create preshared keys in hexadecimal format, for maximum key strength. Each key requires a specific cryptographic algorithm:

- Authentication algorithm
 - HMAC-SHA-256 (64 hexadecimal characters)
- Encryption algorithm
 - 3DES-CBC (48 hexadecimal characters)

You use the configuration mode command **prompt** to enter the value for each key twice. If the two entries do not match, the key is not set.

IPsec Limitations

On a switch with Junos OS in FIPS mode enabled, you cannot configure IPsec SAs to use the IPsec Authentication Header (AH) protocol or the Data Encryption Standard (DES) encryption algorithm. Instead, you must use the Encapsulating Security Payload (ESP) protocol for both encryption and authentication.

Related Documentation

- [Understanding Common Criteria and FIPS Terminology and Supported Cryptographic Algorithms on page 18](#)
- For more information about IPsec, see the *Junos OS System Basics Configuration Guide*.

Downloading Software Packages from Juniper Networks

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

- Junos OS for QFX Series switches, Release 18.1R1 and 18.1R2

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.
2. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. Select the appropriate software package:
 - For Junos OS package, ensure that the name contains the correct switch name and number of the Junos OS release that is FIPS-certified on the switches.

For QFX10002, the image is
`jinstall-host-qfx-10-f-x86-64-18.1-R1_tvp.0-secure-signed.tgz`

For QFX10008 and QFX10016, the image is
`jinstall-host-qfx-10-m-x86-64-18.1-R1_tvp.0-secure-signed.tgz`
 - For Junos OS package, ensure that the name contains the correct switch name and number of the Junos OS release that is Common Criteria-certified on the switches.

For QFX10002, the image is
`jinstall-host-qfx-10-f-x86-64-18.1-R2_tvp.0-secure-signed.tgz`

For QFX10008 and QFX10016, the image is
`jinstall-host-qfx-10-m-x86-64-18.1-R2_tvp.0-secure-signed.tgz`
4. Download the software to a local host or to an internal software distribution site.
5. Install the Junos OS. See [“Installing Software on a QFX Series devices with a Single Routing Engine”](#) on page 35.

**Related
Documentation**

- [Installing Software on a QFX Series devices with a Single Routing Engine](#) on page 35

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

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

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

1. Download the software package as described in [“Downloading Software Packages from Juniper Networks”](#) on page 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. (For instructions, see [Configuring a QFX10000 Device](#))
3. (Optional) Back up the current software configuration to a second storage option. See the [Junos OS Installation and Upgrade Guide](#) for instructions on performing this task.

4. (Optional) Copy the software package to the switch. We recommend that you use FTP to copy the file to the `/var/tmp/` directory.

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

5. Install the new package on the switch:

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

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

- For a software package in a local directory on the switch, use `/var/tmp/package.tgz`.
- For a software package on a remote server, use one of the following paths, replacing *package* with the software package name.
 - `ftp://hostname/pathname/package.tgz`
 - `http://hostname/pathname/package.tgz`



NOTE: If you need to terminate the installation, do not reboot your switch; instead, finish the installation and then issue the `request system software delete package.tgz` command, where *package.tgz* is, for example, `jinstall-host-qfx-10-f-x86-64-18.1-R1_tvp.0-secure-signed.tgz`. This is your last chance to stop the installation.

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

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

Related Documentation

- [Software Installation Overview](#)

Understanding Zeroization to Clear System Data for FIPS Mode

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

The Crypto Officer initiates the zeroization process by entering the ***request system zeroize (FIPS)*** operational command from the CLI after enabling FIPS mode. Use of this command is restricted to the Crypto Officer. (To zeroize the system *before* enabling FIPS mode, use the ***request system zeroize media*** command.)



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

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

- [Why Zeroize? on page 37](#)
- [When to Zeroize? on page 37](#)

Why Zeroize?

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



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

When to Zeroize?

As Crypto Officer, perform zeroization in the following situations:

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



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

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

Related Documentation

- [Zeroizing the System on page 38](#)
- [Enabling FIPS Mode on page 40](#)

Zeroizing the System

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

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

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

To zeroize QFX10002 switch:



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

1. From the CLI, enter

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

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

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

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

To zeroize QFX10008 and QFX10016 switch:



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

1. From the CLI, enter

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

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

```
Erase all data, including configuration and log files? [yes, no] (no)
yes
re0:
-----
warning: zeroizing re0
warning: zeroizing re1
...
Rebooting after scrubbing memory...
...
```

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

Related Documentation

- [Enabling FIPS Mode on page 40](#)
- [Understanding Zeroization to Clear System Data for FIPS Mode on page 36](#)

Enabling FIPS Mode

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

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



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

To enable FIPS mode in Junos OS on the switch:

1. Enter configuration mode:

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

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

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

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

3. Commit the configuration:



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

For switches with multiple Routing Engines:

```
{master:0}[edit security]
root@switch# delete ipsec
{master:0}[edit security]
root@switch# commit synchronize
configuration check succeeds
```



```
[edit]
'system'
  reboot is required to transition to FIPS level 1
commit complete
```

For switches with a single Routing Engine:

```
{master:0}[edit security]
root@switch# delete ipsec
{master:0}[edit security]
root@switch# commit
configuration check succeeds
[edit]
'system'
  reboot is required to transition to FIPS level 1
commit complete
```

4. Reboot the switch:

For switches with multiple Routing Engines:

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

For switches with a single Routing Engine:

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

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

```
Creating initial configuration: ...
mgd: Running FIPS Self-tests
mgd: Testing kernel KATS:
mgd:   NIST 800-90 HMAC DRBG Known Answer Test:      Passed
mgd:   DES3-CBC Known Answer Test:                  Passed
mgd:   HMAC-SHA1 Known Answer Test:                  Passed
mgd:   HMAC-SHA2-256 Known Answer Test:              Passed
mgd:   SHA-2-384 Known Answer Test:                  Passed
mgd:   SHA-2-512 Known Answer Test:                  Passed
mgd:   AES128-CMAC Known Answer Test:                Passed
mgd:   AES-CBC Known Answer Test:                   Passed
mgd: Testing MacSec KATS:
mgd:   AES128-CMAC Known Answer Test:                Passed
mgd:   AES256-CMAC Known Answer Test:                Passed
mgd:   AES-KEYWRAP Known Answer Test:                Passed
mgd: Testing libmd KATS:
mgd:   HMAC-SHA1 Known Answer Test:                  Passed
mgd:   HMAC-SHA2-256 Known Answer Test:              Passed
mgd:   SHA-2-512 Known Answer Test:                  Passed
mgd: Testing OpenSSL KATS:
```

```

mgd: 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 exec Authentication error...
verixec: no signatures for device. file='/sbin/kats/cannot-exec' fsid=192

```

```
fileid=51404 gen=1 uid=0 pid=4818
mgd: /sbin/kats/run-tests: /sbin/kats/cannot-exec: Authentication error
mgd: FIPS Self-tests Passed
```

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

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

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

For switches with multiple Routing Engines:

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

For switches with a single Routing Engine:

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

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

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

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

```
user@switch:fips> show version local
fpc0:
-----
Hostname: switch
Model: qfx10002
Junos: 18.1-20171031_18.1R1
JUNOS QFX Software Suite [18.1-20171031_18.1R1]
JUNOS FIPS mode utilities [18.1-20171031_18.1R1]
JUNOS Crypto Software Suite [18.1-20171031_18.1R1]
JUNOS Online Documentation [18.1-20171031_18.1R1]
JUNOS jsd [powerpc-18.1-20171031_18.1R1-jet-1]
JUNOS SDN Software Suite [18.1-20171031_18.1R1]
JUNOS QFX 10002 Software Suite [18.1-20171031_18.1R1]
JUNOS Web Management Platform Package [18.1-20171031_18.1R1]
JUNOS py-base-powerpc [18.1-20171031_18.1R1]
JUNOS py-extensions-powerpc [18.1-20171031_18.1R1]
```



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

Configure FPCs in FIPS Mode

After enabling FIPS mode, configure the Flexible PIC Concentrators (FPCs) in the FIPS mode.

To bring the FPCs up, follow the below procedure:

1. Enter configuration mode:

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

2. Configure FIPS chassis on the switch:

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

3. Install the new package on the switch:

```
[edit]
root@switch# request system software add <package>
```



NOTE: The package should be jpfe-fips*.tgz, for example, jpfe-fips-x86-32-18.1R1_tvp.1.tgz.

4. Commit the configuration:

```
{master:0}[edit security]
root@switch# commit synchronize
```

5. Reboot the switch:

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

- Related Documentation**
- [Understanding Requirements for Secure Communication Between Routing Engines in FIPS Mode on page 33](#)

Establishing Root Password Access

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

As Crypto Officer, you must establish a root password conforming to the FIPS password requirements in [“Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode” on page 32](#). When you enable FIPS mode in Junos OS on the switch, you cannot configure passwords unless they meet this standard.

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

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

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

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

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

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

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

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

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

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

Ensure that you follow the password guidelines in [“Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode”](#) on page 32.

- To configure public keys for SSH authentication of root logins, use the **ssh-eccdsa** option. You can configure more than one public key for SSH authentication of root logins and for user accounts. When a user logs in as **root**, the public keys are referenced to determine whether the private key matches any of them.
4. If you are finished configuring the switch, commit the configuration and exit:

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

Otherwise, go on to [“Enabling FIPS Mode”](#) on page 40.

Related Documentation

- [Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode on page 32](#)
- 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 Login Access on page 46](#)
- [Configuring FIPS User Login Access on page 47](#)

Configuring Crypto Officer Login Access

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

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

To configure login access for a Crypto Officer:

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

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

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

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

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

3. Following the guidelines in “[Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode](#)” on page 32, assign the Crypto Officer a plain-text password for login authentication. Set the password by typing a password after the prompts **New password** and **Retype new password**.

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

4. Optionally, display the configuration:

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

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

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

Otherwise, go on to “[Configuring FIPS User Login Access](#)” on page 47.

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

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

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

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

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

3. Following the guidelines in "[Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode](#)" on page 32, assign the FIPS a plain-text password for login authentication. Set the password by typing a password after the prompts **New password** and **Retype new password**.

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

4. Optionally, display the configuration:

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

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

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


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

- Related Documentation**
- [Understanding Roles and Services for Junos OS in Common Criteria and FIPS on page 25](#)

CHAPTER 3

Configuring Administrative Credentials and Privileges

- [Understanding the Associated Password Rules for an Authorized Administrator on page 51](#)
- [Authentication methods in FIPS mode of Operation on page 52](#)
- [Configuring a Network Device collaborative Protection Profile for an Authorized Administrator on page 53](#)

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.
- 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 3.

```
[ edit ]
administrator@host# set system login password minimum-changes 3
```

- Contain the minimum number of characters required for a password. By default, Junos OS passwords must be at least 6 characters long. The valid range for this option is 6 to 20 characters.

```
[ edit ]
administrator@host# set system login password minimum-length 6
```

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.



NOTE: Passwords should be changed periodically.

**Related
Documentation**

- [Identifying Secure Product Delivery on page 22](#)

Authentication methods in FIPS mode of Operation

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

- [Username and Password Authentication over the Console and SSH on page 53](#)
- [Username and Public Key Authentication over SSH on page 53](#)

Username and Password Authentication over the Console and SSH

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



NOTE: The maximum password length is 20 characters.

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

Therefore, this leads to a maximum of seven possible attempts in a 1-minute period for each getty active terminal. So, the best approach for the attacker would be to disconnect after 4 failed attempts, and wait for a new getty to be spawned. This would allow the attacker to perform roughly 9.6 attempts per minute (576 attempts per hour or 60 minutes). This would be rounded off to 9 attempts per minute, because there is no such thing as 0.6 attempts. Thus the probability of a successful random attempt is 1/9610, which is less than 1/1 million. The probability of a success with multiple consecutive attempts in a 1-minute period is 9/(9610), which is less than 1/100,000.

Username and Public Key Authentication over SSH

With SSH public-key authentication, the user provides the username and proves ownership of the private key corresponding to the public key stored on the server. The device supports ECDSA (P-256, P-384, and P-521) and RSA (2048-bit or higher since our RSA implementation is FIPS 186-4 compliant). The probability of a success with multiple consecutive attempts in a 1-minute period is 5.6e7/(2128).

Related Documentation

- [Configuring SSH on the Evaluated Configuration for NDcPP on page 58](#)

Configuring a Network Device collaborative Protection Profile for an 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 NDcPP Version 2.0 authorized administrator must have all permissions, including the ability to change the router configuration.

To configure an authorized administrator:

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 hashing algorithm used for password storage as sha512.

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

3. Commit the changes.

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

4. Define your NDcPP Version 2.0 user authorized administrator.

```
[edit]
root@host# set system login user user-name 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
```



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.

7. Commit the changes.

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

- Related Documentation**
- [Understanding the Associated Password Rules for an Authorized Administrator on page 51](#)

Configuring SSH and Console Connection

- [Configuring a System Login Message and Announcement on page 57](#)
- [Configuring SSH on the Evaluated Configuration for NDcPP on page 58](#)
- [Configuring SSH on the Evaluated Configuration for FIPS on page 59](#)
- [Limiting the Number of User Login Attempts for SSH Sessions on page 61](#)

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

- Related Documentation**
- [Configuring SSH on the Evaluated Configuration for NDcPP on page 58](#)

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 through remote management. The following algorithms that needs to be configured to validate SSH for NDcPP.

Before you begin, log in with your root account on the device running Junos OS Release 18.1R2 and edit the configuration.



NOTE: You can enter the configuration commands in any order and commit all the commands at once.

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 MAC algorithm:

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

Supported SSH ciphers algorithm:

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

Related Documentation • [Limiting the Number of User Login Attempts for SSH Sessions on page 61](#)

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.

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 MAC algorithm:

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

Supported SSH ciphers algorithm:

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

Limiting the Number of User Login Attempts for SSH Sessions

An administrator may login remotely to a device through SSH. Administrator credentials are stored locally on the device. If the administrator presents a valid username and password, access to the Target of Evaluation (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 2 through 10, and the default value is 3.

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

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

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

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

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

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

attempt after the threshold. The range is from 5 through 10, and the default value is 5 seconds.

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

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

**Related
Documentation**

- [Configuring SSH on the Evaluated Configuration for NDcPP on page 58](#)

CHAPTER 5

Configuring the Remote Syslog Server

- [Syslog Server Configuration on a Linux System on page 63](#)

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 device. 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 and DUT 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/0day4z+z7tQHRFSrxj2G92ao1iVDBLJparEMbc8w
LdSUDxmgBTM2oad0mm+kreBUQjrmr6775RJn9H9YwIxK0xGm4SFnx/V14
R+1Z9RqmKH2wodIEM34K0wXEHZAzNZ01oLmaAVqT
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 69](#)
- [Sample Code Audits of Configuration Changes on page 70](#)

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 QFX10002, QFX10008, and QFX10016 Devices on page 69](#)

Configuring Audit Log Options for QFX10002, QFX10008, and QFX10016 Devices

To configure audit log options for QFX10002, QFX10008, and QFX10016 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 Audit_logs any any
```

3. Specify the size of files to be archived.

```
[edit system syslog]
root@host#set file Audit_logs archive size 10m
```

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

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

5. Log system messages in a structured format.

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

Related Documentation • [Sample Code Audits of Configuration Changes on page 70](#)

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.

```
[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
  }
}
password {
  format sha512;
}
}
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 read-only;
+   authentication {
+     encrypted-password "$ABC123";
+       # SECRET-DATA
+   }
+ }
[edit system radius-server 192.0.2.15]
- secret "$ABC123"; # SECRET-DATA
+ secret "$ABC123"; # SECRET-DATA

```

Table 5 on page 72 shows sample for syslog auditing for NDcPPv2:

Table 5: 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 5: 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 69](#)

CHAPTER 7

Configuring Event Logging

- [Event Logging Overview on page 75](#)
- [Configuring Event Logging to a Local File on page 76](#)
- [Interpreting Event Messages on page 76](#)
- [Logging Changes to Secret Data on page 77](#)
- [Login and Logout Events Using SSH on page 78](#)
- [Logging of Audit Startup on page 79](#)

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.

- Changes to modification or deletion of cryptographic keys.
- Password resets.

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 76](#)

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 75](#)

Interpreting Event Messages

The following output shows a sample event message.

```
Jul 24 17:43:28 router1 mgd[4163]: UI_CFG_AUDIT_SET_SECRET: User 'admin' set: [system
radius-server 1.2.3.4 secret]
```

[Table 6 on page 76](#) 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 6: Fields in Event Messages

Field	Description	Examples
<i>timestamp</i>	<p>Time when the message was generated, in one of two representations:</p> <ul style="list-style-type: none"> • <i>MMM-DD HH:MM:SS.MS+/-HH:MM</i>, 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). • <i>YYYY-MM-DDTHH:MM:SS.MSZ</i> is the year, month, day, hour, minute, second and millisecond in UTC. 	<p>Apr 24 17:43:28 is the timestamp expressed as local time in the United States.</p> <p>2018-04-24T09:17:15.719Z is 9:17 AM UTC on 24 April 2018.</p>

Table 6: Fields in Event Messages (continued)

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

Related Documentation

- [Event Logging Overview on page 75](#)

Logging Changes to Secret Data

The following are examples of audit logs of events that change the secret data.

Load Merge

When a **load merge** command is issued to merge the contents of the example Common Criteria configuration with the contents of the original configuration, the following audit logs are created concerning the secret data:

```

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]
```

Load Replace

When a **load replace** command is issued to replace the contents of the example Common Criteria configuration with the contents of the original configuration, the following audit logs are created concerning the secret data:

```

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]
```

```
Ju1 24 18:29:09 router1 mgd[4163]: UI_CFG_AUDIT_SET_SECRET: User 'admin' replace: [system login user admin authentication encrypted-password]
```

Load Override

When a **load override** command is issued to override the contents of the example Common Criteria configuration with the contents of the original configuration, the following audit logs are created concerning the secret data:

```
Ju1 25 14:25:51 router1 mgd[4153]: UI_LOAD_EVENT: User 'admin' is performing a 'load override'
Ju1 25 14:25:51 router1 mgd[4153]: UI_CFG_AUDIT_OTHER: User 'admin' override: CC_config2.txt
Ju1 25 14:25:51 router1 mgd[4153]: UI_CFG_AUDIT_SET_SECRET: User 'admin' set: [system radius-server 1.2.3.4 secret]
Ju1 25 14:25:51 router1 mgd[4153]: UI_CFG_AUDIT_SET_SECRET: User 'admin' set: [system login user admin authentication encrypted-password]
Ju1 25 14:25:51 router1 mgd[4153]: UI_CFG_AUDIT_SET_SECRET: User 'admin' set: [system login user admin authentication encrypted-password]
```

Load Update

When a **load update** command is issued to update the contents of the example Common Criteria configuration with the contents of the original configuration, the following audit logs are created concerning the secret data:

```
Ju1 25 14:31:03 router1 mgd[4153]: UI_LOAD_EVENT: User 'admin' is performing a 'load update'
Ju1 25 14:31:03 router1 mgd[4153]: UI_CFG_AUDIT_OTHER: User 'admin' update: CC_config2.txt
Ju1 25 14:31:03 router1 mgd[4153]: UI_CFG_AUDIT_SET_SECRET: User 'admin' set: [system radius-server 1.2.3.4 secret]
Ju1 25 14:31:03 router1 mgd[4153]: UI_CFG_AUDIT_OTHER: User 'admin' deactivate: [system radius-server 1.2.3.4 secret] ""
Ju1 25 14:31:03 router1 mgd[4153]: UI_CFG_AUDIT_SET_SECRET: User 'admin' set: [system login user admin authentication encrypted-password]
Ju1 25 14:31:03 router1 mgd[4153]: UI_CFG_AUDIT_OTHER: User 'admin' deactivate: [system login user admin authentication encrypted-password] ""
Ju1 25 14:31:03 router1 mgd[4153]: UI_CFG_AUDIT_SET_SECRET: User 'admin' set: [system login user test authentication encrypted-password]
Ju1 25 14:31:03 router1 mgd[4153]: UI_CFG_AUDIT_OTHER: User 'admin' deactivate: [system login user test 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 76](#)

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 76](#)

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 78](#)

CHAPTER 8

Performing Self-Tests on a Device

- [Understanding FIPS Self-Tests on page 81](#)

Understanding FIPS Self-Tests

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

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

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

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

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

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

Performing Power-On Self-Tests on the Device

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

The module displays the following status output for QFX10008 Series device while running the power-on self-tests:

```
Verified manifest signed by PackageDevelopmentEc_2017 method ECDSA256+SHA256
cp: /var/host/junos-defaults.conf: No such file or directory
mount_cd9660: /dev/gpt/junos: Invalid argument
ifconfig: devop error: Device not configured
  bcmsdk_5_9_x kldKLD bcmsdk_5_9_x.ko: depends on acb - not available or version
mismatch
linker_load_file: Unsupported file type
kldload: an error occurred while loading the module. Please check dmesg(8) for
more details.
Junosprocs mounted on /junosproc.
@ 1511776671 [2017-11-27 09:57:51 UTC] mgd start
Creating initial configuration: ...
mgd: Running FIPS Self-tests
mgd: Testing kernel KATS:
mgd:   NIST 800-90 HMAC DRBG Known Answer Test:           Passed
mgd:   DES3-CBC Known Answer Test:                       Passed
mgd:   HMAC-SHA1 Known Answer Test:                       Passed
mgd:   HMAC-SHA2-256 Known Answer Test:                   Passed
mgd:   SHA-2-384 Known Answer Test:                       Passed
mgd:   SHA-2-512 Known Answer Test:                       Passed
mgd:   AES128-CMAC Known Answer Test:                     Passed
mgd:   AES-CBC Known Answer Test:                         Passed
mgd: Testing MacSec KATS:
mgd:   AES128-CMAC Known Answer Test:                     Passed
mgd:   AES256-CMAC Known Answer Test:                     Passed
mgd:   AES-KEYWRAP Known Answer Test:                     Passed
mgd: Testing libmd KATS:
mgd:   HMAC-SHA1 Known Answer Test:                       Passed
mgd:   HMAC-SHA2-256 Known Answer Test:                   Passed
mgd:   SHA-2-512 Known Answer Test:                       Passed
mgd: Testing OpenSSL KATS:
mgd:   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 exec Authentication error...
verixec: no signatures for device. file='/sbin/kats/cannot-exec' fsid=192
fileid=51404 gen=1 uid=0 pid=4818
mgd: /sbin/kats/run-tests: /sbin/kats/cannot-exec: Authentication error
mgd: FIPS Self-tests Passed

```



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

CHAPTER 9

Configuration Statements

- [algorithm \(FIPS\) on page 86](#)
- [authentication \(FIPS\) on page 87](#)
- [direction \(FIPS\) on page 88](#)
- [fips \(FIPS\) on page 89](#)
- [internal \(FIPS\) on page 90](#)
- [ipsec \(FIPS\) on page 91](#)
- [key \(FIPS\) on page 92](#)
- [level \(FIPS\) on page 93](#)
- [manual \(FIPS\) on page 94](#)
- [protocol esp \(FIPS\) on page 94](#)
- [security \(FIPS\) on page 95](#)
- [spi \(FIPS\) on page 96](#)

algorithm (FIPS)

Syntax	<code>algorithm <name>;</code>
Hierarchy Level	[edit security ipsec internal security-association manual direction authentication], [edit security ipsec internal security-association manual direction encryption]
Release Information	Statement introduced in Junos OS Release 18.1 for QFX Series switches.
Description	Select the authentication and encryption algorithm for an IPsec security association (SA) between internal Routing Engines.
Options	<p>hmac-sha2-256—Use a 256-bit Hash Message Authentication Code (HMAC) based on Secure Hash Algorithm 2 (SHA2) as the authentication algorithm.</p> <p>3des-cbc—Use a triple-Data Encryption Standard (3DES) cipher block chaining (CBC) as the encryption algorithm.</p> <p>aes-256-cbc—AES 256-bit encryption algorithm (64 hexadecimal characters).</p> <p>aes-192-cbc—AES 192-bit encryption algorithm (48 hexadecimal characters).</p> <p>aes-128-cbc—AES 128-bit encryption algorithm (32 hexadecimal characters).</p>
Required Privilege Level	maintenance—To add and view this statement in the configuration.

authentication (FIPS)

Syntax

```
authentication {
  algorithm (hmac-sha2-256);
  key (ascii-text ascii-text-string | hexadecimal key-value);
}
```

Hierarchy Level [edit security ipsec internal security-association manual direction]

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

Description Define the authentication parameters for communication between internal Routing Engines.



NOTE: We recommend using the hexadecimal format for maximum key strength.

The remaining statements are explained separately.

Required Privilege Level maintenance—To view and add this statement in the configuration.

direction (FIPS)

Syntax	<pre> direction (bidirectional inbound outbound) { protocol esp ; spi <i>spi-value</i>; authentication { algorithm (hmac-sha2-256); key (ascii-text <i>ascii-text-string</i> hexadecimal <i>key-value</i>); } encryption { algorithm (3des-cbc aes-128-cbc aes-192-cbc aes-256-cbc des-cbc); key (ascii-text <i>ascii-text</i> hexadecimal <i>hexadecimal</i>); } } </pre>
Hierarchy Level	[edit security ipsec internal security-association manual]
Release Information	Statement introduced in Junos OS Release 18.1 for QFX Series switches.
Description	Establish a manual security association (SA) for communication between internal Routing Engines.
Options	<p>bidirectional—Apply the same SA values in both directions between Routing Engines.</p> <p>inbound—Apply these SA properties only to the inbound IPsec tunnel.</p> <p>outbound—Apply these SA properties only to the outbound IPsec tunnel.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	maintenance—To view and add this statement in the configuration.

fips (FIPS)

Syntax	<pre>fips { level <i>level</i>; }</pre>
Hierarchy Level	[edit system]
Release Information	Statement introduced in Junos OS Release 18.1 for QFX Series switches.
Description	<p>Configure Junos OS Federal Information Processing Standard (FIPS) mode features on a switch.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

internal (FIPS)

```
Syntax  internal {
        security-association {
            manual
            direction (bidirectional | inbound | outbound) {
                protocol esp;
                spi spi-value;
                authentication {
                    algorithm (hmac-sha2-256);
                    key (ascii-text ascii-text-string | hexadecimal key-value);
                }
                encryption {
                    algorithm 3des-cbc;
                    key (ascii-text ascii-text-string | hexadecimal key-value);
                }
            }
        }
    }
```

Hierarchy Level [edit security ipsec]

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

Description Define an internal security association (SA) for communication between internal Routing Engines.

The remaining statements are explained separately.

Required Privilege Level maintenance—To view and add this statement in the configuration.

ipsec (FIPS)

Syntax

```

ipsec {
  internal {
    security-association {
      manual
      direction (bidirectional | inbound | outbound) {
        protocol esp;
        spi spi-value;
        authentication {
          algorithm (hmac-sha2-256);
          key (ascii-text ascii-text-string | hexadecimal key-value);
        }
        encryption {
          algorithm 3des-cbc;
          key (ascii-text ascii-text-string | hexadecimal key-value);
        }
      }
    }
  }
}

```

Hierarchy Level [edit security]


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

Description Set up an Internet Protocol Security (IPsec) hierarchy in which you can define a manual internal security association (SA) for communication between internal Routing Engines.

The remaining statements are explained separately.

Required Privilege Level maintenance—To view and add this statement in the configuration.

key (FIPS)

Syntax	<code>key (ascii-text <i>ascii-text-string</i> hexadecimal <i>key-value</i>);</code>
Hierarchy Level	[edit security ipsec internal security-association manual direction authentication], [edit security ipsec internal security-association manual direction encryption]
Release Information	Statement introduced in Junos OS Release 18.1 for QFX Series switches.
Description	<p>Following FIPS password guidelines, use the prompt command, in configuration mode, to specify one key value each for the authentication algorithm and the encryption algorithm in an internal IPsec security association (SA) between internal Routing Engines. You must specify a value for each algorithm.</p> <hr/> <div>  <p>NOTE: We recommend using the hexadecimal format for maximum key strength.</p> </div> <hr/> <p>You must enter the hexadecimal value for each key twice, and the strings entered must match; otherwise, the key is not set. The hexadecimal key value is never displayed in plain text.</p>
Options	<p>hexadecimal <i>key-value</i>—The encrypted hexadecimal key value:</p> <ul style="list-style-type: none"> For the authentication algorithm (HMAC-SHA-256), enter a key consisting of 64 hexadecimal characters. For the encryption algorithm (3DES-CBC), enter a key consisting of 48 hexadecimal characters.
Required Privilege Level	maintenance—To add and view this statement in the configuration.

level (FIPS)

Syntax	<code>level <i>level</i>;</code>
Hierarchy Level	<code>[edit system fips]</code>
Release Information	Statement introduced in Junos OS Release 18.1 for QFX Series switches.
Description	<p>Set the level for the Junos OS Federal Information Processing Standards (FIPS) mode on the device. Setting the FIPS level to a value other than the default, 0 (zero), enables FIPS mode on the device.</p> <p>Compared to non-FIPS mode, Junos OS in FIPS mode is a nonmodifiable operational environment with limitations.</p>
Options	<p><i>level</i>—FIPS level on a device, from level 1 (lowest) through level 4 (highest). At level 0 (the default), the device is in non-FIPS mode.</p> <p>Range: 0 through 4</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

manual (FIPS)

```
Syntax manual {
    direction (bidirectional | inbound | outbound) {
        protocol esp;
        spi spi-value;
        authentication {
            algorithm (hmac-sha2-256);
            key (ascii-text ascii-text-string | hexadecimal key-value);
        }
        encryption {
            algorithm 3des-cbc;
            key (ascii-text ascii-text-string | hexadecimal key-value);
        }
    }
}
```

Hierarchy Level [edit security ipsec internal security-association]

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

Description Define a manual security association (SA) for communication between internal Routing Engines.

The remaining statements are explained separately.

Required Privilege Level maintenance—To view and add this statement in the configuration.

protocol esp (FIPS)

```
Syntax protocol esp;
```

Hierarchy Level [edit security ipsec internal security-association manual direction]

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

Description Specify the protocol (esp) used for an internal IPsec security association (SA) between internal Routing Engines.

Options **esp**—Use the TCP/IP Encapsulating Security Protocol (ESP).

Required Privilege Level maintenance—To add and view this statement in the configuration.

security (FIPS)

Syntax

```

security {
  ipsec {
    internal {
      security-association {
        manual {
          direction (bidirectional | inbound | outbound) {
            protocol esp;
            spi spi-value;
            authentication {
              algorithm (hmac-sha2-256);
              key (ascii-text ascii-text-string | hexadecimal key-value);
            }
            encryption {
              algorithm 3des-cbc;
              key (ascii-text ascii-text-string | hexadecimal key-value);
            }
          }
        }
      }
    }
  }
}

```

Hierarchy Level [\[edit\]](#)

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

Description Define security parameters for communication between internal Routing Engines.

The remaining statements are explained separately.

Required Privilege Level security—To view and add this statement in the configuration.

spi (FIPS)

Syntax	<code>spi <i>spi-value</i>;</code>
Hierarchy Level	[edit security ipsec internal security-association manual direction]
Release Information	Statement introduced in Junos OS Release 18.1 for QFX Series switches.
Description	Specify the security parameter index (SPI) value for the internal IPsec security association (SA) between internal Routing Engines. The SPI is an arbitrary value that uniquely identifies the SA to use at the receiving Routing Engine. The sending Routing Engine uses the SPI to identify and select the SA it uses to secure every packet. The receiving Routing Engine uses the SPI to identify and select the encryption algorithm and key it uses to decrypt packets.
Options	spi-value —Integer to use for this SPI. Range: 256 through 16639
Required Privilege Level	maintenance—To add and view this statement in the configuration.

CHAPTER 10

Operational Commands

- request system zeroize

request system zeroize

Syntax	<code>request system zeroize</code>
Release Information	Statement introduced in Junos OS Release 18.1 for QFX Series switches.
Description	Erase and replace with zeros all user-created data from Routing Engines.
Options	none—Zeroize all Routing Engines in Junos OS in FIPS mode. You must verify the request by typing yes to proceed. This command is restricted to Crypto Officers because the maintenance permission bit is one of the permission bits, along with secret and control , that distinguishes Crypto Officers from other FIPS users.
Required Privilege Level	maintenance
List of Sample Output	request system zeroize on page 98
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system zeroize

```
crypto-officer@switch:fips> request system zeroize
warning: System will be rebooted and may not boot without configuration
Erase all data, including configuration and log files? [yes, no] (no) yes
re1:
-----
warning: zeroizing re1
warning: zeroizing re0
...
Rebooting after scrubbing memory...
...
```