Juniper Networks | Engineering Simplicity

Junos® OS

FIPS Evaluated Configuration Guide for NFX250 Network Services Platform

Published
2021-05-05

Release
20.1r1

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

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

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

Junos® OS FIPS Evaluated Configuration Guide for NFX250 Network Services Platform
Release 20.1r1
Copyright © 2021 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 | vi

Documentation and Release Notes | **vi**

Documentation Conventions | **vi**

Documentation Feedback | **ix**

Requesting Technical Support | **ix**

- Self-Help Online Tools and Resources | **x**
- Creating a Service Request with JTAC | **x**

1 **Overview**

Understanding Junos OS in FIPS Mode | 12

- About the Cryptographic Boundary on Your NFX250 Network Services Platform | **12**
- How FIPS Mode Differs from Non-FIPS Mode | **13**
- Validated Version of Junos OS in FIPS Mode | **13**

Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms | 14

- FIPS Terminology | **14**
- Supported Cryptographic Algorithms | **15**

2 **Verifying Secure Delivery of the Product**

Verifying Secure Delivery of the Product | 18

- Verifying Product Integrity | **18**
- Verifying Product Authenticity | **18**

Understanding FIPS Error States and System Panic | 19

- FIPS System Panic | **20**
- Memory Allocation Error | **21**
- Error Recovery from Alternate Boot Media | **21**

3 **Configuring Junos OS in FIPS Mode of Operation**

How to Enable and Configure Junos OS in FIPS Mode—Overview | 23

Disabling FIPS Mode | 24

4 Configuring Roles and Authentication Methods

Understanding Roles and Services for Junos OS in FIPS Mode | 26

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 | 29

Software Environment for Junos OS in FIPS Mode | 29

Critical Security Parameters | 29

Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode | 33

Downloading and Installing Junos Software Packages (FIPS Mode) | 34

Downloading Software Packages from Juniper Networks (FIPS Mode) | 35

Installing Software on an NFX250 Network Services Platform with a Single Routing Engine (FIPS Mode) | 36

Establishing Root Password Access (FIPS Mode) | 38

Enabling NFX250 device to FIPS Mode | 39

Configuring Crypto Officer and FIPS User Identification and Access | 40

Configuring Crypto Officer Login Access | 41

Configuring FIPS User Login Access | 42

5 Performing Self-Tests on a Device

Understanding FIPS Self-Tests | 46

Verifying That FIPS Self-Tests Are Taking Place | 46

6 Junos-FIPS Configuration Restrictions

Understanding Remote Access for Junos OS in FIPS Mode | 50

Understanding Configuration Limitations and Restrictions on Junos OS in FIPS Mode | 50

1

Configuration Statements and Operational Commands

Configuration Statements | 54

internal (FIPS) | **55**

ipsec (FIPS) | **56**

key (FIPS) | **57**

manual (FIPS) | **59**

security (FIPS) | **60**

Operational Commands for Junos OS in FIPS Mode | 62

request system zeroize (FIPS) | **63**

About the Documentation

IN THIS SECTION

- Documentation and Release Notes | vi
- Documentation Conventions | vi
- Documentation Feedback | ix
- Requesting Technical Support | ix

Use this guide to operate NFX250 Network Services Platform in FIPS 140-2 Level 1 environment. FIPS 140-2 defines security levels for hardware and software that perform cryptographic functions.

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at https://www.juniper.net/documentation/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at https://www.juniper.net/books.

Documentation Conventions

Table 1 on page vii 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 vii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric *metric*>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [*community-ids*]**

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

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		

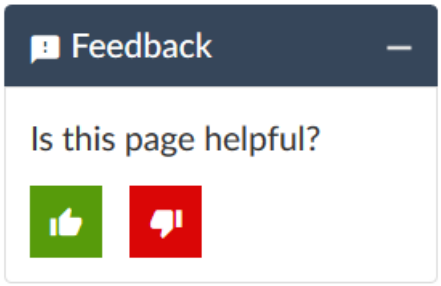
Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

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

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



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

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are

covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: https://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- Create a service request online: https://myjuniper.juniper.net

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

Creating a Service Request with JTAC

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

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

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

1

CHAPTER

Overview

Understanding Junos OS in FIPS Mode | **12**

Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms | **14**

Understanding Junos OS in FIPS Mode

IN THIS SECTION

- About the Cryptographic Boundary on Your NFX250 Network Services Platform | 12
- How FIPS Mode Differs from Non-FIPS Mode | 13
- Validated Version of Junos OS in FIPS Mode | 13

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 NFX250 Network Services Platform running the Juniper Networks Junos operating system (Junos OS) in *FIPS mode* comply with the FIPS 140-2 Level 1 standard.

Operating NFX250 Network Services Platform in a FIPS 140-2 Level 1 environment requires enabling and configuring FIPS mode on the NFX250 device 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 user types can also perform normal configuration tasks on the NFX250 device (such as modify interface types) as individual user configuration allows.

About the Cryptographic Boundary on Your NFX250 Network Services Platform

FIPS 140-2 compliance requires a defined *cryptographic boundary* around each *cryptographic module* on an NFX250 device. Junos OS in FIPS mode prevents the cryptographic module from executing any software that is not part of the FIPS-certified distribution, and allows only FIPS-approved cryptographic algorithms to be used. No critical security parameters (CSPs), such as passwords and keys, can cross the cryptographic boundary of the module by, for example, being displayed on a console or written to an external log file.

For the NFX250 Network Services Platform 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 NFX250 Network Services Platform and the cryptographic boundary of each NFX250 device, see Table 3 on page 13.

Table 3: Cryptographic Boundaries on FIPS-Certified NFX250 Network Services Platform

Switch	Cryptographic Boundary
NFX250	Switch case

How FIPS Mode Differs from Non-FIPS Mode

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

- Self-tests of all cryptographic algorithms are performed at startup.
- Self-tests of random number and key generation are performed continuously.
- Weak cryptographic algorithms such as Data Encryption Standard (DES) and 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.
- *Junos FIPS mode* is a software package that must be installed in order to enable FIPS mode on NFX250 Network Services Platform. The *Junos-FIPS image* is a optional package included within Junos OS image available for NFX250 Network Services Platform.
- Junos FIPS mode is available only on the NFX250 Network Services Platform listed in Table 3 on page 13 that are running Junos OS Release 20.1R1.
- Access to the NFX250 device is through FIPS approved Junos Control Plane (JCP) only. There is no external access to JDM or hypervisor.
- VNFs configurations should not be configured.

For specific configuration limitations and restrictions, see "Understanding Configuration Limitations and Restrictions on Junos OS in FIPS Mode" on page 50.

Validated Version of Junos OS in FIPS Mode

Juniper Networks submits one Junos OS release per year—Junos OS Release 20.1R1, for example—to the National Institute of Standards and Technology (NIST) for validation. To determine whether a Junos OS release is NIST-validated, see the software download page on the Juniper Networks Web site (https://www.juniper.net/) or the National Institute of Standards and Technology site.

RELATED DOCUMENTATION

Verifying Secure Delivery of the Product | 18

Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms

IN THIS SECTION

FIPS Terminology | 14
Supported Cryptographic Algorithms | 15

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

FIPS Terminology

Critical security parameter (CSP)—Security-related information—for example, secret and private cryptographic keys and authentication data such as passwords and personal identification numbers (PINs)—whose disclosure or modification can compromise the security of a cryptographic module or the information it protects. For details, see "Understanding the Operational Environment for Junos OS in FIPS Mode" on page 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. NFX250 Network Services Platform is certified at FIPS 140-2 Level 1. For fixed-configuration NFX250 device, the cryptographic module is the NFX250 device case. For modular NFX250 device, 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 an NFX250 device. For details, see "Understanding Roles and Services for Junos OS in FIPS Mode" on page 26.

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

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

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

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

KATs—Known answer tests. System self-tests that validate the output of cryptographic algorithms approved for FIPS and test the integrity of some Junos OS modules. For details, see "Understanding FIPS Self-Tests" on page 46.

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 an NFX250 device before its operation as a FIPS cryptographic module—or in preparation for repurposing the NFX250 device for non-FIPS operation. The Crypto Officer can zeroize the system with a CLI operational command.

Supported Cryptographic Algorithms

Each implementation of an algorithm is checked by a series of known answer test (KAT) self-tests. Any self-test failure results in a FIPS error state.

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

The following cryptographic algorithms are supported in FIPS mode. Symmetric methods use the same key for encryption and decryption, while asymmetric methods (preferred) use different keys for encryption and decryption.

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

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

ECDSA—Elliptic Curve Digital Signature Algorithm. A variant of the Digital Signature Algorithm (DSA) that uses cryptography based on the algebraic structure of elliptic curves over finite fields. The bit size of the elliptic curve determines the difficulty of decrypting the key. The public key believed to be needed for ECDSA is about twice the size of the security level, in bits. ECDSA using the P-256 curve can be configured under OpenSSH.

HMAC—Defined as "Keyed-Hashing for Message Authentication" in RFC 2104, HMAC combines hashing algorithms with cryptographic keys for message authentication. For Junos OS in FIPS mode, HMAC uses the iterated cryptographic hash 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).

RELATED DOCUMENTATION

Understanding FIPS Self-Tests | 46

2
CHAPTER

Verifying Secure Delivery of the Product

Verifying Secure Delivery of the Product | **18**

Understanding FIPS Error States and System Panic | **19**

Verifying Secure Delivery of the Product

IN THIS SECTION

- Verifying Product Integrity | 18
- Verifying Product Authenticity | 18

Use the following checklists to verify the secure delivery of your Juniper Networks product:

Verifying Product Integrity

To ensure that you received a product that was not tampered with, perform the following checks upon receipt of your Juniper Networks product to verify its integrity:

- Shipping label—Ensure that the shipping label correctly identifies your correct customer name and address as well as the Juniper Networks product you ordered.
- 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 product.
- Inside packaging—Inspect the plastic bag and seal. Ensure that the bag is not cut or removed. Ensure that the seal is intact.

If you identify a problem during the inspection, immediately contact the supplier and provide the order number, tracking number, and a description of the problem.

Verifying Product Authenticity

Perform the following checks upon receipt of your Juniper Networks product to verify its authenticity:

- Verify that the product was ordered using a purchase order. Juniper Networks products are never shipped without a purchase order.
- When a product 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

- Perform the following additional checks to ensure that the box you received was sent by Juniper Networks and not a different company masquerading as Juniper Networks. To verify that a shipment was initiated by Juniper Networks:
  - 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 you received.
  - Log in to the Juniper Networks online customer support portal at https://www.juniper.net/customers/csc/management to view the order status.

RELATED DOCUMENTATION

Understanding FIPS Error States and System Panic

IN THIS SECTION

- FIPS System Panic | **20**
- Memory Allocation Error | **21**
- Error Recovery from Alternate Boot Media | **21**

An NFX250 device operating Junos OS in FIPS mode has certain operational restrictions such as the ability to load only integrity-checked software files and use only FIPS-approved cryptographic algorithms. To ensure correct operation, the NFX250 device performs a series of FIPS self-tests.

The NFX250 device performs additional tests as needed—for example, to ensure that randomly generated numbers are truly random and to verify manually entered keys (passwords).

If it fails a test, the NFX250 device enters a FIPS error state known as *system panic*.

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

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

For details, see:

FIPS System Panic

If an NFX250 device fails a FIPS self-test, the NFX250 device enters a FIPS error state known as *system panic*. The panic condition halts all cryptographic processing and stops all data output from the NFX250 device. To clear the FIPS error, NFX250 device reboots, runs the FIPS self-tests, and if it passes all the tests, returns to normal operation.

If NFX250 device fails a self-test during a reboot from panic mode, the system stops booting and attempts to reboot. If the reboot is unsuccessful, the NFX250 device attempts again to reboot, this time from available boot media.

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

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

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

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

The following error states create a system panic:

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

- The NFX250 device failed a known answer test (KAT).
- The random number is not random.
- Signature generation failed.

- Signature verification failed.
- Certificate verification failed.
- Encryption or decryption failed.
- An environment error occurred.
- An error occurred in a pair-wise conditional test.

Memory Allocation Error

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

FIPS memory failures are logged as follows:

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

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

Error Recovery from Alternate Boot Media

An NFX250 Network Services Platform running Junos OS in FIPS mode performs KATs self-tests at startup. If the NFX250 device fails a KAT, the boot process stops and the NFX250 device attempts to reboot. If the reboot is unsuccessful, the NFX250 device attempts again to reboot, this time from available boot media.

To recover the device in this scenario, the Crypto Officer must remove the tamper-evident seal from the USB port and insert the removable boot media so that the system can boot normally and install Junos OS.

However, if the seal is broken, the NFX250 device is no longer a FIPS cryptographic module. You as Crypto Officer must zeroize, reinstall and reconfigure Junos OS and enable FIPS mode.

RELATED DOCUMENTATION

3

CHAPTER

Configuring Junos OS in FIPS Mode of Operation

How to Enable and Configure Junos OS in FIPS Mode—Overview | 23

Disabling FIPS Mode | 24

How to Enable and Configure Junos OS in FIPS Mode—Overview

You, as Crypto Officer, can enable and configure Junos OS in FIPS mode on your NFX250 device.

Before you begin enabling and configuring FIPS mode on the NFX250 device:

- Verify the secure delivery of your NFX250 device. See "Verifying Secure Delivery of the Product" on page 18.

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

1. Install the Junos OS Release 20.1R1image, if you have not already done so. See "Downloading and Installing Junos Software Packages (FIPS Mode)" on page 34.

2. Establish root password access according to FIPS guidelines. See "Establishing Root Password Access (FIPS Mode)" on page 38.

3. Enable FIPS mode, and commit. See "Enabling NFX250 device to FIPS Mode" on page 39.

4. Configure local login authentication for Crypto Officer access and other FIPS users. See "Configuring Crypto Officer and FIPS User Identification and Access" on page 40.

After you as the Crypto Officer complete Junos OS in FIPS mode configuration, you can connect the NFX250 device to the network and proceed with normal configuration.

Configuring JDM in FIPS mode:

- After you logon to NFX250 FIPS mode, by default, you will be in vjunos0. You can log on to JDM using **ssh jdm** command from vjunos0. You can configure JDM CLI commands from JDM.

RELATED DOCUMENTATION

Understanding Junos OS in FIPS Mode | 12

Disabling FIPS Mode

You might need to disable FIPS mode on your NFX250 to return it to non-FIPS operation.

> **BEST PRACTICE:** For FIPS 140-2 compliance, you must zeroize the system to remove sensitive information before disabling FIPS mode on the NFX250 device. In addition, If the USB tamper proof seal is damaged, then in such case the device should be zeroized.

To disable FIPS mode in Junos OS:

1. Log in to the NFX250 device if you have not already done so:

```
{master:0}
  root:fips>
```

2. Delete the FIPS mode by issuing **request system zeroize** command. System reboots without any FIPS configuration.

```
{master:0}
  root: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
```

RELATED DOCUMENTATION

Enabling NFX250 device to FIPS Mode | 39

4

CHAPTER

Configuring Roles and Authentication Methods

Understanding Roles and Services for Junos OS in FIPS Mode | **26**

Understanding the Operational Environment for Junos OS in FIPS Mode | **28**

Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode | **33**

Downloading and Installing Junos Software Packages (FIPS Mode) | **34**

Downloading Software Packages from Juniper Networks (FIPS Mode) | **35**

Installing Software on an NFX250 Network Services Platform with a Single Routing Engine (FIPS Mode) | **36**

Establishing Root Password Access (FIPS Mode) | **38**

Enabling NFX250 device to FIPS Mode | **39**

Configuring Crypto Officer and FIPS User Identification and Access | **40**

Understanding Roles and Services for Junos OS in FIPS Mode

IN THIS SECTION

- Crypto Officer Role and Responsibilities | 26
- FIPS User Role and Responsibilities | 27
- What Is Expected of All FIPS Users | 27

The Juniper Networks Junos operating system (Junos OS) running in non-FIPS mode allows a wide range of capabilities for users, and authentication is identity-based. In contrast, the FIPS 140-2 standard defines two user roles: *Crypto Officer* and *FIPS user*. These roles are defined in terms of Junos OS user capabilities.

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

In addition to their FIPS roles, both user types can perform normal configuration tasks on the NFX250 device 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

The Crypto Officer is the person responsible for enabling, configuring, monitoring, and maintaining Junos OS in FIPS mode on a device. The Crypto Officer securely installs Junos OS on the NFX250 device, enables FIPS mode, establishes keys and passwords for other users and software modules, and initializes the device before network connection.

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

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 the logs for events of interest.
- Erase user-generated files and data on (zeroize) the NFX250 device.

FIPS User Role and Responsibilities

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

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 device and perform other tasks that are not specific to FIPS mode. FIPS users who are not Crypto Officers can perform reboots and 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 NFX250 device and documentation in a secure area.
- Deploy NFX250 device in secure areas.
- 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

Configuring Crypto Officer and FIPS User Identification and Access | 40

Understanding the Operational Environment for Junos OS in FIPS Mode

IN THIS SECTION

Hardware Environment for Junos OS in FIPS Mode | 29
Software Environment for Junos OS in FIPS Mode | 29
Critical Security Parameters | 29

An NFX250 Network Services Platform running the Juniper Networks Junos operating system (Junos OS) in FIPS mode forms a special type of hardware and software operational environment that is different from the environment of NFX250 device in non-FIPS mode:

Hardware Environment for Junos OS in FIPS Mode

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

For more information about the cryptographic boundary on your NFX250 , see "Understanding Junos OS in FIPS Mode" on page 12.

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

Software Environment for Junos OS in FIPS Mode

An NFX250 Network Services Platform running Junos OS in FIPS mode forms a special type of nonmodifiable operational environment. To achieve this environment on the NFX250 device, the system prevents the execution of any binary file that was not part of the certified Junos OS distribution. When an NFX250 device is in FIPS mode, it can run only Junos OS.

FIPS mode on NFX250 Network Services Platform is available starting with Junos OS Release 20.1R1. The Junos OS in FIPS mode software environment is established after the Crypto Officer successfully enables FIPS mode on an NFX250 Network Services Platform. The Junos OS Release 20.1R1image that includes FIPS mode is available on the Juniper Networks website and can be installed on an NFX250 Network Services Platform.

> **NOTE:** Do not attach the device 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 NFX250 device or Routing Engine as a cryptographic module.

Table 4 on page 31 lists CSPs on NFX250 devices running Junos OS.

Table 4: Critical Security Parameters

CSP	Description	Zeroize	Use
SSH-2 private host key	ECDSA key used to identify the host, generated the first time SSH is configured.	Zeroize command.	Used to identify the host.
SSH-2 session key	Session key used with SSH-2. Encryption: 3DES, AES-128, AES-192, AES-256. MACs: HMAC-SHA-1, HMAC-SHA-256, HMAC- SHA-512, HMAC-SHA-224, HMAC-SHA-384. Key exchange: ECDH Prime curve NID_secp521r1 (NIST Curve P-521).	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-1, SHA-256, SHA-512. **NOTE:** SHA-1 is not recommended to use for password hashing.	Zeroize command.	Used to authenticate a user to the cryptographic module.
Crypto Officer authentication key	Hash of the Crypto Officer's password: SHA-1, SHA-256, SHA-512. **NOTE:** SHA-1 is not recommended to use for password hashing.	Zeroize command.	Used to authenticate the Crypto Officer to the cryptographic module.
HMAC DRBG seed	Seed for deterministic randon bit generator (DRBG).	Seed is not stored by the cryptographic module.	Used for seeding DRBG.
HMAC DRBG V value	The value (V) of output block length (outlen) in bits, which is updated each time another outlen bits of output are produced.	Power cycle.	A critical value of the internal state of DRBG.
HMAC DRBG key value	The current value of the outlen-bit key, which is updated at least once each time that the DRBG mechanism generates pseudorandom bits.	Power cycle.	A critical value of the internal state of DRBG.
NDRNG entropy	Used as entropy input string to the HMAC DRBG.	Power cycle.	A critical value of the internal state of DRBG.

In Junos OS in FIPS mode, all CSPs must enter and leave the cryptographic module in encrypted form. Any CSP encrypted with a non-approved algorithm is considered plain text by FIPS. However, as the Crypto Officer, you can enter user authentication data in plain text.

> **BEST PRACTICE:** For FIPS compliance, configure the NFX250 device over SSH connections because they are encrypted connections.

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.

RELATED DOCUMENTATION

- Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms | **14**
- Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode | **33**
- Understanding Configuration Limitations and Restrictions on Junos OS in FIPS Mode | **50**

Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode

Ensure that the NFX250 device 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. For a list of supported cryptographic algorithms (ciphers), see "Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms" on page 14.

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 FIPS Mode Terminology and Supported Cryptographic Algorithms | **14**

Understanding the Operational Environment for Junos OS in FIPS Mode | **28**

Downloading and Installing Junos Software Packages (FIPS Mode)

NFX250 Network Services Platform can provide the security defined by Federal Information Processing Standards (FIPS) 140-2 Level 1 if these NFX250 devices are operated in the Junos OS in FIPS mode. To operate in Junos OS in FIPS mode, the NFX250 device must have the following software packages installed:

- Junos OS for NFX250 Network Services Platform, Release 20.1R1

To install these software packages, perform the following tasks:

1. Download the Junos OS package and the Junos FIPS mode package from https://www.juniper.net/. See "Downloading Software Packages from Juniper Networks (FIPS Mode)" on page 35.

2. Connect locally to the console port of the active Routing Engine on the NFX250 device.

3. Copy the Junos OS package to the Routing Engine. See the instructions that are appropriate for your NFX250 device:

   - Installing Software on an NFX250 Network Services Platform with a Single Routing Engine (FIPS Mode) on page 36

RELATED DOCUMENTATION

Installing Software on an NFX250 Network Services Platform with a Single Routing Engine (FIPS Mode) | 36

Downloading Software Packages from Juniper Networks (FIPS Mode)

You can download the following Junos OS software packages from the Juniper Networks website:

- Junos OS for NFX250 Network Services Platform, Release 20.1R1

Before you begin to download the software, ensure that you have a Juniper Networks Web account and a valid support contract. To obtain an account, complete the registration form at the Juniper Networks website: https://www.juniper.net/registration/Register.jsp.

> **NOTE:** NFX250 device is supported only on non-flex image. You have to upgrade to the non-flex image to enable fips mode.

To download software packages from Juniper Networks:

1. Using a Web browser, follow the links to the download URL on the Juniper Networks webpage.

   https://www.juniper.net/support/downloads/junos.html

2. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.

3. Select the appropriate software package:

   - For Junos OS package, ensure that the name contains the correct device name and number of the Junos OS release that is FIPS-certified on NFX250 Network Services Platform.

     For example, **jinstall-host-nfx-2-x86-64-20.1R1-secure-signed.tgz**

4. Download the software to a local host or to an internal software distribution site.

5. Install the Junos OS and Junos FIPS mode packages. See “Installing Software on an NFX250 Network Services Platform with a Single Routing Engine (FIPS Mode)” on page 36.

RELATED DOCUMENTATION

Installing Software on an NFX250 Network Services Platform with a Single Routing Engine (FIPS Mode) | 36

Installing Software on an NFX250 Network Services Platform with a Single Routing Engine (FIPS Mode)

You can use this procedure to upgrade Junos OS on an NFX250 Network Services Platform with a single Routing Engine.

To install software upgrades on an NFX250 device with a single Routing Engine:

1. Download the software package as described in "Downloading Software Packages from Juniper Networks (FIPS Mode)" on page 35.

2. If you have not already done so, connect to the console port on the NFX250 device from your management device, and log in to the JDM CLI. (For instructions, see Configuring an NFX250 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 NFX250 device. We recommend that you use FTP to copy the file to the **/var/tmp/** directory.

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

5. Install the new package on the NFX250 device:

   ```
   user@jdm> request system software add package
   ```

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

   - For a software package in a local directory on the NFX250 device, use **/var/tmp/*package*.tgz**.
     - **ftp://*hostname*/*pathname*/*package*.tgz**
     - **http://*hostname*/*pathname*/*package*.tgz**

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

   ```
   user@jdm>  request system reboot
   ```

7. After the reboot has completed, log in and use the **show version** command to verify that the new version of the software is successfully installed. If you installed the Junos FIPS mode package, verify that the FIPS mode utilities are present—as shown in the following example:

```
user@jdm>  show version detail local
Hostname: jdm
Model: <device>
JUNOS Host Software [3.14.61-rt58-WR7.0.0.13_ovp:3.0.4]
JUNOS Host nfx-2 platform package [20.1R1]
JUNOS Host nfx-2 base package [20.1R1]
JUNOS Host nfx-2 control-plane package [20.1R1]
JUNOS Host nfx-2 data-plane package [20.1R1]
JUNOS Host qfx-jdm package [20.1R1]
KERNEL 3.14.61-rt58-WR7.0.0.13_ovp
MGD release 20.1R1-secure [dc-builder] built by dc-builder on 2017-07-29 02:06:12
 UTC
CLI release 20.1R1-secure built by dc-builder on 2017-07-29 02:06:15 UTC
SDXD release 20.1R1-secure [dc-builder] built by dc-builder on 2017-07-29 02:06:21
 UTC
base-actions-dd release 20.1R1-secure [dc-builder] built by dc-builder on
2017-07-29 02:04:42 UTC
jdm-actions-dd release 20.1R1-secure [dc-builder] built by dc-builder on 2017-07-29
 02:04:45 UTC
jdmd-actions-dd release 20.1R1-secure [dc-builder] built by dc-builder on
2017-07-29 02:04:48 UTC

{master:0}
root@jdm>
```

RELATED DOCUMENTATION

- Troubleshooting Software Installation

Establishing Root Password Access (FIPS Mode)

As Crypto Officer, you must establish a root password conforming to the FIPS password requirements in "Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode" on page 33. When you enable FIPS mode in Junos OS on the device, you cannot configure passwords unless they meet this standard.

Local passwords are encrypted with the secure hash algorithm 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 NFX250 device as follows:

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

   ```
   {master:0}
   jdm-sysuser> configure
   Entering configuration mode
   ```

2. 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.

     ```
     {master:0}
     [edit system ]
     jdm-sysuser#set 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 33.

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

3. If you are finished configuring the NFX250 device, commit the configuration and quit:

   ```
   {master:0}
   ```

```
[edit]
jdm-sysuser# commit
commit complete
jdm-sysuser# quit
```

RELATED DOCUMENTATION

- Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode | 33
- For more information about the root password and root logins, see the *Junos OS System Basics Configuration Guide*.
- Understanding Remote Access for Junos OS in FIPS Mode | 50

Enabling NFX250 device to FIPS Mode

FIPS mode is not automatically enabled when you install Junos OS on the NFX250 device.

As Crypto Officer, you must explicitly transition the device from non-FIPS mode to the FIPS mode for which NFX250 Network Services Platform are certified.

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 device:

1. Enter in to JDM from NFX250 device.

```
root@jdm> ssh jdm-sysuser@vjunos0
   --- JUNOS 20.1R1.10 Kernel 64-bit  JNPR-10.3-20180204.bcafb2a_buil
```

2. Add FIPS package on the device.

```
jdm-sysuser> request system software add optional://fips-mode.tgz
```

```
    Verified fips-mode signed by PackageProductionEc_2018 method ECDSA256+SHA256
```

3. Establish root password access according to FIPS guidelines. See "Establishing Root Password Access (FIPS Mode)" on page 38

4. Initiate zeroize operation to change the Junos OS in to FIPS mode.

```
root@jdm> request system zeroize to-fips
warning: System will be rebooted and current installation will be zeroized.
    warning: This will stop all VNFs and remove all VNF images and data.
    warning: All user configuration (except vjunos0) and data shall be deleted.
    Reboot system to switch device to FIPS mode? [yes,no] (no) yes

    Staging zeroize (to_fips) operation ...
    System should be kept powered on until operation completes.
```

NOTE: The configuration **set system fips level 1** is automatically configured when FIPS transition is completed.

RELATED DOCUMENTATION

Disabling FIPS Mode | 24

Understanding Junos OS in FIPS Mode | 12

Configuring Crypto Officer and FIPS User Identification and Access

IN THIS SECTION

Configuring Crypto Officer Login Access | 41

Configuring FIPS User Login Access | 42

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

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

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

To configure login access for a Crypto Officer:

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

```
{master:0}
  root:fips> configure
     Entering configuration mode
{master:0} [edit]
root: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: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 33, assign the Crypto Officer a plain-text password for login authentication. Set the password by typing a password after the prompts **New password** and **Retype new password**.

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

4. Optionally, display the configuration:

```
[edit]
root:fips# edit system
[edit system]
root: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 NFX250 device, commit the configuration and exit:

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

Otherwise, go on to "Configuring FIPS User Login Access" on page 42.

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

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

2. Give the user a username, assign the FIPS user a user ID (for example, **6401**) and a class (for example, **operator**). 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:fips# set system login user fips-user1 uid 6401 class operator
   ```

3. Following the guidelines in "Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode" on page 33, 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:fips# set system login user fips-user1 class operator authentication plain-text-password
   ```

4. Optionally, display the configuration:

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

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

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

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

RELATED DOCUMENTATION

Understanding Roles and Services for Junos OS in FIPS Mode | 26

5
CHAPTER

Performing Self-Tests on a Device

Understanding FIPS Self-Tests | **46**

Verifying That FIPS Self-Tests Are Taking Place | **46**

Understanding FIPS Self-Tests

The cryptographic module enforces security rules to ensure that an NFX250 device running the Juniper Networks Junos operating system (Junos OS) in FIPS mode meets the security requirements of FIPS 140-2 Level 1. To validate the output of cryptographic algorithms approved for FIPS and test the integrity of some system modules, the system performs the following series of known answer test (KAT) self-tests:

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

The KAT self-tests are performed automatically at startup and reboot, regardless of whether FIPS mode is enabled on the NFX250 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 system fails a KAT, it writes the details to a system log file, enters FIPS error state (panic), and reboots the NFX250 device.

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

RELATED DOCUMENTATION

Understanding FIPS Error States and System Panic | 19

Verifying That FIPS Self-Tests Are Taking Place

Purpose

Verify that FIPS self-tests are taking place on the NFX250 device.

Action

You can run FIPS self-tests manually by issuing the **request system fips self-test** command.

```
{master:0}
```

root:fips> **request system fips self-test**

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

```
  AES-CBC Known Answer Test:                        Passed
  AES-GCM Known Answer Test:                        Passed
  SSH-RSA-ENC Known Answer Test:                    Passed
  SSH-RSA-SIGN Known Answer Test:                   Passed
  KDF-IKE-V1 Known Answer Test:                     Passed
  KDF-IKE-V2 Known Answer Test:                     Passed
Testing SSH IPsec KATS:
  NIST 800-90 HMAC DRBG Known Answer Test:          Passed
  DES3-CBC Known Answer Test:                       Passed
  HMAC-SHA1 Known Answer Test:                      Passed
  HMAC-SHA2-256 Known Answer Test:                  Passed
  AES-CBC Known Answer Test:                        Passed
  SSH-RSA-ENC Known Answer Test:                    Passed
  SSH-RSA-SIGN Known Answer Test:                   Passed
  KDF-IKE-V1 Known Answer Test:                     Passed
Testing file integrity:
  File integrity Known Answer Test:                 Passed
Testing crypto integrity:
  Crypto integrity Known Answer Test:               Passed
Expect an exec Authentication error...
/sbin/kats/run-tests: /sbin/kats/cannot-exec: Authentication error

{master:0}
```

After a self-test is run on the NFX250 device, the system log (syslog) file is updated to display the known answer tests (KATs) that are executed. To view the system log file, issue the command **file show /var/log/messages**. The system log file displays the date and time at which each KAT was executed, the name of the test, and its status.

RELATED DOCUMENTATION

Understanding FIPS Self-Tests | 46

CHAPTER 6

Junos-FIPS Configuration Restrictions

Understanding Remote Access for Junos OS in FIPS Mode | 50

Understanding Configuration Limitations and Restrictions on Junos OS in FIPS Mode | 50

Understanding Remote Access for Junos OS in FIPS Mode

When the NFX250 device is in Junos OS in FIPS mode, only SSH is available as a remote access service. To secure the information sent on administrative connections, use SSHv2 for CLI configuration. For SSH configuration information, see the *Junos OS System Basics Configuration Guide*.

> **BEST PRACTICE:** For FIPS compliance, configure the NFX250 device over SSH connections because they are encrypted connections.

The Ethernet management (MGMT) port on the NFX250 device is enabled by default.

In Junos OS in FIPS mode, all critical security parameters (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.

RELATED DOCUMENTATION

Understanding Configuration Limitations and Restrictions on Junos OS in FIPS Mode | 50

Junos OS System Basics and Services Command Reference

Understanding Configuration Limitations and Restrictions on Junos OS in FIPS Mode

In FIPS mode, an NFX250 device operates as a nonmodifiable operational environment in which only files shipped as part of Junos OS can be executed.

In contrast to non-FIPS mode, Junos OS in FIPS mode:

- Conforms to FIPS 140-2.
- Requires special installation procedures.
- Mandates the use of internal, manual IPsec tunnels with specific requirements.
- Limits services used for remote access.

- Allows only the use of approved ciphers.
- Requires user logout on disconnect at the console.
- Sets strict requirements for passwords.
- Requires special system logging considerations.
- Disables the following Junos OS protocols and services so that you cannot configure them. Attempts to configure these services or to load configurations with these services configured result in a configuration syntax error.
  - finger
  - FTP
  - rlogin
  - rsh
  - Telnet
  - Trivial File Transfer Protocol (TFTP)
  - Transport Layer Security (TLS) protocol
  - xnm-clear-text

  If you try to load a configuration that includes statements not supported by Junos OS in FIPS mode, you see a warning message. For example, suppose you attempt to configure Telnet for remote access:

```
[edit]
crypto-officer:fips# set system services telnet
```

  You receive the following warning and cannot add the **system services telnet** statement to the loaded configuration:

```
[edit]
'telnet'
warning: not allowed in JUNOS-FIPS; ignored
```

RELATED DOCUMENTATION

- Understanding Junos OS in FIPS Mode | 12
- Understanding Remote Access for Junos OS in FIPS Mode | 50
- Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms | 14
- Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode | 33

1

PART

Configuration Statements and Operational Commands

Configuration Statements | 54

Operational Commands for Junos OS in FIPS Mode | 62

CHAPTER 7

Configuration Statements

IN THIS CHAPTER

- internal (FIPS) | **55**
- ipsec (FIPS) | **56**
- key (FIPS) | **57**
- manual (FIPS) | **59**
- security (FIPS) | **60**

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 20.1R1for NFX series.

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.

RELATED DOCUMENTATION

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 20.1R1for NFX series.

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.

RELATED DOCUMENTATION

key (FIPS)

Syntax

```
key (ascii-text ascii-text-string | hexadecimal key-value);
```

Hierarchy Level

```
[edit security ipsec internal security-association manual direction bidirectional manual direction bidirectional
    authentication]
[edit security ipsec internal security-association manual direction bidirectional manual direction inbound
    authentication]
[edit security ipsec internal security-association manual direction bidirectional manual direction outbound
    authentication]
```

Release Information

Statement introduced in Junos OS Release 20.1R1for NFX series.

Description

Following FIPS password guidelines, use the **prompt** command, in configuration mode, to specify one key (password) 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.

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

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.

Options

hexadecimal *key-value*—The encrypted hexadecimal key value:

- 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.

RELATED DOCUMENTATION

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 20.1R1for NFX series.

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.

RELATED DOCUMENTATION

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 20.1R1for NFX series.

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.

RELATED DOCUMENTATION

CHAPTER 8

Operational Commands for Junos OS in FIPS Mode

IN THIS CHAPTER

- request system zeroize (FIPS) | 63

request system zeroize (FIPS)

Syntax

request system zeroize

Release Information

Command introduced in Junos OS Release 20.1R1for NFX series.

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 (FIPS) on page 63
zeroize from FIPS mode to non-FIPS mdoe on page 64

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system zeroize (FIPS)

```
{master:0}

root@jdm> request system zeroize to-fips

warning: System will be rebooted and current installation will be zeroized.
warning: This will stop all VNFs and remove all user configuration and data.
Reboot system to zeroize currently running installation? [yes,no] (no) yes

Staging zeroize (self) operation ...
System should be kept powered on until operation completes.
upgrade_platform: -------------------
upgrade_platform: Parameters passed:
```

```
upgrade_platform: silent=0
upgrade_platform: package=
upgrade_platform: clean install=0
upgrade_platform: on primary   =0
upgrade_platform: clean upgrade=0
upgrade_platform: zeroize      =to-fips
upgrade_platform: Need reboot after staging=1
upgrade_platform: -------------------
upgrade_platform:
bzImage-intel-x86-64.bin: OK
initramfs.cpio.gz: OK
version.txt: OK
upgrade_platform: Checksum verified and OK...
```

zeroize from FIPS mode to non-FIPS mdoe

```
{master:0}
```

```
root@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

warning: ipsec-key-management subsystem not running - not needed by configuration.
warning: zeroizing re0
```