JUNIPER
NETWORKS | Engineering Simplicity

Junos® OS

Common Criteria Evaluated Configuration
Guide for EX4300 Devices

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

Junos® OS Common Criteria Evaluated Configuration Guide for EX4300 Devices
19.4R1

YEAR 2000 NOTICE

END USER LICENSE AGREEMENT

Table of Contents

3 **Configuring Administrative Credentials and Privileges**

About the Documentation

Use this guide to configure and evaluate EX4300-48MP switches for Common Criteria (CC) compliance. Common Criteria for information technology is an international agreement signed by several countries that permit the evaluation of security products against a common set of standards.

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

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.

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:
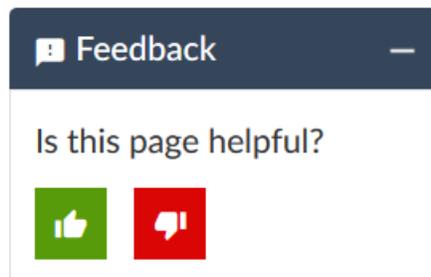
  • Click the thumbs-up icon if the information on the page was helpful to you.

  • 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 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 2.1, 24 September 2018 (NDcPP Version2.1).

This document is available at https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V2.1.pdf.

> **NOTE:** On EX4300-48MP, Junos OS Release 19.4R1 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 several countries that permits the evaluation of security products against a common set of standards. In the Common Criteria Recognition Arrangement (CCRA) at https://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 https://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 2.1 applies to EX4300-48MP devices.

Understanding Junos OS in FIPS Mode

IN THIS SECTION

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

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

The *Security Administrator* enables FIPS mode in Junos OS and sets up keys and passwords for the system and other *FIPS users*.

About the Cryptographic Boundary on Your EX 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 in unencrypted form.

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

How FIPS Mode Differs from Non-FIPS Mode

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

- Self-tests of all cryptographic algorithms are performed at startup.

- Self-tests of random number and key generation are performed continuously.

- Weak cryptographic algorithms such as Data Encryption Standard (DES) and Message Digest 5 (MD5) are disabled.

- Weak or unencrypted management connections must not be configured.

- Passwords must be encrypted with strong one-way algorithms that do not permit decryption.

- Administrator passwords must be at least 10 characters long.

Validated Version of Junos OS in FIPS Mode

To determine whether a Junos OS release is NIST-validated, see the software download page on the Juniper Networks Web site (https://apps.juniper.net/compliance/) or the National Institute of Standards and Technology site.

RELATED DOCUMENTATION

Understanding Common Criteria and FIPS Terminology and Supported Cryptographic Algorithms

IN THIS SECTION

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

Terminology

Common Criteria—Common Criteria for information technology is an international agreement signed by several 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 2.1, 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 23.

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

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

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

KATs—Known answer tests. System self-tests that validate the output of cryptographic algorithms approved for FIPS and test the integrity of some Junos OS modules. For details, see "Understanding FIPS Self-Tests" on page 89.

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 Security Administrator can zeroize the system with a CLI operational command. For details, see "Understanding Zeroization to Clear System Data for FIPS Mode" on page 32.

Supported Cryptographic Algorithms

Table 3 on page 16 summarizes the high level protocol algorithm support.

Table 3: Protocols Allowed in FIPS Mode

Protocol	Key Exchange	Authentication	Cipher	Integrity
SSHv2	- dh-group14-sha1 - ECDH-sha2-nistp256 - ECDH-sha2-nistp384 - ECDH-sha2-nistp521	Host (module): - ECDSA P-256 - SSH-RSA Client (user): - ECDSA P-256 - ECDSA P-384 - ECDSA P-521 - SSH-RSA	- AES CTR 128 - AES CTR 256 - AES CBC 128 - AES CBC 256	- HMAC-SHA-1 - HMAC-SHA-256 - HMAC-SHA-512

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 strength, in bits. ECDSA uses the P-256, P-384, and P-521 curves that can be configured under OpenSSH.

HMAC—Defined as "Keyed-Hashing for Message Authentication" in RFC 2104, HMAC combines hashing algorithms with cryptographic keys for message authentication.

SHA-256, SHA-384, and SHA-512—Secure hash algorithms (SHA) belonging to the SHA-2 standard defined in FIPS PUB 180-2. Developed by NIST, SHA-256 produces a 256-bit hash digest, SHA-384 produces a 384-bit hash digest, and SHA-512 produces a 512-bit hash digest.

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

RELATED DOCUMENTATION

Identifying Secure Product Delivery

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

- Shipping label—Ensure that the shipping label correctly identifies the correct customer name and address as well as the device.

- Outside packaging—Inspect the outside shipping box and tape. Ensure that the shipping tape has not been cut or otherwise compromised. Ensure that the box has not been cut or damaged to allow access to the device.

- Inside packaging—Inspect the plastic bag and seal. Ensure that the bag is not cut or removed. Ensure that the seal remains intact.

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

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

- Verify that the device was ordered using a purchase order. Juniper Networks devices are never shipped without a purchase order.

- When a device is shipped, a shipment notification is sent to the e-mail address provided by the customer when the order is taken. Verify that this e-mail notification was received. Verify that the e-mail contains the following information:

  - Purchase order number

  - Juniper Networks order number used to track the shipment

  - Carrier tracking number used to track the shipment

  - List of items shipped including serial numbers

  - Address and contacts of both the supplier and the customer

- Verify that the shipment was initiated by Juniper Networks. To verify that a shipment was initiated by Juniper Networks, you should perform the following tasks:

  - Compare the carrier tracking number of the Juniper Networks order number listed in the Juniper Networks shipping notification with the tracking number on the package received.

- Log on to the Juniper Networks online customer support portal at https://support.juniper.net/support/ to view the order status. Compare the carrier tracking number or the Juniper Networks order number listed in the Juniper Networks shipment notification with the tracking number on the package received.

RELATED DOCUMENTATION

Understanding the Common Criteria Evaluated Configuration | 12

Understanding Management Interfaces

The following management interfaces can be used in the evaluated configuration:

- Local Management Interfaces—The RJ-45 console port on the rear panel of a device is configured as RS-232 data terminal equipment (DTE). You can use the command-line interface (CLI) over this port to configure the device from a terminal.

- Remote Management Protocols—The device can be remotely managed over any Ethernet interface. SSHv2 is the only permitted remote management protocol that can be used in the evaluated configuration. The remote management protocols J-Web and Telnet are not available for use on the device in the evaluated configuration.

RELATED DOCUMENTATION

Understanding the Common Criteria Evaluated Configuration | 12

2
CHAPTER

Configuring Roles and Authentication Methods

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

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.

Security Administrator performs all FIPS-mode-related configuration tasks and issue all statements and commands for Junos OS in FIPS mode.

Security Administrator Role and Responsibilities

The Security Administrator is the person responsible for enabling, configuring, monitoring, and maintaining Junos OS in FIPS mode on a switch. The Security Administrator 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 Security Administrator administer the system in a secure manner by keeping passwords secure and checking audit files.

The permissions that distinguish the Security Administrator from other FIPS users are **secret**, **security**, **maintenance**, and **control**. For FIPS compliance, assign the Security Administrator to a login class that contains all of these permissions.

Among the tasks related to Junos OS in FIPS mode, the Security Administrator is expected to:

- Set the initial root password. The length of the password should be at least 10 characters.

- Reset user passwords for FIPS-approved algorithms during upgrades from Junos OS.

- Examine log and audit files for events of interest.

- Erase user-generated files, keys, and data by zeroizing the switch.

FIPS User Role and Responsibilities

All FIPS users, including the Security Administrator, can view the configuration. Only the user assigned as the Security Administrator can modify the configuration.

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

What Is Expected of All FIPS Users

All FIPS users, including the Security Administrator, 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

Understanding the Operational Environment for Junos OS in FIPS Mode

IN THIS SECTION

-
-
-

EX 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

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

For more information about the cryptographic boundary on your switch, see "Understanding Junos OS in FIPS Mode" on page 13.

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

Software Environment for Junos OS in FIPS Mode

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

FIPS mode on EX Series switches are available starting with Junos OS Release 19.4R1. The Junos OS in FIPS mode software environment is established after the Security Administrator successfully enables FIPS mode on an EX Series switch.

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

Enabling FIPS mode disables many of the usual Junos OS protocols and services. In particular, you cannot configure the following services in Junos OS in FIPS mode:

- finger
- ftp
- rlogin
- telnet
- tftp
- xnm-clear-text

Attempts to configure these services, or load configurations with these services configured, result in a configuration syntax error.

You can use only SSHv2 as a remote access service.

All passwords established for users after upgrading to Junos OS in FIPS mode must conform to Junos OS in FIPS mode specifications. Passwords must be between 10 and 20 characters in length and require the use of at least three of the five defined character sets (uppercase and lowercase letters, digits, punctuation marks, and keyboard characters, such as % and &, not included in the other four categories). Attempts to configure passwords that do not conform to these rules result in an error. All passwords and keys used to authenticate peers must be at least 10 characters in length, and in some cases the length must match the digest size.

> **NOTE:** Do not attach the switch to a network until you, the Security Administrator, complete the configuration from the local console connection.

Critical Security Parameters

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

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

Table 4 on page 25 lists CSPs on switches running Junos OS.

Table 4: Critical Security Parameters

CSP	Description	Zeroize	Use
SSHv2 private host key	ECDSA / RSA key used to identify the host, generated the first time SSH is configured.	Zeroize command.	Used to identify the host.
SSHv2 session keys	Session key used with SSHv2 and as a Diffie-Hellman private key. Encryption: AES-128, AES-256. MACs: HMAC-SHA-1, HMAC-SHA-2-256, HMAC-SHA2-512. Key exchange: dh-group14-sha1, ECDH-sha2-nistp256, ECDH-sha2-nistp384, and ECDH-sha2-nistp521.	Power cycle and terminate session.	Symmetric key used to encrypt data between host and client.

Table 4: Critical Security Parameters *(continued)*

CSP	Description	Zeroize	Use
User authentication key	Hash of the user's password: SHA256, SHA512.	Zeroize command.	Used to authenticate a user to the cryptographic module.
Security Administrator authentication key	Hash of the Security Administrator's password: SHA256, SHA512.	Zeroize command.	Used to authenticate the Security Administrator 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.

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

Ensure that the switch is in FIPS mode before you configure the Security Administrator or any users. All passwords established for users by the Security Administrator 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.

Downloading Software Packages from Juniper Networks

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

- Junos OS for EX4300-48MP switches, Release 19.4R1

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

To download software packages from Juniper Networks:

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

   https://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 software package that you want to download. You can select software that supports a specific platform or technology.:

   - For Junos OS package, ensure that the name contains the correct switch name and Junos OS release.

     For EX4300-48MP, the image is **jinstall-host-ex-4300mp-x86-64-19.4R1-secure-signed.tgz**.

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

5. Install the Junos OS. See .

RELATED DOCUMENTATION

Installing Software on EX 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 28.

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 Junos OS on the EX4300 for EX4300-48MP Series devices.

3. (Optional) Back up the current software configuration to a second storage option. See the *Junos OS Installation and Upgrade Guide* for instructions on performing this task.

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

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

5. Install the new package on the switch:

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

   Replace *package* with one of the following paths:

   - For a software package in a local directory on the switch, use **/var/tmp/***package***.tgz**.
   - For a software package on a remote server, use one of the following paths, replacing *package* with the software package name—for example, **jinstall-host-ex-4300mp-x86-64-19.4R1-secure-signed.tgz**
     .
     - **ftp://*hostname/pathname/package*.tgz**
     - **http://*hostname/pathname/package*.tgz**

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

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

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

```
user@switch:> show version local
Hostname: hostname
Model: ex4300-48mp
Junos: 19.4R1
JUNOS OS Kernel 64-bit  [20191115.14c2ad5_builder_stable_11]
JUNOS OS libs [20191115.14c2ad5_builder_stable_11]
JUNOS OS runtime [20191115.14c2ad5_builder_stable_11]
JUNOS OS time zone information [20191115.14c2ad5_builder_stable_11]
JUNOS OS libs compat32 [20191115.14c2ad5_builder_stable_11]
JUNOS OS 32-bit compatibility [20191115.14c2ad5_builder_stable_11]
JUNOS py extensions2 [20191119.064603_builder_junos_194_r1]
JUNOS py extensions [20191119.064603_builder_junos_194_r1]
JUNOS py base2 [20191119.064603_builder_junos_194_r1]
JUNOS py base [20191119.064603_builder_junos_194_r1]
JUNOS OS vmguest [20191115.14c2ad5_builder_stable_11]
JUNOS OS crypto [20191115.14c2ad5_builder_stable_11]
JUNOS network stack and utilities [20191119.064603_builder_junos_194_r1]
JUNOS libs [20191119.064603_builder_junos_194_r1]
JUNOS libs compat32 [20191119.064603_builder_junos_194_r1]
JUNOS runtime [20191119.064603_builder_junos_194_r1]
JUNOS na telemetry [19.4R1.1]
JUNOS Web Management Platform Package [20191119.064603_builder_junos_194_r1]
JUNOS qfx runtime [20191119.064603_builder_junos_194_r1]
JUNOS common platform support [20191119.064603_builder_junos_194_r1]
JUNOS qfx platform support [20191119.064603_builder_junos_194_r1]
JUNOS Openconfig [19.4R1.1]
JUNOS dcp network modules [20191119.064603_builder_junos_194_r1]
JUNOS modules [20191119.064603_builder_junos_194_r1]
JUNOS qfx modules [20191119.064603_builder_junos_194_r1]
JUNOS qfx Data Plane Crypto Support [20191119.064603_builder_junos_194_r1]
JUNOS daemons [20191119.064603_builder_junos_194_r1]
JUNOS qfx daemons [20191119.064603_builder_junos_194_r1]
JUNOS Services URL Filter package [20191119.064603_builder_junos_194_r1]
JUNOS Services TLB Service PIC package [20191119.064603_builder_junos_194_r1]
JUNOS Services Telemetry [20191119.064603_builder_junos_194_r1]
JUNOS Services TCP-LOG [20191119.064603_builder_junos_194_r1]
JUNOS Services SSL [20191119.064603_builder_junos_194_r1]
```

```
JUNOS Services SOFTWIRE [20191119.064603_builder_junos_194_r1]
JUNOS Services Stateful Firewall [20191119.064603_builder_junos_194_r1]
JUNOS Services RTCOM [20191119.064603_builder_junos_194_r1]
JUNOS Services RPM [20191119.064603_builder_junos_194_r1]
JUNOS Services PCEF package [20191119.064603_builder_junos_194_r1]
JUNOS Services NAT [20191119.064603_builder_junos_194_r1]
JUNOS Services Mobile Subscriber Service Container package
[20191119.064603_builder_junos_194_r1]
JUNOS Services MobileNext Software package [20191119.064603_builder_junos_194_r1]
JUNOS Services Logging Report Framework package
[20191119.064603_builder_junos_194_r1]
JUNOS Services LL-PDF Container package [20191119.064603_builder_junos_194_r1]
JUNOS Services Jflow Container package [20191119.064603_builder_junos_194_r1]
JUNOS Services Deep Packet Inspection package
[20191119.064603_builder_junos_194_r1]
JUNOS Services IPSec [20191119.064603_builder_junos_194_r1]
JUNOS Services IDS [20191119.064603_builder_junos_194_r1]
JUNOS IDP Services [20191119.064603_builder_junos_194_r1]
JUNOS Services HTTP Content Management package
[20191119.064603_builder_junos_194_r1]
JUNOS Services Crypto [20191119.064603_builder_junos_194_r1]
JUNOS Services Captive Portal and Content Delivery Container package
[20191119.064603_builder_junos_194_r1]
JUNOS Services COS [20191119.064603_builder_junos_194_r1]
JUNOS AppId Services [20191119.064603_builder_junos_194_r1]
JUNOS Services Application Level Gateways [20191119.064603_builder_junos_194_r1]
JUNOS Services AACL Container package [20191119.064603_builder_junos_194_r1]
JUNOS SDN Software Suite [20191119.064603_builder_junos_194_r1]
JUNOS Extension Toolkit [20191119.064603_builder_junos_194_r1]
JUNOS Phone-home [20191119.064603_builder_junos_194_r1]
JUNOS Packet Forwarding Engine Support (DC-PFE)
[20191119.064603_builder_junos_194_r1]
JUNOS Packet Forwarding Engine Support (M/T Common)
[20191119.064603_builder_junos_194_r1]
JUNOS Juniper Malware Removal Tool (JMRT)
[1.0.0+20191119.064603_builder_junos_194_r1]
JUNOS J-Insight [20191119.064603_builder_junos_194_r1]
JUNOS jfirmware [20191119.064603_builder_junos_194_r1]
JUNOS Online Documentation [20191119.064603_builder_junos_194_r1]
JUNOS jail runtime [20191115.14c2ad5_builder_stable_11]
JUNOS FIPS mode utilities [20191119.064603_builder_junos_194_r1]
JUNOS Host Software [3.14.52-rt50-WR7.0.0.9_ovp:3.1.0]
JUNOS Host ex-4300mp control-plane package [19.4R1.1]
JUNOS Host ex-4300mp platform package [19.4R1.1]
```

```
JUNOS Host ex-4300mp data-plane package [19.4R1.1]
JUNOS Host ex-4300mp base package [19.4R1.1]
```

RELATED DOCUMENTATION

Troubleshooting Software Installation

Understanding Software Installation on EX Series Switches

Understanding Zeroization to Clear System Data for FIPS Mode

IN THIS SECTION

- Why Zeroize? | **33**
- When to Zeroize? | **33**

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

The Security Administrator initiates the zeroization process by entering the **request system zeroize** operational command from the CLI after enabling FIPS mode. Use of this command is restricted to the Security Administrator.

In reference to cryptographic key destruction, TOE does not support delayed key destruction.

> ⚠️ **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?

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. You must zeroize the system to remove sensitive information before disabling FIPS mode on the device.

When to Zeroize?

As Security Administrator, 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 before disabling FIPS mode 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.

RELATED DOCUMENTATION

Zeroizing the System

To zeroize your switch:

1. Log in to the switch as Security Administrator and from the CLI, enter

```
security-administrator@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
warning: zeroizing localre
```

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 | **35**

Understanding Zeroization to Clear System Data for FIPS Mode | **32**

Enabling FIPS Mode

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

As Security Administrator, 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 27. When you enable FIPS mode in Junos OS on the device, you cannot configure passwords unless they meet this standard.

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

> **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. Zeroize the device to delete all CSPs before entering FIPS mode. Refer to "Understanding Zeroization to Clear System Data for FIPS Mode" on page 32 section for details.

2. After the device comes up in 'Amnesiac mode', login using username **root** and password **""** (blank).

   ```
   FreeBSD/amd64 (Amnesiac) (ttyu0)
   login: root
   Password:
   --- JUNOS 19.4R1.1 Kernel 64-bit  JNPR-11.0-20191115.14c2ad5_buil
   root@:~ # cli
   root>
   ```

3. Configure root authentication with password at least 10 characters or more.

   ```
   root> edit
   Entering configuration mode
   [edit]
   root# set system root-authentication plain-text-password
   New password:
   Retype new password:
   ```

```
    [edit]
    root# commit
configuration check succeeds
commit complete
```

4. Load configuration onto device and commit new configuration.

5. Configure security-administrator and login with security-administrator credentials.

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

> **NOTE:** The device might display the **Encrypted-password must be re-configured to use FIPS compliant hash** warning to delete older CSPs in loaded configuration.

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

```
    [edit]
    security-administrator@hostname# commit
    [edit]
'system'
warning: reboot is required to transition to FIPS level 1
commit complete
    [edit]
    security-administrator@switch# run request system reboot
```

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

```
    security-administrator@hostname:fips>
```

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

RELATED DOCUMENTATION

Configuring Security Administrator and FIPS User Identification and Access

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

Configuring Security Administrator 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 Security Administrator. In most cases the **super-user** class suffices for the Security Administrator.

To configure login access for a Security Administrator:

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

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

2. Name the user "security-administrator" and assign the Security Administrator 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# set system login user security-administrator uid 6400 class super-user
```

3. Following the guidelines in "Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode" on page 27, assign the Security Administrator 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# set system login user security-administrator class super-user authentication plain-text-password
```

4. Optionally, display the configuration:

```
[edit]
root@switch# edit system
[edit system]
root@switch# show
login {
    user security-administrator {
        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# commit
commit complete
root@switch# exit
root@switch> exit
```

Configuring FIPS User Login Access

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

To configure login access for a FIPS user:

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

```
security-administrator@switch:fips> configure
Entering configuration mode
[edit]
security-administrator@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**, **network**, **resetview**, and **view-configuration**.

   For a list of permissions, see Understanding Junos OS Access Privilege Levels.

```
[edit]
security-administrator@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 27, assign the FIPS user a plain-text password for login authentication. Set the password by typing a password after the prompts **New password** and **Retype new password**.

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

4. Optionally, display the configuration:

```
[edit]
security-administrator@switch:fips# edit system
[edit system]
security-administrator@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]
security-administrator@switch:fips# commit
security-administrator@switch:fips> exit
```

RELATED DOCUMENTATION

Understanding Roles and Services for Junos OS in Common Criteria and FIPS | 21

3
CHAPTER

Configuring Administrative Credentials and Privileges

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 ]
    security-administrator@switch:fips# 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 ]
    security-administrator@switch:fips# 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 10 characters long. The valid range for this option is 10 to 20 characters.

    ```
    [ edit ]
    security-administrator@switch:fips# set system login password minimum-length 10
    ```

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

```
[ edit ]
security-administrator@switch:fips# set system login password format sha512
```

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

> **NOTE:** The new hash algorithm affect only those passwords that are generated after commit.

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

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 2.1 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]
    security-administrator@switch:fips# set system login class security-admin permissions all
    ```

2. Configure the hashing algorithm used for password storage as sha512.

    ```
    [edit]
    security-administrator@switch:fips# set system login password format sha512
    ```

3. Commit the changes.

    ```
    [edit]
    security-administrator@switch:fips# commit
    ```

4. Define your NDcPP Version 2.1 authorized administrator.

    ```
    [edit]
    security-administrator@switch:fips# set system login user NDcPPv2-user class security-admin authentication
        encrypted-password

            OR
    security-administrator@switch:fips# set system login user NDcPPv2-user class security-admin authentication
        plain-text-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]
security-administrator@switch:fips# 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]
security-administrator@switch:fips# 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]
security-administrator@switch:fips# commit
```

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

RELATED DOCUMENTATION

Configuring Inactivity Timeout Period, and Terminating Local and Remote Idle Session

Configuring Session Termination

Terminate the session after the security administrator specifies inactive timeout period.

1. Set the idle timeout.

```
[edit]
security-administrator@switch:fips# set system login class security-admin idle-timeout 2
```

2. Configure the login access privileges.

```
[edit]
security-administrator@switch:fips# set system login class security-admin permissions all
```

3. Commit the configuration.

```
[edit]
security-administrator@switch:fips# commit
```

```
commit complete
```

4. Set the password.

```
[edit]
security-administrator@switch:fips#set system login user NDcPPv2-user authentication plain-text-password
New password:
Retype new password:
```

5. Define login class.

```
[edit]
security-administrator@switch:fips# set system login user NDcPPv2-user class security-admin
```

6. Commit the configuration.

```
[edit]
security-administrator@switch:fips# commit
```

```
commit complete
```

Sample Output for Local Administrative Session Termination

```
con switch
Trying a.b.c.d...
'autologin': unknown argument ('set ?' for help).
Connected to device.example.com
Escape character is '^]'.

Type the hot key to suspend the connection: <CTRL>Z
FreeBSD/amd64 (switch) (ttyu0)
login: NDcPPv2-user
Password:
Last login: Sun Oct 23 22:42:27 from 10.224.33.70

--- JUNOS 19.4R1.4 Kernel 64-bit  JNPR-11.0-20190316.df99236_buil
NDcPPv2-user@switch> Warning: session will be closed in 1 minute if there is no
activity
Warning: session will be closed in 10 seconds if there is no activity
Idle timeout exceeded: closing session
```

```
FreeBSD/amd64 (switch) (ttyu0)
```

Sample Output for Remote Administrative Session Termination

```
ssh NDcPPv2-user@switch
Password:
Last login: Sun Oct 23 22:48:05 2019
--- JUNOS 19.4R1.4 Kernel 64-bit  JNPR-11.0-20190316.df99236_buil
NDcPPv2-user@switch> exit

Connection to switch closed.
ssh NDcPPv2-user@switch
Password:
Last login: Sun Oct 23 22:50:50 2019 from 10.224.33.70
--- JUNOS 19.4R1.6 Kernel 64-bit  JNPR-11.0-20190316.df99236_buil
NDcPPv2-user@switch> Warning: session will be closed in 1 minute if there is no
activity
Warning: session will be closed in 10 seconds if there is no activity
Idle timeout exceeded: closing session

Connection to switch closed.
```

Sample Output for User Initiated Termination

```
ssh NDcPPv2-user@switch
Password:
Last login: Sun Oct 23 22:48:05 2019
--- JUNOS 19.4R1.4 Kernel 64-bit  JNPR-11.0-20190316.df99236_buil
NDcPPv2-user@switch> exit

Connection to switch closed.
```

4
CHAPTER

Configuring SSH and Console Connection

Configuring a System Login Message and Announcement

A login message appears before the user logs in and an 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]
> security-administrator@switch:fips# **set system login message** *login-message-banner-text*

To configure system announcement, use the following command:

> [edit]
> security-administrator@switch:fips# **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 NDcPPv2.1 | 51

Configuring SSH on the Evaluated Configuration for NDcPPv2.1

SSH through remote management interface allowed in the evaluated configuration. This topic describes how to configure SSH for remote management of TOE. The following algorithms that needs to be configured to validate SSH for NDcPPv2.1.

To configure SSH on the device:

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

```
[edit ]
security-administrator@switch:fips# set system services ssh hostkey-algorithm ssh-ecdsa
security-administrator@switch:fips# set system services ssh hostkey-algorithm no-ssh-dss
security-administrator@switch:fips# set system services ssh hostkey-algorithm ssh-rsa
security-administrator@switch:fips# set system services ssh hostkey-algorithm no-ssh-ed25519
```

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

```
[edit ]
security-administrator@switch:fips# set system services ssh key-exchange dh-group14-sha1
security-administrator@switch:fips# set system services ssh key-exchange ecdh-sha2-nistp256
security-administrator@switch:fips# set system services ssh key-exchange ecdh-sha2-nistp384
security-administrator@switch:fips# set system services ssh key-exchange ecdh-sha2-nistp521
```

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

```
[edit ]
security-administrator@switch:fips# set system services ssh macs hmac-sha1
security-administrator@switch:fips# set system services ssh macs hmac-sha2-256
security-administrator@switch:fips# set system services ssh macs hmac-sha2-512
```

4. Specify the ciphers allowed for protocol version 2.

```
[edit ]
security-administrator@switch:fips# set system services ssh ciphers aes128-cbc
security-administrator@switch:fips# set system services ssh ciphers aes256-cbc
security-administrator@switch:fips# set system services ssh ciphers aes128-ctr
security-administrator@switch:fips# 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 | 53

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]
security-administrator@switch:fips# 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]
security-administrator@switch:fips# set retry-options tries-before-disconnect <number>
```

Here, **tries-before-disconnect** is the number of times a user can attempt to enter a password when logging in. The connection closes if a user fails to log in after the number specified. The range is from 1 through 10, and the default value is 10.

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

```
[edit system login]
security-administrator@switch:fips# 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]
security-administrator@switch:fips# 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]
security-administrator@switch:fips# set services ssh root-login deny
```

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

RELATED DOCUMENTATION

5
CHAPTER

Configuring the Remote Syslog Server

Syslog Server Configuration on a Linux System

IN THIS SECTION

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.

Use the configuration details to establish session between the target of evaluation (TOE) and the audit server. Examine the generated audit data transferred to the audit server.

The NDcPP logs capture the following events:

- Changes to secret key data in the configuration.
- Committed changes.
- Login and logout of users.
- System startup.
- Failure to establish an SSH session.
- Establishment or 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.

- Capture all changes to the configuration.

- Store logging information remotely.

Configuring Event Logging to a Remote Server

To configure event logging to a remote server when the SSH connection to the ToE is initiated from the remote system log server.

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

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

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

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

   ```
   [edit system login]
   security-administrator@switch:fips# set 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 system login]
   security-administrator@switch:fips# set user syslog-mon class monitor authentication ssh-rsa public key from
       syslog-monitor key pair
   ```

4. Set up NETCONF with SSH.

   ```
   [edit system services]
   security-administrator@switch:fips# set netconf ssh
   ```

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

   ```
   [edit system]
   security-administrator@switch:fips# set syslog file messages any any
   commit
   ```

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

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

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.

    ```
    security-administrator@switch:fips# $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 are received on 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 logging and remote event logged in syslog server and record the particular software (name, version) used on the audit server during testing.

The following output shows test log results for syslog-server.

```
  switch@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
 AAAAB3NzaC1yc2EAAAADAQABAAABAQCrUREJUBpjwAoIgRrGy9zgt+
D2pikk3Q/Wdf8I5vr+njeqJhCx2bUAkrRbYXNILQQAZbg7kLfi/8TqqL
eon4HOP2e6oCSorKdx/GrOTzLONL4fh0EyuSAk8bs5JuwWNBUokV025
gzpGFsBusGnlj6wqqJ/sjFsMmfxyCkbY+pUWb8m1/A9YjOFT+6esw+9S
tF6Gbg+VpbYYk/Oday4z+z7tQHRFSrxj2G92aoliVDBLJparEMBc8w
LdSUDxmgBTM2oadOmm+kreBUQjrmr6775RJn9H9YwIxKOxGm4SFnX/Vl4
R+lZ9RqmKH2wodIEM34K0wXEHzAzNZ01oLmaAVqT
syslog-monitor key pair
[host@nms5-vm-linux2 ~]$ eval `ssh-agent -s`
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)
```

Net configuration channel

```
  switch@nms5-vm-linux2 ~]$ ssh syslog-mon@starfire -s netconf
 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'
```

Net configuration channel

```
  switch@nms5-vm-linux2 ~]$ ssh syslog-mon@starfire -s netconf
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 that the local syslogs and remote syslogs received were similar.

```
Local :
Jan 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 acess 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
```

```
Jan 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 acess 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
```

6
CHAPTER

Configuring Audit Log Options

Configuring Audit Log Options in the Evaluated Configuration

IN THIS SECTION

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

Configuring Audit Log Options for EX4300-48MP devices

To configure audit log options for EX4300-48MP devices:

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

   ```
   [edit system syslog]
   security-administrator@switch:fips# set archive files 2
   ```

2. Specify the file in which to log data.

   ```
   [edit system syslog]
   security-administrator@switch:fips# set file  Audit_logs any any
   ```

3. Specify the size of files to be archived.

   ```
   [edit system syslog]
   security-administrator@switch:fips# set file  Audit_logs archive size 10m
   ```

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

   ```
   [edit system syslog]
   security-administrator@switch:fips# set file  Audit_logs explicit-priority
   ```

5. Log system messages in a structured format.

```
[edit system syslog]
security-administrator@switch:fips# set file  Audit_logs structured-data
```

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 **syslog:**

```
[edit system]
syslog {
    file syslog {
        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 **syslog:**

```
[edit system]
syslog {
    file syslog {
        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 syslog {
      any notice;
      authorization info;
   }
   file interactive-commands {
      interactive-commands any;
   }
}
...
```

```
    ...
```

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

```
security-administrator@switch:fips# 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 68 shows sample for syslog auditing for NDcPPv2:

Table 5: Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
FAU_GEN.1	None	None	
FAU_GEN.2	None	None	
FAU_STG_EXT.1	None	None	
FAU_STG.1	None	None	
FCS_CKM.1	None	None	
FCS_CKM.2	None	None	
FCS_CKM.4	None	None	

Table 5: Auditable Events *(continued)*

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
FCS_COP.1/DataEncryption	None	None	
FCS_COP.1/SigGen	None	None	
FCS_COP.1/Hash	None	None	
FCS_COP.1/KeyedHash	None	None	
FCS_COP.1(1)/KeyedHashCMAC	None	None	
FCS_RBG_EXT.1	None	None	
FIA_PMG_EXT.1	None	None	

Table 5: Auditable Events *(continued)*

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address)	

Table 5: Auditable Events *(continued)*

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
			Successful Local Login Jan 3 09:59:36 login[7637]: LOGIN_INFORMATION: User root logged in from host [unknown] on device ttyu0 Jan 3 09:59:36 login[7637]: LOGIN_ROOT: User root logged in as root from host [unknown] on device ttyu0 Unsuccessful Local Login Jan 3 09:57:52 login[7637]: LOGIN_PAM_ AUTHENTICATION_ERROR: Failed password for user root Jan 3 09:57:52 login[7637]: LOGIN_FAILED: Login failed for user root from host ttyu0 Successful Remote Login Jan 3 09:32:07 mgd[47035]: UI_AUTH_EVENT: Authenticated user 'test1' assigned to class 'j-read-only' Jan 3 09:32:07 mgd[47035]: UI_LOGIN_EVENT: User 'test1' login, class 'j-read-only' [47035],

Table 5: Auditable Events *(continued)*

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
			ssh-connection '10.1.5.153 36784 10.1.2.68 22', client-mode 'cli'
			Unsuccessful Remote Login
			Jan 3 09:26:56 sshd: SSHD_LOGIN_FAILED: Login failed for user 'test1' from host '10.1.5.153'

Table 5: Auditable Events *(continued)*

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address)	

Table 5: Auditable Events *(continued)*

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
			Successful Local Login Jan 3 09:59:36 login[7637]: LOGIN_INFORMATION: User root logged in from host [unknown] on device ttyu0 Jan 3 09:59:36 login[7637]: LOGIN_ROOT: User root logged in as root from host [unknown] on device ttyu0 Unsuccessful Local Login Jan 3 09:57:52 login[7637]: LOGIN_PAM_ AUTHENTICATION_ERROR: Failed password for user root Jan 3 09:57:52 login[7637]: LOGIN_FAILED: Login failed for user root from host ttyu0 Successful Remote Login Jan 3 09:32:07 mgd[47035]: UI_AUTH_EVENT: Authenticated user 'test1' assigned to class 'j-read-only' Jan 3 09:32:07 mgd[47035]: UI_LOGIN_EVENT: User 'test1' login, class 'j-read-only' [47035], ssh-connection '10.1.5.153 36784

Table 5: Auditable Events *(continued)*

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
			10.1.2.68 22', client-mode 'cli' Unsuccessful Remote Login Jan 3 09:26:56 sshd: SSHD_LOGIN_FAILED: Login failed for user 'test1' from host '10.1.5.153'
FIA_UAU.7	None	None	
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None	Dec 28 21:51:21 mgd[8007]: UI_CMDLINE_READ_LINE: User 'root', command 'request vmhost software add /var/tmp/junos-vmhost-install-mx-x86-64-19.1-20181231.0.tgz no-validate'
FMT_MTD.1/CoreData	None	None	
FMT_SMF.1	All management activities of TSF data	None	Refer to the audit events listed in this table.
FMT_SMR.2	None	None	
FPT_SKP_EXT.1	None	None	
FPT_APW_EXT.1	None	None	

Table 5: Auditable Events *(continued)*

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
FPT_TST_EXT.1	None	None	Enter **request system fips self-test** at command line for on demand self-test. or Reboot the device to view the self-test during startup.
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None	Dec 28 21:51:21 mgd[8007]: UI_CMDLINE_READ_LINE: User 'root', command 'request vmhost software add /var/tmp/junos-vmhost-install-mx-x86-64-19.1-20181231.0.tgz no-validate'
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).	Apr 22 15:31:37 mgd[11121]: UI_CMDLINE_READ_LINE: User 'root', command 'set date 201904221532.00 Apr 22 15:32:05 mgd[11121]: UI_CMDLINE_READ_LINE: User 'root', command 'show system uptime '
FPT_STM_EXT.1 FTA_SSL_EXT.1 (if "terminate the session is selected)	The termination of a local interactive session by the session locking mechanism.	None	Jan 3 11:59:29 cli: UI_CLI_IDLE_TIMEOUT: Idle timeout for user 'root' exceeded and session terminated
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None	Jan 3 11:26:23 cli: UI_CLI_IDLE_TIMEOUT: Idle timeout for user 'root' exceeded and session terminated

Table 5: Auditable Events *(continued)*

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
FTA_SSL.4	The termination of an interactive session.	None	Local Jan 3 11:47:25 mgd[52521]: UI_LOGOUT_EVENT: User 'root' logout Remote Jan 3 11:43:33 sshd[52425]: Received disconnect from 10.1.5.153 port 36800:11: disconnected by user
FTA_TAB.1	None	None	
FTP_ITC.1	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.	Initiation of the trusted path Jan 3 12:09:00 sshd[53492]: Accepted keyboard-interactive/pam for root from 10.1.5.153 port 36802 ssh2 Termination of the trusted path Jan 3 12:09:03 sshd[53492]: Received disconnect from 10.1.5.153 port 36802:11: disconnected by user Jan 3 12:09:36 sshd: Failure of the trusted path SSHD_LOGIN_FAILED: Login failed for user 'root' from host '10.1.5.153'

Table 5: Auditable Events *(continued)*

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	None	Initiation of the trusted path Jan 3 12:09:00 sshd[53492]: Accepted keyboard-interactive/pam for root from 10.1.5.153 port 36802 ssh2 Termination of the trusted path Jan 3 12:09:03 sshd[53492]: Received disconnect from 10.1.5.153 port 36802:11: disconnected by user Jan 3 12:09:36 sshd: Failure of the trusted path SSHD_LOGIN_FAILED: Login failed for user 'root' from host '10.1.5.153'
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure	Dec 17 15:02:12 sshd[9842]: Unable to negotiate with 10.1.5.153 port 43836: no matching key exchange method found. Their offer: diffie-hellman-group1-sha1,ext-info-c

Table 5: Auditable Events *(continued)*

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate Any addition, replacement or removal of trust anchors in the TOE's trust store	Reason for failure of certificate validation Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store	Dec 28 22:20:23 veriexec[9371]: cannot validate /packages/db/pkginst. 9286/manifest.ecerts: subject issuer mismatch: /C=US/ST=CA/L= Sunnyvale/O=Juniper Networks/ OU=Juniper CA/CN= PackageProductionTest Ec_2017_NO_DEFECTS/ emailAddress=ca@juni per.net
FIA_X509_EXT.2	None	None	
FPT_TUD_EXT.2	Failure of update	Reason for failure (including identifier of invalid certificate)	Dec 28 22:20:23 veriexec[9371]: cannot validate /packages/db/pkginst. 9286/manifest.ecerts: subject issuer mismatch: /C=US/ST=CA/L= Sunnyvale/O= Juniper Networks/ OU= Juniper CA/CN= PackageProductionTest Ec_2017_ NO_DEFECTS/ emailAddress= ca@juniper.net
FMT_MOF.1/Functions	None	None	
FMT_MOF.1/Services	None	None	
FMT_MTD.1/CryptoKeys	None	None	

Table 5: Auditable Events *(continued)*

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
FCS_MACSEC_EXT.1	Session establishment	Secure Channel Identifier (SCI)	Apr 10 20:43:35 dot1xd[6622]: DOT1XD_MKA_ SECURE_CHANNEL_ CREATED: Macsec receive secure channel created for 64:87:88:5a :19:30 on interface xe-0/0/0
FCS_MACSEC_EXT.1.7	Creation of Connectivity Association	Connectivity Association Key Names	Apr 10 20:43:38 dot1xd[6622]: DOT1XD_MKA_SECURE_ ASSOCIATION_ESTABLISHED: Macsec secure association established with an :2 on interface xe-0/0/0
FCS_MACSEC_EXT.3.1	Creation and update of Secure Association Key	Creation and update times	Apr 29 16:01:49 fpc0 vsc8584_macsec_rx _sa_create: ifd 148 (ge-0/0/0), port_no 0, vsc8584_handle 0x1543be98, an 3, key 0x18ccb058, lowest_pn 1, sci 0x18ccb044
FIA_AFL.1	Administrator lockout due to excessive authentication failures	None	Jan 3 08:13:59 sshd: SSHD_LOGIN_ ATTEMPTS_THRESHOLD: Threshold for unsuccessful authentication attempts (2) reached by user 'test1'

Table 5: Auditable Events *(continued)*

Requirement	Auditable Events	Additional Audit Record Contents	How event generated
FPT_RPL.1	Detected replay attempt	None	Apr 15 10:05:16.142910 MKA actor #0 received duplicate or delayed PDU Apr 15 10:05:16.142932 MKA actor #0 received MKPDU, SCI 3C:94:D5:A0:A0:07/1, MI 27:D7:9F:97:53: CF:EF:86:00:52:C1:78, MN 1530

RELATED DOCUMENTATION

| Configuring Audit Log Options in the Evaluated Configuration **| 65**

7

CHAPTER

Configuring Event Logging

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 events. Some of the logging events are listed below:

- 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

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;
}
```

Interpreting Event Messages

The following output shows a sample event message.

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

Table 6 on page 85 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
timestamp	Time when the message was generated, in one of two representations: • *MMM-DD HH:MM:SS.MS+/-HH:MM,* 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). • *YYYY-MM-DDTHH:MM:SS.MSZ* is the year, month, day, hour, minute, second and millisecond in UTC.	Feb 27 02:33:04 is the timestamp expressed as local time in the United States. 2012-02-27T09:17:15.719Z is 2:33 AM UTC on 27 Feb 2012.
hostname	Name of the host that originally generated the message.	router1
process	Name of the Junos OS process that generated the message.	mgd
processID	UNIX process ID (PID) of the Junos OS process that generated the message.	4153
TAG	Junos OS system log message tag, which uniquely identifies the message.	UI_DBASE_LOGOUT_EVENT
username	Username of the user initiating the event.	"admin"
message-text	English-language description of the event .	set: [system radius-server 1.2.3.4 secret]

RELATED DOCUMENTATION

Logging Changes to Secret Data

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

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

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

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

RELATED DOCUMENTATION

Interpreting Event Messages | 84

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 | 84

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 | 86

8
CHAPTER

Performing Self-Tests on a Device

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

- **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 when 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 ECDSA key pairs, and manually entered keys.

On demand, self tests can be executed by entering **request system fips self-test** at command line.

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

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

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

Performing Power-On Self-Tests on the Device

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

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

```
@ 1574740128 [2019-11-26 03:48:48 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-ECB Known Answer Test: Passed
mgd: AES-KEYWRAP Known Answer Test: Passed
mgd: KBKDF Known Answer Test: Passed
mgd: Testing libmd KATS:
mgd: HMAC-SHA1 Known Answer Test: Passed
mgd: HMAC-SHA2-256 Known Answer Test: Passed
mgd: SHA-2-512 Known Answer Test: Passed
mgd: Testing OpenSSL KATS:
mgd: NIST 800-90 HMAC DRBG Known Answer Test: Passed
mgd: FIPS ECDSA Known Answer Test: Passed
mgd: FIPS ECDH Known Answer Test: Passed
mgd: FIPS RSA Known Answer Test: Passed
mgd: DES3-CBC Known Answer Test: Passed
mgd: HMAC-SHA1 Known Answer Test: Passed
mgd: HMAC-SHA2-224 Known Answer Test: Passed
mgd: HMAC-SHA2-256 Known Answer Test: Passed
mgd: HMAC-SHA2-384 Known Answer Test: Passed
mgd: HMAC-SHA2-512 Known Answer Test: Passed
mgd: AES-CBC Known Answer Test: Passed
mgd: AES-GCM Known Answer Test: Passed
mgd: ECDSA-SIGN Known Answer Test: Passed
mgd: KDF-IKE-V1 Known Answer Test: Passed
mgd: KDF-SSH-SHA256 Known Answer Test: Passed
mgd: KAS-ECC-EPHEM-UNIFIED-NOKC Known Answer Test: Passed
mgd: KAS-FFC-EPHEM-NOKC Known Answer Test: Passed
mgd: Testing QuickSec 7.0 KATS:
mgd: NIST 800-90 HMAC DRBG Known Answer Test: Passed
mgd: DES3-CBC Known Answer Test: Passed
mgd: HMAC-SHA1 Known Answer Test: Passed
mgd: HMAC-SHA2-224 Known Answer Test: Passed
mgd: HMAC-SHA2-256 Known Answer Test: Passed
mgd: HMAC-SHA2-384 Known Answer Test: Passed
mgd: HMAC-SHA2-512 Known Answer Test: Passed
mgd: AES-CBC Known Answer Test: Passed
mgd: AES-GCM Known Answer Test: Passed
mgd: SSH-RSA-ENC Known Answer Test: Passed
mgd: SSH-RSA-SIGN Known Answer Test: Passed
mgd: SSH-ECDSA-SIGN Known Answer Test: Passed
```

```
mgd: KDF-IKE-V1 Known Answer Test: Passed
mgd: KDF-IKE-V2 Known Answer Test: Passed
mgd: Testing QuickSec KATS:
mgd: NIST 800-90 HMAC DRBG Known Answer Test: Passed
mgd: DES3-CBC Known Answer Test: Passed
mgd: HMAC-SHA1 Known Answer Test: Passed
mgd: HMAC-SHA2-224 Known Answer Test: Passed
mgd: HMAC-SHA2-256 Known Answer Test: Passed
mgd: HMAC-SHA2-384 Known Answer Test: Passed
mgd: HMAC-SHA2-512 Known Answer Test: Passed
mgd: AES-CBC Known Answer Test: Passed
mgd: AES-GCM Known Answer Test: Passed
mgd: SSH-RSA-ENC Known Answer Test: Passed
mgd: SSH-RSA-SIGN Known Answer Test: Passed
mgd: KDF-IKE-V1 Known Answer Test: Passed
mgd: KDF-IKE-V2 Known Answer Test: Passed
mgd: Testing SSH IPsec KATS:
mgd: NIST 800-90 HMAC DRBG Known Answer Test: Passed
mgd: DES3-CBC Known Answer Test: Passed
mgd: HMAC-SHA1 Known Answer Test: Passed
mgd: HMAC-SHA2-256 Known Answer Test: Passed
mgd: AES-CBC Known Answer Test: Passed
mgd: SSH-RSA-ENC Known Answer Test: Passed
mgd: SSH-RSA-SIGN Known Answer Test: Passed
mgd: KDF-IKE-V1 Known Answer Test: Passed
mgd: Testing file integrity:
mgd: File integrity Known Answer Test: Passed
mgd: Testing crypto integrity:
mgd: Crypto integrity Known Answer Test: Passed
mgd: Expect an everiexec: no fingerprint for file='/sbin/kats/cannot-exec' fsid=216
 fileid=49356 gen=1 uid=0 pid=6685
xec Authentication error...
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.

9

CHAPTER

Operational Commands

request system zeroize

Syntax

request system zeroize

Release Information

Command introduced in Junos OS Release 12.1 for EX 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 Security Administrator 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

Output Fields

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

Sample Output

request system zeroize

security-administrator@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

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