JUNIPer | Engineering
NETWORKS | Simplicity

Junos® OS

Common Criteria Evaluated Configuration Guide for EX2300 and EX3400 Devices

Published
2020-05-25

Release
19.1R2

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

Junos® *OS Common Criteria Evaluated Configuration Guide for EX2300 and EX3400 Devices*
19.1R2

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About the Documentation

Use this guide to configure and evaluate EX2300 and EX3400 devices 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.

Table 2 on page vii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

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

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

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

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

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

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

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

Documentation Feedback

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

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the Juniper Networks TechLibrary site, and do one of the following:
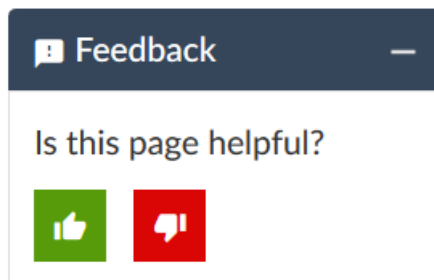
  - Click the thumbs-up icon if the information on the page was helpful to you.

  - Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.

- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

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

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

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.

- Product warranties—For product warranty information, visit https://www.juniper.net/support/warranty/.

- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

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

- Find CSC offerings: https://www.juniper.net/customers/support/

- Search for known bugs: https://prsearch.juniper.net/

- Find product documentation: https://www.juniper.net/documentation/

- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/

- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/

- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/

- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/

- Create a service request online: https://myjuniper.juniper.net

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

Creating a Service Request with JTAC

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

- Visit https://myjuniper.juniper.net.

- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

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

1
CHAPTER

Overview

Understanding 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 Version 2.1).

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

Understanding Common Criteria

Common Criteria for information technology is an international agreement signed by 28 countries that permits the evaluation of security products against a common set of standards. In the Common Criteria Recognition Arrangement (CCRA) at 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 EX2300 and EX3400 devices.

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 28 countries that permits the evaluation of security products against a common set of standards.

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

NDcPP—Collaborative Protection Profile for Network Devices, version 2.1, dated 24-September-2018.

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.

Authorized Administrator—Person with appropriate permissions who is responsible for securely enabling, configuring, monitoring, and maintaining Junos OS in FIPS mode on a switch. For details, see "Understanding Roles and Services for Junos OS in Common Criteria and FIPS" on page 20.

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

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

FIPS maintenance role—The role the Authorized Administrator assumes to perform physical maintenance or logical maintenance services such as hardware or software diagnostics. For FIPS 140-2 compliance, the Authorized 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.

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

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 88.

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

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

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

Zeroization—Erasure of all CSPs and other user-created data on a switch before its operation as a FIPS cryptographic module—or in preparation for repurposing the switch for non-FIPS operation. The Authorized Administrator can zeroize the system with a CLI operational command. For details, see "Understanding Zeroization to Clear System Data" on page 31.

Supported Cryptographic Algorithms

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

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

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

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

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

ECDSA—Elliptic Curve Digital Signature Algorithm. A variant of the Digital Signature Algorithm (DSA) that uses cryptography based on the algebraic structure of elliptic curves over finite fields. The bit size of the elliptic curve determines the difficulty of decrypting the key. The public key believed to be needed for ECDSA is about twice the size of the security level, in bits. ECDSA uses the P-256, P-384, and P-521 curves that can be configured under OpenSSH.

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

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

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

> **NOTE:** 3DES is supported only in FIPS.

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

RELATED DOCUMENTATION

Understanding FIPS Self-Tests **| 88**

Understanding Zeroization to Clear System Data **| 31**

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.

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

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

Security Administrator roles and responsibilities are as follows:

1. Security Administrator can administer the TOE locally and remotely.

2. Create, modify, and delete administrator accounts, including configuration of authentication failure parameters.

3. Re-enable an Administrator account.

4. Responsible for the configuration and maintenance of cryptographic elements related to the establishment of secure connections to and from the evaluated product.

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

All other user types defined for Junos OS in FIPS mode (read-only, administrative user, and so on) must fall into one of the two categories: Authorized Administrator or FIPS user. For this reason, user authentication in Junos is identity based with role based authorization.

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

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

Authorized Administrator Role and Responsibilities

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

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

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

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

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

FIPS User Role and Responsibilities

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

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

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

What Is Expected of All FIPS Users

All FIPS users, including the Authorized 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

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*.

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

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

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

Software Environment for Junos OS in FIPS Mode

An EX 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 19.1R2 for EX2300 and EX3400. The Junos OS in FIPS mode software environment is established after the Authorized 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 after enabling FIPS mode.

> **NOTE:** Do not attach the switch to a network until you, the Authorized 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 3 on page 25 lists CSPs on switches running Junos OS.

Table 3: Critical Security Parameters

CSP	Description	Zeroization method	Use
SSH-2 private host key	ECDSA key used to identify the host, generated the first time SSH is configured. RSA key used to identify the host, generated the first time SSH is configured.	Zeroize command.	Used to identify the host.
SSH-2 session key	Session key used with SSH-2. and as a Diffie-Hellman private key. Encryption: 3DES (FIPS only), AES-128, AES-256. MACs: HMAC-SHA-1, HMAC SHA-256, HMAC SHA-512. Key exchange: DH Group exchange (2048 ≤ key ≤ 8192), ECDH: ECDH-sha2-nistp256, ECDH-sha2-nistp384, and ECDH-sha2-nistp521.	Power cycle and terminate session.	Symmetric key used to encrypt data between host and client.
User authentication key	Hash of the user's password: SHA-256, SHA-512.	Zeroize command.	Used to authenticate a user to the cryptographic module.
Authorized Administrator authentication key	Hash of the Authorized Administrator's password: SHA-256, SHA-512.	Zeroize command.	Used to authenticate the Authorized 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.

Table 3: Critical Security Parameters *(continued)*

CSP	Description	Zeroization method	Use
NDRNG entropy	Used as entropy input string to the HMAC DRBG.	Power cycle.	A critical value of the internal state of DRBG.

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

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

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

RELATED DOCUMENTATION

Understanding Password Specifications and Guidelines for Junos OS

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

- **Length.** Passwords must be a minimum of 10 characters long, and a maximum of 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. Include at least one change of case, one or more digits, and one or more punctuation marks.

- Changed periodically.

- Not divulged to anyone.

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

- Words that might be found in or exist as a permuted form in a system files such as **/etc/passwd**.

- The hostname of the system (always a first guess).

- Any word or phrase that appears in a dictionary or other well-known source, including dictionaries and thesauruses in languages other than English; works by classical or popular writers; or common words and phrases from sports, sayings, movies or television shows.

- Permutations on any of the above—for example, a dictionary word with letters replaced with digits (**root**) or with digits added to the end.

- Any machine-generated password. Algorithms reduce the search space of password-guessing programs and so must not be used.

RELATED DOCUMENTATION

Understanding the Operational Environment for Junos OS in FIPS Mode | **23**

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 EX2300 and EX3400 switches, Release 19.1R2

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

To download software packages from Juniper Networks:

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

   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 EX2300 and EX3400, the image is **junos-arm-32-19.1R2.8.tgz**.

4. The hash values/checksum for the image **junos-arm-32-19.1R2.8.tgz** is available at
   https://support.juniper.net/support/downloads

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

6. Compute the hash locally for the downloaded file.

7. Manually compare the published hash value with a hash value computed over the downloaded file

8. If the hash values match, the administrator should proceed with the installation. If the values do not match, the update should be discarded and the administrator should contact Juniper Networks.

9. Install the Junos OS. See "Installing Software on an EX Series devices with a Single Routing Engine" on page 29.

RELATED DOCUMENTATION

Installing Software on an EX Series devices with a Single Routing Engine | 29

Installing Software on an 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 Connecting and Configuring an EX Series Switch (CLI Procedure) for EX2300 and EX3400 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, **junos-arm-32-19.1R2.8.tgz** .

  - **ftp://*hostname*/*pathname*/*package*.tgz**

  - **http://*hostname*/*pathname*/*package*.tgz**

> **NOTE:** If you need to terminate the installation, do not reboot your switch; instead, finish the installation and then issue the **request system software delete *package*.tgz** command, where *package*.**tgz** is, for example, **junos-arm-32-19.1R2.8.tgz**. This is your last chance to stop the installation.

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

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

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

```
user@switch:> show version local
Model: ex3400-24p
Junos: 19.1R1.6
JUNOS OS Kernel 32-bit  [20190305.df99236_builder_stable_11]
JUNOS OS libs [20190305.df99236_builder_stable_11]
JUNOS OS runtime [20190305.df99236_builder_stable_11]
JUNOS OS time zone information [20190305.df99236_builder_stable_11]
JUNOS py extensions [20190321.051058_builder_junos_191_r1]
JUNOS py base [20190321.051058_builder_junos_191_r1]
JUNOS OS crypto [20190305.df99236_builder_stable_11]
JUNOS network stack and utilities [20190321.051058_builder_junos_191_r1]
JUNOS libs [20190321.051058_builder_junos_191_r1]
JUNOS runtime [20190321.051058_builder_junos_191_r1]
JUNOS Web Management Platform Package [20190321.051058_builder_junos_191_r1]
JUNOS ex libs [20190321.051058_builder_junos_191_r1]
JUNOS ex runtime [20190321.051058_builder_junos_191_r1]
JUNOS ex platform support [20190321.051058_builder_junos_191_r1]
```

```
JUNOS dcp network modules [20190321.051058_builder_junos_191_r1]
JUNOS modules [20190321.051058_builder_junos_191_r1]
JUNOS ex modules [20190321.051058_builder_junos_191_r1]
JUNOS ex Data Plane Crypto Support [20190321.051058_builder_junos_191_r1]
JUNOS daemons [20190321.051058_builder_junos_191_r1]
JUNOS SDN Software Suite [20190321.051058_builder_junos_191_r1]
JUNOS Extension Toolkit [20190321.051058_builder_junos_191_r1]
JUNOS Phone-home [20190321.051058_builder_junos_191_r1]
JUNOS Packet Forwarding Engine Support (EX34XX)
[20190321.051058_builder_junos_191_r1]
JUNOS jdocs ex [20190321.051058_builder_junos_191_r1]
JUNOS jail runtime [20190305.df99236_builder_stable_11]
JUNOS FIPS mode utilities [20190321.051058_builder_junos_191_r1]
```

RELATED DOCUMENTATION

Troubleshooting Software Installation

Understanding Software Installation on EX Series Switches

Understanding Zeroization to Clear System Data

IN THIS SECTION

- Why Zeroize? | **32**
- When to Zeroize? | **32**

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

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

> ⚠️ **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 n a valid Common Criteria configuration until all critical security parameters (CSPs) have been entered—or reentered—in accordance with the guidance provided in this document.

> **BEST PRACTICE:** You must zeroize the system to remove sensitive information before repurposing the switch.

When to Zeroize?

As Authorized Administrator, perform zeroization in the following situations:

- **Before Enabling FIPS mode of operation:** To prepare your switch for operation to comply with the requirements of NDcPP Version 2.1, perform zeroization before applying the guidance provided in this document.

- **Before repurposing:** To begin repurposing, perform zeroization on the switch.

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

RELATED DOCUMENTATION

Zeroizing the System

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

You must zeroize the system to remove sensitive information before repurposing the switch.

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

To zeroize your switch:

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

1. From the CLI, enter

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

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

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

> **NOTE:** The sample output might vary for EX2300 and EX3400 device.

Establishing Root Password Access

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

As Authorized Administrator, you must establish a root password conforming to the FIPS password requirements in "Understanding Password Specifications and Guidelines for Junos OS" on page 27. If you enable FIPS mode in Junos OS on the switch, you cannot configure passwords unless they meet this standard.

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

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

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

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

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

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

    > [edit]
    > root@switch# **set system login password format** (sha256 | sha512)

    > **NOTE:** The authentication algorithm for plain-text passwords must be configured as sha256 for EX2300 and EX3400 switches.

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

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

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

    Ensure that you follow the password guidelines in "Understanding Password Specifications and Guidelines for Junos OS" on page 27.

    - To configure public keys for SSH authentication of root logins, use the **ssh-ecdsa** option. You can configure more than one public key for SSH authentication of root logins and for user accounts. When a user logs in as **root**, the public keys are referenced to determine whether the private key matches any of them.

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

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

RELATED DOCUMENTATION

For more information about the root password and root logins, see the *Junos OS System Basics Configuration Guide*.

Enabling FIPS Mode

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

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

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

To enable FIPS mode in Junos OS on the switch:

1. Enter configuration mode:

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

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

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

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

3. Commit the configuration:

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

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

4. Reboot the switch:

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

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

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

```
mgd:    NIST 800-90 HMAC DRBG Known Answer Test:          Passed
mgd:    FIPS ECDSA Known Answer Test:                     Passed
mgd:    FIPS ECDH Known Answer Test:                      Passed
mgd:    FIPS RSA Known Answer Test:                       Passed
mgd:    DES3-CBC Known Answer Test:                       Passed
mgd:    HMAC-SHA1 Known Answer Test:                      Passed
mgd:    HMAC-SHA2-224 Known Answer Test:                  Passed
mgd:    HMAC-SHA2-256 Known Answer Test:                  Passed
mgd:    HMAC-SHA2-384 Known Answer Test:                  Passed
mgd:    HMAC-SHA2-512 Known Answer Test:                  Passed
mgd:    AES-CBC Known Answer Test:                        Passed
mgd:    AES-GCM Known Answer Test:                        Passed
mgd:    ECDSA-SIGN Known Answer Test:                     Passed
mgd:    KDF-IKE-V1 Known Answer Test:                     Passed
mgd:    KDF-SSH-SHA256 Known Answer Test:                 Passed
mgd: Testing QuickSec 7.0 KATS:
mgd:    NIST 800-90 HMAC DRBG Known Answer Test:          Passed
mgd:    DES3-CBC Known Answer Test:                       Passed
mgd:    HMAC-SHA1 Known Answer Test:                      Passed
mgd:    HMAC-SHA2-224 Known Answer Test:                  Passed
mgd:    HMAC-SHA2-256 Known Answer Test:                  Passed
mgd:    HMAC-SHA2-384 Known Answer Test:                  Passed
mgd:    HMAC-SHA2-512 Known Answer Test:                  Passed
mgd:    AES-CBC Known Answer Test:                        Passed
mgd:    AES-GCM Known Answer Test:                        Passed
mgd:    SSH-RSA-ENC Known Answer Test:                    Passed
mgd:    SSH-RSA-SIGN Known Answer Test:                   Passed
mgd:    SSH-ECDSA-SIGN Known Answer Test:                 Passed
mgd:    KDF-IKE-V1 Known Answer Test:                     Passed
mgd:    KDF-IKE-V2 Known Answer Test:                     Passed
mgd: Testing QuickSec KATS:
mgd:    NIST 800-90 HMAC DRBG Known Answer Test:          Passed
mgd:    DES3-CBC Known Answer Test:                       Passed
mgd:    HMAC-SHA1 Known Answer Test:                      Passed
mgd:    HMAC-SHA2-224 Known Answer Test:                  Passed
mgd:    HMAC-SHA2-256 Known Answer Test:                  Passed
mgd:    HMAC-SHA2-384 Known Answer Test:                  Passed
mgd:    HMAC-SHA2-512 Known Answer Test:                  Passed
mgd:    AES-CBC Known Answer Test:                        Passed
mgd:    AES-GCM Known Answer Test:                        Passed
mgd:    SSH-RSA-ENC Known Answer Test:                    Passed
mgd:    SSH-RSA-SIGN Known Answer Test:                   Passed
mgd:    KDF-IKE-V1 Known Answer Test:                     Passed
mgd:    KDF-IKE-V2 Known Answer Test:                     Passed
```

```
mgd: Testing SSH IPsec KATS:
mgd:   NIST 800-90 HMAC DRBG Known Answer Test:        Passed
mgd:   DES3-CBC Known Answer Test:                     Passed
mgd:   HMAC-SHA1 Known Answer Test:                    Passed
mgd:   HMAC-SHA2-256 Known Answer Test:                Passed
mgd:   AES-CBC Known Answer Test:                      Passed
mgd:   SSH-RSA-ENC Known Answer Test:                  Passed
mgd:   SSH-RSA-SIGN Known Answer Test:                 Passed
mgd:   KDF-IKE-V1 Known Answer Test:                   Passed
mgd: Testing file integrity:
mgd:   File integrity Known Answer Test:               Passed
mgd: Testing crypto integrity:
mgd:   Crypto integrity Known Answer Test:             Passed
mgd: Expect an exec Authentication error...
veriexec: no signatures for device. file='/sbin/kats/cannot-exec' fsid=192
fileid=51404 gen=1 uid=0 pid=4818
mgd: /sbin/kats/run-tests: /sbin/kats/cannot-exec: Authentication error
mgd: FIPS Self-tests Passed
```

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

```
--- JUNOS 18.1R3-S2-20170816 built 2014-12-29 04:12:22 UTC
root@switch:fips>
```

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

```
user@switch:fips> show version local
Model: ex3400-24p
Junos: 19.1R1.6
JUNOS OS Kernel 32-bit  [20190305.df99236_builder_stable_11]
JUNOS OS libs [20190305.df99236_builder_stable_11]
JUNOS OS runtime [20190305.df99236_builder_stable_11]
JUNOS OS time zone information [20190305.df99236_builder_stable_11]
JUNOS py extensions [20190321.051058_builder_junos_191_r1]
JUNOS py base [20190321.051058_builder_junos_191_r1]
JUNOS OS crypto [20190305.df99236_builder_stable_11]
JUNOS network stack and utilities [20190321.051058_builder_junos_191_r1]
JUNOS libs [20190321.051058_builder_junos_191_r1]
JUNOS runtime [20190321.051058_builder_junos_191_r1]
JUNOS Web Management Platform Package [20190321.051058_builder_junos_191_r1]
JUNOS ex libs [20190321.051058_builder_junos_191_r1]
JUNOS ex runtime [20190321.051058_builder_junos_191_r1]
JUNOS ex platform support [20190321.051058_builder_junos_191_r1]
```

```
JUNOS dcp network modules [20190321.051058_builder_junos_191_r1]
JUNOS modules [20190321.051058_builder_junos_191_r1]
JUNOS ex modules [20190321.051058_builder_junos_191_r1]
JUNOS ex Data Plane Crypto Support [20190321.051058_builder_junos_191_r1]
JUNOS daemons [20190321.051058_builder_junos_191_r1]
JUNOS SDN Software Suite [20190321.051058_builder_junos_191_r1]
JUNOS Extension Toolkit [20190321.051058_builder_junos_191_r1]
JUNOS Phone-home [20190321.051058_builder_junos_191_r1]
JUNOS Packet Forwarding Engine Support (EX34XX)
[20190321.051058_builder_junos_191_r1]
JUNOS jdocs ex [20190321.051058_builder_junos_191_r1]
JUNOS jail runtime [20190305.df99236_builder_stable_11]
JUNOS FIPS mode utilities [20190321.051058_builder_junos_191_r1]
```

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

RELATED DOCUMENTATION

Configuring Authorized Administrator and FIPS User Identification and Access

IN THIS SECTION

- Configuring Authorized Administrator Login Access | 41
- Configuring FIPS User Login Access | 42

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

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

To configure login access for a Authorized Administrator:

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

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

2. Name the user "authorized-administrator" and assign the Authorized 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:fips# set system login user authorized-administrator uid 6400 class super-user
   ```

3. Following the guidelines in "Understanding Password Specifications and Guidelines for Junos OS" on page 27, assign the Authorized 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:fips# set system login user authorized-administrator class super-user authentication
       plain-text-password
   ```

4. Optionally, display the configuration:

   ```
   [edit]
   root@switch:fips# edit system
   [edit system]
   root@switch:fips# show
   login {
   ```

```
    user authorized-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:fips# commit
commit complete
   root@switch:fips# exit
   root@switch:fips> exit
```

Otherwise, go on to .

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 Authorized Administrator, you set up FIPS users.

To configure login access for a FIPS user:

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

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

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

```
[edit]
authorized-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" on page 27, assign the FIPS a plain-text password for login authentication. Set the password by typing a password after the prompts **New password** and **Retype new password**.

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

4. Optionally, display the configuration:

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

RELATED DOCUMENTATION

Understanding Roles and Services for Junos OS in Common Criteria and FIPS | 20

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

- Contain the minimum number of character sets or character set changes. The minimum number of character sets required in plain-text passwords in Junos FIPS is 3.

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

- Contain the minimum number of characters required for a password. For the purposes of the evaluated configuration the minimum password length must be configured as 10 characters. (A maximum of 20 characters)

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

> **NOTE:** The authentication algorithm for plain-text passwords must be configured as sha256 for EX2300 and EX3400 switches.
>
> ```
> [ edit ]
> administrator@host# set system login password format sha256
> ```

Weak passwords are:

- Words that might be found in or exist as a permuted form in a system file such as **/etc/passwd**.

- The hostname of the system (always a first guess).

- Any words appearing in a dictionary. This includes dictionaries other than English, and words found in works such as Shakespeare, Lewis Carroll, Roget's Thesaurus, and so on. This prohibition includes common words and phrases from sports, sayings, movies, and television shows.

- Permutations on any of the above. For example, a dictionary word with vowels replaced with digits (for example f00t) or with digits added to the end.

- Any machine-generated passwords. Algorithms reduce the search space of password-guessing programs and so should not be used.

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

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

RELATED DOCUMENTATION

Identifying Secure Product Delivery | 17

Authentication Methods in FIPS Mode of Operation

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

Username and Password Authentication over the Console and SSH

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

> **NOTE:** The maximum password length is 20 characters.

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

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

Username and Public Key Authentication over SSH

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

RELATED DOCUMENTATION

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

2. Configure the hashing algorithm used for password storage as sha256.

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

   > **NOTE:** The authentication algorithm for plain-text passwords must be configured as sha256 for EX2300 and EX3400 switches.

3. Commit the changes.

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

4. Define your NDcPP Version 2.1 authorized administrator.

   ```
   [edit]
   ```

```
root@host# set system login user user-name class security-admin authentication encrypted-password
    <password>
```

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

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

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

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

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

7. Commit the changes.

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

RELATED DOCUMENTATION

Understanding the Associated Password Rules for an Authorized Administrator **| 45**

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]
user@host# **set system login message** *login-message-banner-text*

To configure system announcement, use the following command:

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

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

RELATED DOCUMENTATION

Configuring SSH on the Evaluated Configuration

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

- Before you begin, log in with your root account on the device.

To configure SSH on the device:

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

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

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

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

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

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

4. Specify the ciphers allowed for protocol version 2.

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

5. Specify the number of minutes or maximum amount of data, before a rekey is forced on a session.

```
[edit system services ssh]
user@host# set rekey time-limit 60
user@host# set rekey data-limit 1g
```

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

An administrator may login remotely to a device through SSH. Administrator credentials are stored locally on the device. If the administrator presents a valid username and password, access to the Target of Evaluation (TOE) is granted. If the credentials are invalid, the TOE allows the authentication to be retried after an interval that starts after 1 second and increases exponentially. If the number of authentication attempts exceed the configured maximum, no authentication attempts are accepted for a configured time interval. When the interval expires, authentication attempts are again accepted.

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

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

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

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

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

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

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

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

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

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

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

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

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

RELATED DOCUMENTATION

Configuring SSH on the Evaluated Configuration | 52

Configuring the Time and Date

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

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

RELATED DOCUMENTATION

Configuring SSH on the Evaluated Configuration

Configuring the user session idle timeout

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

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

Terminating a local or remote session

- To exit a local or remote session, use either of the following commands:

  -
    user@host> **exit**

  -
    user@host> **quit**

5
CHAPTER

Configuring the Remote Syslog Server

Syslog Server Configuration on a Linux System

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

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

- Committed changes

- Login and logout of users

- Failure to establish an SSH session

- Establishment or termination of an SSH session

- Changes to the system time

Configuring Event Logging to a Local File

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

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

Configuring Event Logging to a Remote Server

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

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

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

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

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

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

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

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

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

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

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

4. Set up NETCONF with SSH.

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

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

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

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

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

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

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

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

8. After logging in to the **external_syslog_server** session, establish a tunnel to the device and start NETCONF.

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

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

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

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

SSH through remote management interface allowed in the evaluated configuration. If the existing ssh connection is broken unintentionally, for example reboot, re-initiate the connection after the device is up. There is no mechanism to retain an existing or established connection, which is broken. This topic describes how to configure SSH for remote management of TOE. The following algorithms that needs to be configured to validate SSH for NDcPP.

The following output shows test log results for syslog server.

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

Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
```

```
Enter same passphrase again:
Your identification has been saved in /home/host/.ssh/syslog-monitor.
Your public key has been saved in /home/host/.ssh/syslog-monitor.pub.
The key fingerprint is:
ef:75:d7:68:c5:ad:8d:6f:5e:7a:7e:9b:3d:f1:4d:3f syslog-monitor key pair
The key's randomart image is:
+--[ RSA 2048]----+
|                 |
|                 |
|                 |
|              ..|
|       S      +|
|        .     Bo|
|        . . *.X|
|        . . o E@|
|        .   .BX|
+-----------------+
[host@nms5-vm-linux2 ~]$ cat /home/host/.ssh/syslog-monitor.pub
ssh-rsa
 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`
Agent pid 1453
[host@nms5-vm-linux2 ~]$ ssh-add ~/.ssh/syslog-monitor
Enter passphrase for /home/host/.ssh/syslog-monitor:
Identity added: /home/host/.ssh/syslog-monitor (/home/host/.ssh/syslog-monitor)
```

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

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

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

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


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

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

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

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

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

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

```
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/dfcd'
....................................
```

```
Remote : an 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation
 in progress: Redundancy interface management process checking new configuration
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/rdd'
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child '/usr/sbin/rdd',
 PID 4317, status 0
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in
progress: Dynamic flow capture service checking new configuration
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_START: Starting child '/usr/sbin/dfcd'
Jan 20 17:09:30  starfire mgd[4186]: UI_CHILD_STATUS: Cleanup child
'/usr/sbin/dfcd', PID 4318, status 0
Jan 20 17:09:30  starfire mgd[4186]: UI_COMMIT_PROGRESS: Commit operation in
progress: Connectivity fault management process checking new configuration
...............
```

6

CHAPTER

Configuring Audit Log Options

Configuring Audit Log Options in the Evaluated Configuration

Locally stored audit data is protected by the access controls applied by Junos OS filesystem, and no additional configuration is required to protect the audit logs on the EX2300 and EX3400 devices. The following section describes how to configure audit log options in the evaluated configuration.

Configuring Audit Log Options for EX2300 and EX3400 Devices

To configure audit log options for EX2300 and EX3400 devices:

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

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

2. Specify the file in which to log data.

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

3. Specify the size of files to be archived.

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

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

   ```
   [edit system syslog]
   ```

```
root@host#set file  Audit_logs explicit-priority
```

5. Log system messages in a structured format.

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

Sample Code Audits of Configuration Changes

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

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

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

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

```
        pfe info;
    }
}
```

Example: System Logging of Configuration Changes

This example shows a sample configuration and makes changes to users and secret data.

```
[edit system]
location {
    country-code US;
    building B1;
}
...
login {
    message "UNAUTHORIZED USE OF THIS ROUTER\n\tIS STRICTLY PROHIBITED!";
        user admin {
            uid 2000;
             class super-user;
        authentication {
            encrypted-password "$ABC123";
            # SECRET-DATA
        }
    }
    password {
        format sha512;
    }
}
radius-server 192.0.2.15 {
    secret "$ABC123" # SECRET-DATA
}
services {
    ssh;
}
syslog {
    user *{
        any emergency;
    }
    file messages {
        any notice;
        authorization info;
    }
```

```
      file interactive-commands {
         interactive-commands any;
       }
    }
    ...
    ...
```

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

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

Table 4 on page 69 shows sample for syslog auditing for NDcPPv2.1:

Table 4: Auditable Events

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

Table 4: Auditable Events *(continued)*

Requirement	Auditable Events	Additional Audit Record Contents	How Event is Generated
			SSH Nov 6 17:01:11 sshd[15077]: %AUTH-6: Accepted keyboard-interactive/pam for test from 192.168.228.71 port 57500 ssh2 Nov 6 17:01:12 mgd[15082]: %INTERACT-6-UI_AUTH_EVENT: Authenticated user 'test' assigned to class 'j-read-only' Nov 6 17:01:12 mgd[15082]: %INTERACT-6-UI_LOGIN_EVENT: User 'test' login, class 'j-read-only' [15082], ssh-connection '192.168.228.71 57500 10.1.2.86 22', client-mode 'cli' Nov 7 13:33:09 sshd[16791]: %AUTH-7: (pam_sm_authenticate): DEBUG: Updating lock-attempts of user: test attempts: 1 Nov 7 13:33:09 sshd[16789]: %AUTH-3: error: PAM: authentication error for test from 192.168.228.71 Nov 7 13:33:09 sshd: %AUTH-5-SSHD_LOGIN_FAILED: Login failed for user 'test' from host '192.168.228.71' Nov 7 13:33:09 sshd[16790]: %AUTH-6: Postponed keyboard-interactive for test from 192.168.228.71 port 57754 ssh2 Console Nov 6 19:17:22 login[15369]: %AUTH-7: (pam_sm_authenticate): DEBUG: Updating lock-attempts of user: acumensec attempts: 1 Nov 6 19:17:22 login[15369]: %AUTH-3-LOGIN_PAM_AUTHENTICATION_ERROR: Failed password for user acumensec Nov 6 19:17:22 login[15369]: %AUTH-5-LOGIN_FAILED: Login failed for user acumensec from host ttyu0 Nov 6 19:17:23 login[15369]: %AUTHPRIV-5: 1 LOGIN FAILURE ON ttyu0, acumensec Nov 6 19:17:32 login: %AUTH-5: Login attempt for user acumensec from host [unknown] Nov 6 19:17:33 login[15381]: %AUTH-7: (pam_sm_authenticate): DEBUG: PAM_USER:

Table 4: Auditable Events *(continued)*

Requirement	Auditable Events	Additional Audit Record Contents	How Event is Generated
			acumensec Nov 6 19:17:33 login[15381]: %AUTH-7: (pam_sm_authenticate): DEBUG: Updating lock-attempts of user: acumensec attempts: 2 Nov 6 19:17:33 login[15381]: %AUTH-3-LOGIN_PAM_AUTHENTICATION_ERROR: Failed password for user acumensec Nov 6 19:17:33 login[15381]: %AUTH-5-LOGIN_FAILED: Login failed for user acumensec from host ttyu0 Nov 6 19:13:48 login: %AUTH-5: Login attempt for user acumensec from host [unknown] Nov 6 19:13:52 login[15359]: %AUTH-7: (pam_sm_authenticate): DEBUG: PAM_USER: acumensec Nov 6 19:13:52 login[15359]: %AUTH-7: (pam_sm_authenticate): DEBUG: Updating lock-attempts of user: acumensec attempts: 1 Nov 6 19:13:52 login[15359]: %AUTH-7: (pam_sm_acct_mgmt): DEBUG: PAM_USER: acumensec Nov 6 19:13:52 login[15359]: %AUTH-6-LOGIN_INFORMATION: User acumensec logged in from host [unknown] on device ttyu0 Nov 6 19:13:53 mgd[15367]: %INTERACT-6-UI_AUTH_EVENT: Authenticated user 'acumensec' assigned to class 'j-super-user' Nov 6 19:13:53 mgd[15367]: %INTERACT-6-UI_LOGIN_EVENT: User 'acumensec' login, class 'j-super-user' [15367], ssh-connection '', client-mode 'cli'
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address)	

Table 4: Auditable Events *(continued)*

Requirement	Auditable Events	Additional Audit Record Contents	How Event is Generated
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).	

Table 4: Auditable Events *(continued)*

Requirement	Auditable Events	Additional Audit Record Contents	How Event is Generated
			Nov 7 13:24:27 mgd[16383]: %INTERACT-6-UI_CMDLINE_READ_LINE: User 'acumensec', command 'edit system login ' Nov 7 13:26:40 mgd[16383]: %CHANGE-6-UI_CFG_AUDIT_SET: User 'acumensec' set: [system login retry-options tries-before-disconnect] <unconfigured> -> "3" Nov 7 13:26:40 mgd[16383]: %INTERACT-6-UI_CMDLINE_READ_LINE: User 'acumensec', command 'set retry-options tries-before-disconnect 3 ' Nov 7 13:27:04 mgd[16383]: %CHANGE-6-UI_CFG_AUDIT_SET: User 'acumensec' set: [system login retry-options lockout-period] <unconfigured> -> "5" Nov 7 13:27:04 mgd[16383]: %INTERACT-6-UI_CMDLINE_READ_LINE: User 'acumensec', command 'set retry-options lockout-period 5 ' Nov 7 13:33:19 sshd: %AUTH-5-SSHD_LOGIN_FAILED: Login failed for user 'test' from host '192.168.228.71' Nov 7 13:33:34 sshd: %AUTH-5-SSHD_LOGIN_ATTEMPTS_THRESHOLD: Threshold for unsuccessful authentication attempts (3) reached by user 'test' Nov 7 13:33:34 sshd[16789]: %AUTH-6: Disconnecting: Too many password failures for test [preauth] Nov 7 13:34:33 sshd[16796]: %AUTH-7: (pam_sm_authenticate): DEBUG: PAM_USER: test Nov 7 13:34:33 sshd[16796]: %AUTH-7: (pam_sm_authenticate): DEBUG: Updating lock-attempts of user: test attempts: 4 Nov 7 13:34:33 sshd[16796]: %AUTH-7: (pam_sm_acct_mgmt): DEBUG: PAM_USER: test Nov 7 13:34:33 sshd[16796]: %AUTH-3: Account for user test is locked. Nov 7 13:34:33 sshd[16794]: %AUTH-3: error: PAM: user account has expired for test from 192.168.228.71 Nov 7 13:34:33 sshd: %AUTH-5-SSHD_LOGIN_FAILED:

Table 4: Auditable Events *(continued)*

Requirement	Auditable Events	Additional Audit Record Contents	How Event is Generated
			Login failed for user 'test' from host '192.168.228.71' Nov 7 13:40:16 sshd[16806]: %AUTH-5-LIBJNX_LOGIN_ACCOUNT_UNLOCKED: Account for user 'test' has been unlocked for logins
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process.	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)	Nov 7 14:10:34 mgd[17399]: %INTERACT-6-UI_CMDLINE_READ_LINE: User 'acumensec', command 'set date 202112270000.00 ' Nov 7 14:10:34 mgd[17399]: %INTERACT-6-UI_CHILD_START: Starting child '/bin/date' Dec 27 00:00:00 date: %AUTH-5: date set by root
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	No additional information.	Nov 13 13:30:08 mgd[10215]: UI_CMDLINE_READ_LINE: User 'acumensec', command 'request system software add /var/tmp/simple-pkg-x86-32_tmfink_BAD_FIRST_BYTE.tgz reboot ' Nov 13 13:30:08 mgd[10215]: PVIDB: Attribute 'mgd.mgd_packages_not_filtered' not present in Db Nov 13 13:30:08 mgd[10215]: UI_CHILD_START: Starting child '/usr/libexec/ui/package' Nov 13 13:30:08 mgd[10215]: /usr/libexec/ui/package -X update -reboot /var/tmp/simple-pkg-x86-32_tmfink_BAD_FIRST_BYTE.tgz Nov 13 13:30:11 veriexec[11981]: cannot validate /packages/ db/pkginst.11864/manifest.ecerts: subject issuer mismatch: /C=US/ST=CA/L=Sunnyvale/O=Juniper Networks/OU=Juniper CA/CN=PackageCA/emailAddress=ca@juniper.net Nov 13 13:30:11 veriexec[11982]: cannot validate /packages/db /pkginst.11864/manifest.ecerts: subject issuer mismatch: /C=US/ST=CA/L=Sunnyvale/O=Juniper Networks/OU=Juniper CA/CN=PackageCA /emailAddress=ca@juniper.net

Table 4: Auditable Events *(continued)*

Requirement	Auditable Events	Additional Audit Record Contents	How Event is Generated
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure	
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	No additional information.	
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.	Nov 7 12:58:36 sshd[19815]: %AUTH-7: (pam_sm_acct_mgmt): DEBUG: PAM_USER: acumensec Nov 7 12:58:36 sshd[19813]: %AUTH-6: Accepted keyboard-interactive/pam for acumensec from 192.168.228.71 port 57864 ssh2 Nov 7 12:58:38 mgd[19818]: %INTERACT-6-UI_AUTH_EVENT: Authenticated user 'acumensec' assigned to class 'j-super-user' Nov 7 12:58:38 mgd[19818]: %INTERACT-6-UI_LOGIN_EVENT: User 'acumensec' login, class 'j-super-user' [19818], ssh-connection '192.168.228.71 57864 10.1.2.86 22', client-mode 'cli'
FTA_SSL_EXT.1 (if terminate the session is selected)	The termination of a local interactive session by the session locking mechanism.	No additional information.	Nov 8 12:34:44 : %USER-6-UI_CLI_IDLE_TIMEOUT: Idle timeout for user 'juniper' exceeded and session terminated Nov 8 12:34:44 mgd[26870]: %INTERACT-6-UI_LOGOUT_EVENT: User 'juniper' logout
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	No additional information.	Nov 8 11:45:41 : %USER-6-UI_CLI_IDLE_TIMEOUT: Idle timeout for user 'juniper' exceeded and session terminated Nov 8 11:45:41 mgd[25926]: %INTERACT-6-UI_LOGOUT_EVENT: User 'juniper' logout

Table 4: Auditable Events *(continued)*

Requirement	Auditable Events	Additional Audit Record Contents	How Event is Generated
FTA_SSL.4	The termination of an interactive session.	No additional information.	Nov 7 17:51:31 mgd[17966]: %INTERACT-6-UI_CMDLINE_READ_LINE: User 'acumensec', command 'quit ' Nov 7 17:51:31 mgd[17966]: %INTERACT-6-UI_LOGOUT_EVENT: User 'acumensec' logout
FMT_MOF.1/ Manual Update	Any attempt to initiate a manual update	No additional information.	Nov 13 13:30:08 mgd[10215]: UI_CMDLINE_READ_LINE: User 'acumensec', command 'request system software add /var/tmp/simple-pkg-x86-32_tmfink_BAD_FIRST_BYTE.tgz reboot '

Table 4: Auditable Events *(continued)*

Requirement	Auditable Events	Additional Audit Record Contents	How Event is Generated
FMT_SMF.1	All management activities of TSF data.	No additional information	

Table 4: Auditable Events *(continued)*

Requirement	Auditable Events	Additional Audit Record Contents	How Event is Generated
			Nov 6 18:28:58 mgd[15264]: %INTERACT-6-UI_CMDLINE_READ_LINE: User 'acumensec', command 'request security pki generate-key-pair certificate-id rsa size 2048 type rsa '
			Nov 7 14:10:34 mgd[17399]: %INTERACT-6-UI_CMDLINE_READ_LINE: User 'acumensec', command 'set date 202112270000.00 '
			Nov 7 13:26:40 mgd[16383]: %INTERACT-6-UI_CMDLINE_READ_LINE: User 'acumensec', command 'set retry-options tries-before-disconnect 3 '
			Nov 7 13:27:04 mgd[16383]: %INTERACT-6-UI_CMDLINE_READ_LINE: User 'acumensec', command 'set retry-options lockout-period 5 '
			Nov 7 15:51:11 mgd[16916]: %INTERACT-6-UI_CMDLINE_READ_LINE: User 'acumensec', command 'set system login user good1 class super-user authentication plain-text-password '
			Nov 6 19:30:44 mgd[15415]: %INTERACT-6-UI_CMDLINE_READ_LINE: User 'acumensec', command 'edit '
			Nov 6 19:30:44 mgd[15415]: %INTERACT-5-UI_DBASE_LOGIN_EVENT: User 'acumensec' entering configuration mode
			Nov 6 16:57:39 mgd[15062]: %INTERACT-6-UI_CMDLINE_READ_LINE: User 'acumensec', command 'set system services netconf ssh '
			Nov 13 13:30:08 mgd[10215]: UI_CMDLINE_READ_LINE: User 'acumensec', command 'request system software add /var/tmp/simple-pkg-x86-32_tmfink_BAD_FIRST_BYTE.tgz reboot '
			Nov 8 11:42:32 mgd[21811]: %CHANGE-6-UI_CFG_AUDIT_SET: User 'acumensec' set: [system login class security-admin

Table 4: Auditable Events *(continued)*

Requirement	Auditable Events	Additional Audit Record Contents	How Event is Generated
			idle-timeout] "1 -> "1" Nov 8 11:42:32 mgd[21811]: %INTERACT-6-UI_CMDLINE_READ_LINE: User 'acumensec', command 'set system login class security-admin idle-timeout 1 ' Nov 8 11:42:44 mgd[21811]: %INTERACT-6-UI_CMDLINE_READ_LINE: User 'acumensec', command 'commit ' Nov 7 18:03:07 mgd[18482]: %INTERACT-6-UI_CMDLINE_READ_LINE: User 'acumensec', command 'set system login message "Warning: ONLY AUTHORIZED USERS" ' Nov 7 13:24:27 mgd[16383]: %INTERACT-6-UI_CMDLINE_READ_LINE: User 'acumensec', command 'edit system login '

RELATED DOCUMENTATION

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 following events:

- Starting and stopping services.
- Changes to configuration of audit behavior.
- Changes to thresholds for SSH re-keying.
- 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;
}
```

RELATED DOCUMENTATION

Interpreting Event Messages

The following output shows a sample event message.

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

describes the fields for an event message. If the system logging utility cannot determine the value in a particular field, a hyphen (-) appears instead.

Table 5: Fields in Event Messages

Field	Description	Examples
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.	Jul 24 17:43:28 is the timestamp expressed as local time in the United States. 2012-07-24T09:17:15.719Z is 9:17 AM UTC on 24 July 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.

Load Merge

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

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

Load Replace

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

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

Load Override

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

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

Load Update

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

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

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

RELATED DOCUMENTATION

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 | 82

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 | 85

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

- **quicksec_7_0_kats**—KAT for Quicksec_7_0 Toolkit cryptographic implementation

- **openssl_kats**—KAT for OpenSSL cryptographic implementation

- **kernel_kats**——KAT for kernel cryptographic routines

Although KAT self-tests are performed for all four cryptographic libraries, only algorithms from the md, openssl, and kernel libraries are invoked in the NDcPP v2.1 configuration. No algorithms from quicksec are used for NDcPP v2.1 conformance.

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

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

If one of the KATs fail, the device panics and reboot continuously. The device can be recovered using USB install.

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

Performing Power-On Self-Tests on the Device

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

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

```
Verified manifest signed by PackageDevelopmentEc_2017 method ECDSA256+SHA256
cp: /var/host/junos-defaults.conf: No such file or directory
mount_cd9660: /dev/gpt/junos: Invalid argument
ifconfig: devop error: Device not configured
 bcmsdk_5_9_x kldKLD bcmsdk_5_9_x.ko: depends on acb - not available or version
```

```
mismatch
linker_load_file: Unsupported file type
kldload: an error occurred while loading the module. Please check dmesg(8) for
more details.
Junosprocfs mounted on /junosproc.
@ 1511776671 [2017-11-27 09:57:51 UTC] mgd start
Creating initial configuration:  ...
mgd: Running FIPS Self-tests
mgd: Testing kernel KATS:
mgd:   NIST 800-90 HMAC DRBG Known Answer Test:        Passed
mgd:   DES3-CBC Known Answer Test:                     Passed
mgd:   HMAC-SHA1 Known Answer Test:                    Passed
mgd:   HMAC-SHA2-256 Known Answer Test:                Passed
mgd:   SHA-2-384 Known Answer Test:                    Passed
mgd:   SHA-2-512 Known Answer Test:                    Passed
mgd:   AES128-CMAC Known Answer Test:                  Passed
mgd:   AES-CBC Known Answer Test:                      Passed
mgd: Testing MacSec KATS:
mgd:   AES128-CMAC Known Answer Test:                  Passed
mgd:   AES256-CMAC Known Answer Test:                  Passed
mgd:   AES-KEYWRAP Known Answer Test:                  Passed
mgd: Testing libmd KATS:
mgd:   HMAC-SHA1 Known Answer Test:                    Passed
mgd:   HMAC-SHA2-256 Known Answer Test:                Passed
mgd:   SHA-2-512 Known Answer Test:                    Passed
mgd: Testing OpenSSL KATS:
mgd:   FIPS RNG Known Answer Test:                     Passed
mgd:   NIST 800-90 HMAC DRBG Known Answer Test:        Passed
mgd:   FIPS ECDSA Known Answer Test:                   Passed
mgd:   FIPS ECDH Known Answer Test:                    Passed
mgd:   FIPS RSA Known Answer Test:                     Passed
mgd:   DES3-CBC Known Answer Test:                     Passed
mgd:   HMAC-SHA1 Known Answer Test:                    Passed
mgd:   HMAC-SHA2-224 Known Answer Test:                Passed
mgd:   HMAC-SHA2-256 Known Answer Test:                Passed
mgd:   HMAC-SHA2-384 Known Answer Test:                Passed
mgd:   HMAC-SHA2-512 Known Answer Test:                Passed
mgd:   AES-CBC Known Answer Test:                      Passed
mgd:   AES-GCM Known Answer Test:                      Passed
mgd:   ECDSA-SIGN Known Answer Test:                   Passed
mgd:   KDF-IKE-V1 Known Answer Test:                   Passed
mgd:   KDF-SSH-SHA256 Known Answer Test:               Passed
mgd: Testing QuickSec 7.0 KATS:
mgd:   NIST 800-90 HMAC DRBG Known Answer Test:        Passed
```

```
mgd:    DES3-CBC Known Answer Test:                      Passed
mgd:    HMAC-SHA1 Known Answer Test:                     Passed
mgd:    HMAC-SHA2-224 Known Answer Test:                 Passed
mgd:    HMAC-SHA2-256 Known Answer Test:                 Passed
mgd:    HMAC-SHA2-384 Known Answer Test:                 Passed
mgd:    HMAC-SHA2-512 Known Answer Test:                 Passed
mgd:    AES-CBC Known Answer Test:                       Passed
mgd:    AES-GCM Known Answer Test:                        Passed
mgd:    SSH-RSA-ENC Known Answer Test:                   Passed
mgd:    SSH-RSA-SIGN Known Answer Test:                  Passed
mgd:    SSH-ECDSA-SIGN Known Answer Test:                Passed
mgd:    KDF-IKE-V1 Known Answer Test:                    Passed
mgd:    KDF-IKE-V2 Known Answer Test:                    Passed
mgd: Testing QuickSec KATS:
mgd:    NIST 800-90 HMAC DRBG Known Answer Test:         Passed
mgd:    DES3-CBC Known Answer Test:                      Passed
mgd:    HMAC-SHA1 Known Answer Test:                     Passed
mgd:    HMAC-SHA2-224 Known Answer Test:                 Passed
mgd:    HMAC-SHA2-256 Known Answer Test:                 Passed
mgd:    HMAC-SHA2-384 Known Answer Test:                 Passed
mgd:    HMAC-SHA2-512 Known Answer Test:                 Passed
mgd:    AES-CBC Known Answer Test:                       Passed
mgd:    AES-GCM Known Answer Test:                        Passed
mgd:    SSH-RSA-ENC Known Answer Test:                   Passed
mgd:    SSH-RSA-SIGN Known Answer Test:                  Passed
mgd:    KDF-IKE-V1 Known Answer Test:                    Passed
mgd:    KDF-IKE-V2 Known Answer Test:                    Passed
mgd: Testing SSH IPsec KATS:
mgd:    NIST 800-90 HMAC DRBG Known Answer Test:         Passed
mgd:    DES3-CBC Known Answer Test:                      Passed
mgd:    HMAC-SHA1 Known Answer Test:                     Passed
mgd:    HMAC-SHA2-256 Known Answer Test:                 Passed
mgd:    AES-CBC Known Answer Test:                       Passed
mgd:    SSH-RSA-ENC Known Answer Test:                   Passed
mgd:    SSH-RSA-SIGN Known Answer Test:                  Passed
mgd:    KDF-IKE-V1 Known Answer Test:                    Passed
mgd: Testing file integrity:
mgd:    File integrity Known Answer Test:                Passed
mgd: Testing crypto integrity:
mgd:    Crypto integrity Known Answer Test:              Passed
mgd: Expect an exec Authentication error...
veriexec: no signatures for device. file='/sbin/kats/cannot-exec' fsid=192
fileid=51404 gen=1 uid=0 pid=4818
```

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

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

The self-test output for non-FIPS mode:

```
Junosprocfs mounted on /junosproc.
loader.name="FreeBSD/armv6 U-Boot loader"
loader.version="1.2"
FreeBSD/armv6 U-Boot loader
1.2918+0 records in
918+0 records out
477360 bytes transferred in 0.038118 secs (12523078 bytes/sec)
@ 1585074069 [2020-03-24 18:21:09 UTC] mgd start
Creating initial configuration:  ...mgd: Running FIPS Self-tests
veriexec: no fingerprint for file='/sbin/kats/cannot-exec' fsid=171 fileid=49356
gen=1 uid=0 pid=13089
mgd: FIPS Self-tests Passed
<output>Generating RSA key /etc/ssh/ssh_host_key</output>
<output>Generated SSH key file /etc/ssh/ssh_host_key.pub with fingerprint
SHA256:16UKRuM1AAKa7wD8IAL6OS2MVoCSHS3KLKwbTjs+i7k

Generating public/private rsa1 key pair.
Your identification has been saved in /etc/ssh/ssh_host_key.
Your public key has been saved in /etc/ssh/ssh_host_key.pub.
The key fingerprint is:
SHA256:16UKRuM1AAKa7wD8IAL6OS2MVoCSHS3KLKwbTjs+i7k root@
The key's randomart image is:+---[RSA1 2048]---+
|o+o+. ...        |
|Bo+ ..   .       |
|%+ o    o o   .  |
|*O+o   o o o o   |
|=.B..    S . o   |
|++ o   . o .     |
|ooo        .     |
|o*               |
|E++              |
+----[SHA256]-----+
```

```
mgd: commit complete
@ 1585074211 [2020-03-24 18:23:31 UTC] mgd doneLock Manager
RDM Embedded 7 [04-Aug-2006] http://www.birdstep.com
Copyright (c) 1992-2006 Birdstep Technology, Inc.  All Rights Reserved.


Unix Domain sockets Lock manager
Lock manager 'lockmgr' started successfully.


Database Initialization Utility
RDM Embedded 7 [04-Aug-2006] http://www.birdstep.com
Copyright (c) 1992-2006 Birdstep Technology, Inc.  All Rights Reserved.Profile
database initialized
umount: /jail/var/tmp/uploads: not a file system root directory
Enhanced arp scale is disabled
/etc/rc: WARNING: No dump device.  Savecore not run.
Prefetching /usr/sbin/rpd ...
Prefetching /usr/sbin/lacpd ...
Prefetching /usr/sbin/chassisd ...
Starting jlaunchhelperd.
sysctl: unknown oid 'kern.rtc_retries'
Starting cron.
Tue Mar 24 18:24:02 UTC 2020
FreeBSD/arm (Amnesiac) (ttyu0)
login:
```

9
CHAPTER

Configuration Statements

fips

Syntax

```
fips {
    level level;
    }
```

Hierarchy Level

```
[edit system]
```

Release Information

Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description

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

The remaining statements are explained separately.

Required Privilege Level

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

RELATED DOCUMENTATION

.

level

Syntax

```
level level;
```

Hierarchy Level

```
[edit system fips]
```

Release Information

Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description

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

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

Options

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

Range: 0 through 4

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

Required Privilege Level

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

10

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. You must verify the request by typing **yes** to proceed. This command is restricted to Authorized Administrators (with login class security-admin permissions) because the **maintenance** permission bit is one of the permission bits, along with **secret** and **control**, that distinguishes Authorized Administrators 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

```
authorized-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
re1:
------------------------------------------------------------------------
warning: zeroizing re1
warning: zeroizing re0
...
Rebooting after scrubbing memory...
...
```

Note: The sample output might vary for EX2300 and EX3400 device.