Junos® OS

FIPS Evaluated Configuration Guide for EX4300-48MP Device

Published
2025-02-23

RELEASE
22.4R1-S1

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

Junos® OS FIPS Evaluated Configuration Guide for EX4300-48MP Device
22.4R1-S1

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 This Guide

Use this guide to operate EX4300-48MP device in Federal Information Processing Standards (FIPS) 140-3 Level 1 environment. FIPS 140-3 defines security levels for hardware and software that perform cryptographic functions.

RELATED DOCUMENTATION

- Common Criteria and FIPS Certifications

CHAPTER 1

Overview

IN THIS CHAPTER

Understanding Junos OS in FIPS Mode

IN THIS SECTION

Federal Information Processing Standards (FIPS) 140-3 defines security levels for hardware and software that perform cryptographic functions. This Juniper Networks switches running the Juniper Networks Junos operating system (Junos OS) in *FIPS mode* comply with the FIPS 140-3 Level 1 standard.

Operating switches in a FIPS 140-3 Level 1 environment requires enabling and configuring FIPS mode on the devices from the Junos OS CLI.

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

Supported Platforms

For the features described in this document, the following platforms are supported to qualify NDcPPv2.2e:

- EX4300-48MP (https://www.juniper.net/us/en/products/switches/ex-series/ex4300-multigigabit-enterprise-switch.html)

About the Cryptographic Boundary on Your Device

FIPS 140-3 compliance requires a defined *cryptographic boundary* around each *cryptographic module* on a device. Junos OS in FIPS mode prevents the cryptographic module from executing any software that is not part of the FIPS-certified distribution, and allows only FIPS-approved cryptographic algorithms to be used. No critical security parameters (CSPs), such as passwords and keys, can cross the cryptographic boundary of the module in unencrypted format.

For the Juniper Networks switches that are certified at FIPS-140-3 Level 1, the cryptographic boundary of the module is determined by the chassis type. For a list of FIPS-certified switches and the cryptographic boundary of each switch, see Table 1 on page 3.

Table 1: Cryptographic Boundaries on FIPS-Certified Switches

Switch	Chassis Type	Cryptographic Boundary
EX4300-48MP	Fixed configuration	Switch case

How FIPS Mode Differs from Non-FIPS Mode

Junos OS in FIPS mode differs in the following ways from Junos OS in non-FIPS mode:

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

Validated Version of Junos OS in FIPS Mode

To determine whether a Junos OS release is NIST-validated, see the compliance page on the Juniper Networks Web site (https://apps.juniper.net/compliance/).

RELATED DOCUMENTATION

Identifying Secure Product Delivery | 7

Understanding FIPS Terminology and Supported Cryptographic Algorithms

IN THIS SECTION

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

FIPS Terminology

Critical security parameter (CSP)	Security-related information—for example, secret and private cryptographic keys and authentication data such as passwords and personal identification numbers (PINs)—whose disclosure or modification can compromise the security of a cryptographic module or the information it protects. For details, see "Understanding the Operational Environment for Junos OS in FIPS Mode" on page 16.
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.
FIPS	Federal Information Processing Standards. FIPS 140-3 specifies requirements for security and cryptographic modules. Junos OS in FIPS mode complies with FIPS 140-3 Level 1.
FIPS maintenance role	The role the Crypto Officer assumes to perform physical maintenance or logical maintenance services such as hardware or software diagnostics. For FIPS 140-3 compliance, the Crypto Officer zeroizes the Routing Engine on entry to and exit from the FIPS maintenance role to erase all plain-text secret and private keys and unprotected CSPs.

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

KATs Known answer tests. System self-tests that validate the output of cryptographic algorithms approved for FIPS and test the integrity of some Junos OS modules. For details, see "Understanding FIPS Self-Tests" on page 71.

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

Supported Cryptographic Algorithms

Table 2 on page 6 summarizes the high level protocol algorithm support.

Table 2: Protocols Allowed in FIPS Mode

Protocol	Key Exchange	Authentication	Cipher	Integrity
SSHv2	• ECDH-sha2-nistp256 • ECDH-sha2-nistp384 • ECDH-sha2-nistp521	Host (module): • ECDSA P-256 • SSH-RSA Client (user): • ECDSA P-256 • ECDSA P-384 • ECDSA P-521 • SSH-RSA • RSA-SHA2-256 • RSA-SHA2-512	• AES-CTR-128 • AES-CTR-192 • AES-CTR-256 • AES-CBC-128 • AES-CBC-192 • AES-CBC-256	• HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-512
MACsec MKA	MACsec Key Agreement	Shared secret	• AES-GCM-128 • AES-GCM-256	HMAC-SHA-256

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

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

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

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

ECDSA	Elliptic Curve Digital Signature Algorithm. A variant of the Digital Signature Algorithm (DSA) that uses cryptography based on the algebraic structure of elliptic curves over finite fields. The bit size of the elliptic curve determines the difficulty of decrypting the key. The public key believed to be needed for ECDSA is about twice the size of the security level, in bits.
HMAC	Defined as “Keyed-Hashing for Message Authentication” in RFC 2104, HMAC combines hashing algorithms with cryptographic keys for message authentication.
SHA-256 and SHA-512	Secure hash algorithms (SHA) belonging to the SHA-2 standard defined in FIPS PUB 180-2. Developed by NIST, SHA-256 produces a 256-bit hash digest and SHA-512 produces a 512-bit hash digest.
MACsec MKA	MACsec key aggrement belongs to AES-GCM-128 and AES-GCM-256 as per standard SP800-38D.

RELATED DOCUMENTATION

Understanding FIPS Self-Tests | **71**

Understanding Zeroization to Clear System Data for FIPS Mode | **26**

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.

Understanding Management Interfaces

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

- Local Management Interfaces—The RJ-45 console port on the device is configured as RS-232 data terminal equipment (DTE). You can use the command-line interface (CLI) over this port to configure the device from a terminal.
- Remote Management Protocols—The device can be remotely managed over any Ethernet interface. SSHv2 is the only permitted remote management protocol that can be used in the evaluated

configuration. The remote management protocols J-Web and Telnet are not available for use on the device.

2

CHAPTER

Configuring Administrative Credentials and Privileges

IN THIS CHAPTER

Associated Password Rules for an Authorized Administrator Overview

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.

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: Do not use control characters in passwords.

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

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

```
[ edit ]
crypto-officer@host:fips# set system login password minimum-length 10
```

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

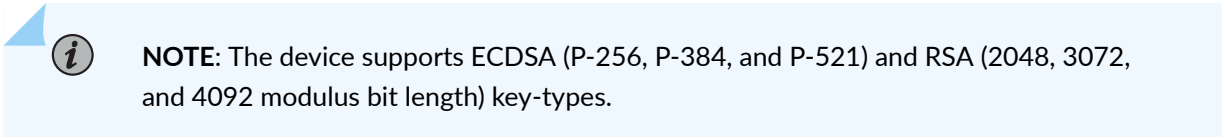
```
[ edit ]
crypto-officer@host:fips# set system login password change-type character-sets
```

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

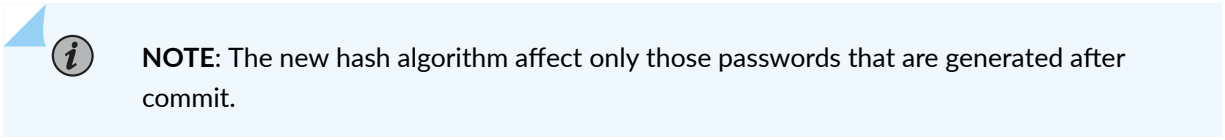
```
[ edit ]
crypto-officer@host:fips# set system login password minimum-changes 3
```

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

```
[ edit ]
crypto-officer@host:fips# set system login password format sha512
```



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



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

Weak passwords are:

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

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

3

CHAPTER

Configuring Roles and Authentication Methods

IN THIS CHAPTER

Understanding Roles and Services for Junos OS

IN THIS SECTION

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 140-3 standard defines two user roles: *Crypto Officer* and *FIPS user*. These roles are defined in terms of Junos OS user capabilities.

All other user types defined for Junos OS in FIPS mode such as read-only and administrative user must fall into one of the two categories: Crypto Officer or FIPS user. For this reason, user authentication in Junos is identity based with role based authorization.

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

Crypto Officer Role and Responsibilities

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

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

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

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

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

FIPS User Role and Responsibilities

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

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

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

What Is Expected of All FIPS Users

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

All FIPS users must:

- Keep all passwords confidential.
- Store devices and documentation in a secure area.
- Deploy devices in secure areas.
- Check audit files periodically.
- Conform to all other FIPS 140-3 security rules.
- Follow these guidelines:
  - Users are trusted.
  - Users abide by all security guidelines.
  - Users do not deliberately compromise security.
  - Users behave responsibly at all times.

RELATED DOCUMENTATION

Zeroizing the System | 27

Configuring Crypto Officer and FIPS User Identification and Access | 30

Understanding the Operational Environment for Junos OS in FIPS Mode

IN THIS SECTION

A Juniper Networks device 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 device in non-FIPS mode:

Hardware Environment for Junos OS in FIPS Mode

Junos OS in FIPS mode establishes a cryptographic boundary in the device that no critical security parameters (CSPs) can cross using plain text. Each hardware component of the device that requires a cryptographic boundary for FIPS 140-3 compliance is a separate cryptographic module.

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

Software Environment for Junos OS in FIPS Mode

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

The Junos OS in FIPS mode software environment is established after the Crypto Officer successfully enables FIPS mode on the device. The Junos OS image that includes FIPS package is available on the Juniper Networks website and can be installed on your device.

For FIPS 140-3 compliance, we recommend that you delete all user-created files and data by (*zeroizing*) the device before enabling FIPS mode.

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

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

Attempts to configure these services, or load configurations with these services configured, result in a configuration syntax error. You can use only SSHv2 as a remote access service.

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

NOTE: Do not attach the device to a network until the Crypto Officer completes 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 device or Routing Engine as a cryptographic module.

Table 3 on page 18 lists CSPs on devices running Junos OS.

Table 3: Critical Security Parameters

CSP	Description	Zeroization Method	Use
SSHv2 private host key	ECDSA / RSA key used to identify the host, generated the first time SSH is configured.	Zeroize command.	Used to identify the host.
SSHv2 session key	Session key used with SSHv2. and as a Diffie-Hellman private key. Encryption: AES-128, AES-192, and AES-256. MACs: HMAC-SHA-1, HMAC-SHA-2-256, and HMAC-SHA2-512. Key exchange: ECDH-sha2-nistp256, ECDH-sha2-nistp384, and ECDH-sha2-nistp521.	Power cycle and terminate session.	Symmetric key used to encrypt data between host and client.
User authentication key	Hash of the user's password: SHA-256, SHA-512.	Zeroize command.	Used to authenticate a user to the cryptographic module.
Crypto Officer authentication key	Hash of the Crypto Officer's password: SHA-256, SHA-512.	Zeroize command.	Used to authenticate the Crypto Officer to the cryptographic module.

Table 3: Critical Security Parameters *(Continued)*

CSP	Description	Zeroization Method	Use
HMAC DRBG seed	Seed for deterministic randon bit generator (DRBG).	Seed is not stored by the cryptographic module.	Used for seeding DRBG.
HMAC DRBG V value	The value (V) of output block length (outlen) in bits, which is updated each time another outlen bits of output are produced.	Power cycle.	A critical value of the internal state of DRBG.
HMAC DRBG key value	The current value of the outlen-bit key, which is updated at least once each time that the DRBG mechanism generates pseudorandom bits.	Power cycle.	A critical value of the internal state of DRBG.
NDRNG entropy	The NDRNG provides 448 bits of entropy collected per NIST SP 800-90B. **NOTE**: The NDRNG provides 448 bits of entropy collected per NIST SP 800-90B from the Junos kernel software entropy source to seed the DRBG. The entropy is conditioned using a vetted conditioning component (SHA-512) and reseeds the DRBG whenever an additional 448 bits of entropy have been collected.	Power cycle.	A critical value of the internal state of DRBG.
MACsec PSK	Input into the device via console port or SSH connection.	Zeroize command.	Credential used for device to device authentication.
MACsec CAK	Entered as a Pre-Shared Key.	Zeroize command.	A secret key possessed by members of a MACSec connectivity association.

Table 3: Critical Security Parameters *(Continued)*

CSP	Description	Zeroization Method	Use
MACsec CKN	Entered as a Pre-Shared Key.	Zeroize command.	Connectivity Key Name: Identifies the CAK.
MACsec SAK	Derived from the CAK using Sp800-108 KDF.	Zeroize command.	Security Association Key. Used for creating SA for encryption / dencryption MACsec traffic. AES GCM (128, 256 bits)
MACsec KEK	Derived from the CAK using Sp800-108 KDF.	Zeroize command.	Used to transmit SAKs to other members of a MACSec connectivity association.
MACsec ICK	Derived from the CAK using Sp800-108 KDF.	Zeroize command.	Used to verify the integrity and authenticity of MPDUs.

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 device over SSH connections because they are encrypted connections.

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

RELATED DOCUMENTATION

Understanding Zeroization to Clear System Data for FIPS Mode | 26

Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode

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

- Length. Passwords must contain between 10 and 20 characters.
- Character set requirements. Passwords must contain at least three of the following five defined character sets:
  - Uppercase letters
  - Lowercase letters
  - Digits
  - Punctuation marks
  - Keyboard characters not included in the other four sets—such as the percent sign (%) and the ampersand (&)
- Authentication requirements. All passwords and keys used to authenticate peers must contain at least 10 characters, and in some cases the number of characters must match the digest size.
- Password encryption. To change the default encryption method (SHA512) include the `format` statement at the [`edit system login password`] hierarchy level.

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

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

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

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

- The hostname of the system (always a first guess).
- Any word or phrase that appears in a dictionary or other well-known source, including dictionaries and thesauruses in languages other than English; works by classical or popular writers; or common words and phrases from sports, sayings, movies or television shows.
- Permutations on any of the above—for example, a dictionary word with letters replaced with digits (**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 | 16

Downloading Software Packages from Juniper Networks

You can download the Junos OS software packages for your device from the Juniper Networks website.

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

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://support.juniper.net/support/downloads/
2. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. Download the software. See Downloading Software.

RELATED DOCUMENTATION

Installing Software on a Device with a Single Routing Engine | 23

Installing Software on a Device with a Single Routing Engine

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

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

1. Download the software package as described in "Downloading Software Packages from Juniper Networks" on page 22.
2. If you have not already done so, connect to the console port on the device from your management device, and log in to the Junos OS CLI.
3. (Optional) Back up the current software configuration to a second storage option. See the *Junos OS Installation and Upgrade Guide* for instructions on performing this task.
4. (Optional) Copy the software package to the device. We recommend that you use FTP to copy the file to the **/var/tmp/** directory.

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

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

   NOTE: If you need to terminate the installation, do not reboot your device; instead, finish the installation and then issue the `request system software delete package.tgz` command, where *package*`.tgz` command. This is your last chance to stop the installation.
6. Reboot the device 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` command to verify that the new version of the software is successfully installed.

```
user@host> show version
Hostname: hostname
Model: ex4300-48mp
Junos: 22.4R1-S1.1
JUNOS OS Kernel 64-bit  [20230120.4e9750f_builder_stable_12_224]
JUNOS OS libs [20230120.4e9750f_builder_stable_12_224]
JUNOS OS runtime [20230120.4e9750f_builder_stable_12_224]
JUNOS OS time zone information [20230120.4e9750f_builder_stable_12_224]
JUNOS OS libs compat32 [20230120.4e9750f_builder_stable_12_224]
JUNOS OS 32-bit compatibility [20230120.4e9750f_builder_stable_12_224]
JUNOS py extensions [20230203.030933_builder_junos_224_r1_s1]
JUNOS py base [20230203.030933_builder_junos_224_r1_s1]
JUNOS OS vmguest [20230120.4e9750f_builder_stable_12_224]
JUNOS OS package [20230117.184352_builder_stable_12]
JUNOS OS crypto [20230120.4e9750f_builder_stable_12_224]
JUNOS OS boot-ve files [20230120.4e9750f_builder_stable_12_224]
JUNOS network stack and utilities [20230203.030933_builder_junos_224_r1_s1]
JUNOS libs [20230203.030933_builder_junos_224_r1_s1]
JUNOS libs compat32 [20230203.030933_builder_junos_224_r1_s1]
JUNOS runtime [20230203.030933_builder_junos_224_r1_s1]
JUNOS na telemetry [22.4R1-S1.1]
JUNOS Web Management Platform Package [20230203.030933_builder_junos_224_r1_s1]
JUNOS qfx modules [20230203.030933_builder_junos_224_r1_s1]
JUNOS qfx runtime [20230203.030933_builder_junos_224_r1_s1]
JUNOS Routing mpls-oam-basic [20230203.030933_builder_junos_224_r1_s1]
JUNOS Routing mpls-oam-advanced [20230203.030933_builder_junos_224_r1_s1]
JUNOS Routing lsys [20230203.030933_builder_junos_224_r1_s1]
JUNOS Routing controller-internal [20230203.030933_builder_junos_224_r1_s1]
JUNOS Routing controller-external [20230203.030933_builder_junos_224_r1_s1]
JUNOS Routing 32-bit Compatible Version [20230203.030933_builder_junos_224_r1_s1]
JUNOS Routing aggregated [20230203.030933_builder_junos_224_r1_s1]
JUNOS probe utility [20230203.030933_builder_junos_224_r1_s1]
JUNOS common platform support [20230203.030933_builder_junos_224_r1_s1]
JUNOS qfx platform support [20230203.030933_builder_junos_224_r1_s1]
JUNOS Openconfig [22.4R1-S1.1]
JUNOS dcp network modules [20230203.030933_builder_junos_224_r1_s1]
JUNOS modules [20230203.030933_builder_junos_224_r1_s1]
JUNOS L2 RSI Scripts [20230203.030933_builder_junos_224_r1_s1]
JUNOS qfx Data Plane Crypto Support [20230203.030933_builder_junos_224_r1_s1]
```

```
JUNOS daemons [20230203.030933_builder_junos_224_r1_s1]
JUNOS qfx daemons [20230203.030933_builder_junos_224_r1_s1]
JUNOS Services URL Filter package [20230203.030933_builder_junos_224_r1_s1]
JUNOS Services TLB Service PIC package [20230203.030933_builder_junos_224_r1_s1]
JUNOS Services Telemetry [20230203.030933_builder_junos_224_r1_s1]
JUNOS Services TCP-LOG [20230203.030933_builder_junos_224_r1_s1]
JUNOS Services SSL [20230203.030933_builder_junos_224_r1_s1]
JUNOS Services SOFTWIRE [20230203.030933_builder_junos_224_r1_s1]
JUNOS Services Stateful Firewall [20230203.030933_builder_junos_224_r1_s1]
JUNOS Services RTCOM [20230203.030933_builder_junos_224_r1_s1]
JUNOS Services RPM [20230203.030933_builder_junos_224_r1_s1]
JUNOS Services PCEF package [20230203.030933_builder_junos_224_r1_s1]
JUNOS Services NAT [20230203.030933_builder_junos_224_r1_s1]
JUNOS Services Mobile Subscriber Service Container package
[20230203.030933_builder_junos_224_r1_s1]
JUNOS Services MobileNext Software package [20230203.030933_builder_junos_224_r1_s1]
JUNOS Services Logging Report Framework package [20230203.030933_builder_junos_224_r1_s1]
JUNOS Services LL-PDF Container package [20230203.030933_builder_junos_224_r1_s1]
JUNOS Services Jflow Container package [20230203.030933_builder_junos_224_r1_s1]
JUNOS Services Deep Packet Inspection package [20230203.030933_builder_junos_224_r1_s1]
JUNOS Services IPSec [20230203.030933_builder_junos_224_r1_s1]
JUNOS Services IDS [20230203.030933_builder_junos_224_r1_s1]
JUNOS IDP Services [20230203.030933_builder_junos_224_r1_s1]
JUNOS Services HTTP Content Management package [20230203.030933_builder_junos_224_r1_s1]
JUNOS Services DNS Filter package (i386) [20230203.030933_builder_junos_224_r1_s1]
JUNOS Services Crypto [20230203.030933_builder_junos_224_r1_s1]
JUNOS Services Captive Portal and Content Delivery Container package
[20230203.030933_builder_junos_224_r1_s1]
JUNOS Services COS [20230203.030933_builder_junos_224_r1_s1]
JUNOS AppId Services [20230203.030933_builder_junos_224_r1_s1]
JUNOS Services Application Level Gateways [20230203.030933_builder_junos_224_r1_s1]
JUNOS Services AACL Container package [20230203.030933_builder_junos_224_r1_s1]
JUNOS SDN Software Suite [20230203.030933_builder_junos_224_r1_s1]
JUNOS Extension Toolkit [20230203.030933_builder_junos_224_r1_s1]
JUNOS Phone-home [20230203.030933_builder_junos_224_r1_s1]
JUNOS Packet Forwarding Engine Support (DC-PFE) [20230203.030933_builder_junos_224_r1_s1]
JUNOS Packet Forwarding Engine Support (M/T Common) [20230203.030933_builder_junos_224_r1_s1]
JUNOS Juniper Malware Removal Tool (JMRT) [1.0.0+20230203.030933_builder_junos_224_r1_s1]
JUNOS J-Insight [20230203.030933_builder_junos_224_r1_s1]
JUNOS jfirmware [20221102.183251_builder_junos_224_r1]
JUNOS Online Documentation [20230203.030933_builder_junos_224_r1_s1]
JUNOS jail runtime [20230120.4e9750f_builder_stable_12_224]
JUNOS FIPS mode utilities [20230203.030933_builder_junos_224_r1_s1]
```

```
JUNOS dsa [20230203.030933_builder_junos_224_r1_s1]
Junos host: 22.4R1-S1.1
JUNOS Host kernel-release [3.14.52-rt50-WR7.0.0.9_ovp]
JUNOS Host kernel-version [#1 SMP Wed Nov 2 04:59:59 PDT 2022]
JUNOS Host ex-4300mp platform package [22.4R1-S1.1]
JUNOS Host ex-4300mp control-plane package [22.4R1-S1.1]
JUNOS Host ex-4300mp base package [22.4R1-S1.1]
JUNOS Host ex-4300mp data-plane package [22.4R1-S1.1]
```

Understanding Zeroization to Clear System Data for FIPS Mode

IN THIS SECTION

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

The Crypto Officer initiates the zeroization process by entering the **request system zeroize** operational command from the CLI. Use of this command is restricted to the Crypto Officer.

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

For FIPS 140-3 compliance, you must zeroize the system to remove sensitive information before disabling FIPS mode on the device.

When to Zeroize?

As Crypto Officer, perform zeroization in the following situations:

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

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

RELATED DOCUMENTATION

Enabling FIPS Mode | 28

Zeroizing the System

To zeroize your device:

1. Login to the device as Crypto Officer and from the CLI, enter

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

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

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

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

RELATED DOCUMENTATION

Enabling FIPS Mode | 28

Understanding Zeroization to Clear System Data for FIPS Mode | 26

Enabling FIPS Mode

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

As Crypto Officer, you must explicitly enable FIPS mode on the switch by setting the FIPS level to 1 (one), the FIPS 140-3 level at which your devices 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-256 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. Zeroize the switch to delete all CSPs before entering FIPS mode.
2. After the device comes up in Amnesiac mode, login using console with username *root* and password (*blank*).

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

```
root@switch> edit
Entering configuration mode

[edit]root@switch# set system root-authentication plain-text-password
New password:
Retype new password:
root@switch# commit
configuration check succeeds commit complete
```

4. Load configurationon to switch and commit new configuration.
5. Configure Crypto Officer and login with Crypto Officer credentials.
6. The `fips-mode.tgz` is an optional package needed for enabling FIPS. This package is part of Junos OS software. To enable this package, use below command:

```
root@host>request system software add optional://fips-mode.tgz
Verified fips-mode signed by PackageProductionECP256_2022 method ECDSA256+SHA256
```

7. Configure system boundary fips by setting the `set system fips level 1` command followed by the `commit` command.

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

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

8. After deleting and reconfiguring the CSPs, commit is successful and the switch needs reboot to enter FIPS mode.

```
crypto-officer@switch# commit
configuration check succeeds
[edit]
  'system'
    warning: reboot is required to transition to FIPS level 1
commit complete
```

```
[edit]
crypto-officer@switch# run request system reboot
```

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

```
crypto-officer@switch:fips>
```

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

Configuring Crypto Officer and FIPS User Identification and Access

IN THIS SECTION

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

Configuring Crypto Officer Login Access

Junos OS in FIPS mode offers a finer granularity of user permissions than those mandated by FIPS 140-3.

For FIPS 140-3 compliance, any FIPS user with the **secret**, **security**, **maintenance**, and **control** permission bits set is a Crypto Officer. In most cases the **super-user** class suffices for the Crypto Officer.

To configure login access for a Crypto Officer:

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

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

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

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

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

3. Following the guidelines in "Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode" on page 21, assign the Crypto Officer a plain-text password for login authentication. Set the password by typing a password after the prompts `New password` and `Retype new password`.

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

4. Optionally, display the configuration:

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

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

```
[edit]
root@switch# commit
commit completeroot@switch# exit
root@switch> exit
```

Configuring FIPS User Login Access

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

As the Crypto Officer you set up FIPS users.

To configure login access for a FIPS user:

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

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

2. Give the user a username, assign the FIPS user a user ID (for example, **6401**, which must be unique number associated with the login account in the range of 1 through 64000) and a class (for example , read-only).

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

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

3. Following the guidelines in "Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode" on page 21, assign the FIPS a plain-text password for login authentication. Set the password by typing a password after the prompts `New password` and `Retype new password`.

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

4. Optionally, display the configuration:

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

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

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

RELATED DOCUMENTATION

Understanding Roles and Services for Junos OS | 14

4

CHAPTER

Configuring SSH and Console Connection

IN THIS CHAPTER

Configure 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.

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

To configure SSH on the DUT:

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

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

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

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

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

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

4. Specify the ciphers allowed for protocol version 2.

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

Supported SSH hostkey algorithm:

```
ssh-ecdsa            Allow generation of ECDSA host-key
ssh-rsa              Allow generation of RSA host-key
```

Supported SSH key-exchange algorithm:

```
ecdh-sha2-nistp256   The EC Diffie-Hellman on nistp256 with SHA2-256
ecdh-sha2-nistp384   The EC Diffie-Hellman on nistp384 with SHA2-384
ecdh-sha2-nistp521   The EC Diffie-Hellman on nistp521 with SHA2-512
```

Supported MAC algorithm:

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

Supported SSH ciphers algorithm:

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

5

CHAPTER

Configuring MACsec

IN THIS CHAPTER

Overview of Media Access Control Security (MACsec) in FIPS mode

Media Access Control Security (MACsec) is an 802.1AE IEEE industry-standard security technology that provides secure communication for all traffic on Ethernet links. MACsec provides point-to-point security on Ethernet links between directly connected nodes and is capable of identifying and preventing most security threats, including denial of service, intrusion, man-in-the-middle, masquerading, passive wiretapping, and playback attacks.

MACsec allows you to secure point to point Ethernet link for almost all traffic, including frames from the Link Layer Discovery Protocol (LLDP), Link Aggregation Control Protocol (LACP), Dynamic Host Configuration Protocol (DHCP), Address Resolution Protocol (ARP), and other protocols that are not typically secured on an Ethernet link because of limitations with other security solutions. MACsec can be used in combination with other security protocols such as IP Security (IPsec) and Secure Sockets Layer (SSL) to provide end-to-end network security.

MACsec is standardized in IEEE 802.1AE. The IEEE 802.1AE standard can be seen on the IEEE organization website at IEEE 802.1: BRIDGING & MANAGEMENT.

Each implementation of an algorithm is checked by a series of known answer test (KAT) self-tests and crypto algorithms validations (CAV). The following cryptographic algorithms are added specifically for MACsec.

- Advanced Encryption Standard (AES)-Cipher Message Authentication Code (CMAC)
- Advanced Encryption Standard (AES) Key Wrap

Pre-shared key configurations for both connectivity association key name (CKN) and connectivity association key (CAK):

```
crypto-officer@hostname:fips# prompt security macsec connectivity-association connectivity-
association-name pre-shared-key cak
New cak (secret):
Retype new cak (secret):
```

```
crypto-officer@hostname:fips#  set security macsec connectivity-association ca_name pre-shared-
key ckn ckn
```

NOTE: In the above `set security macsec connectivity-association` *`ca_name`* `pre-shared-key ckn` *`ckn`* command, you need to define a user defined name for the *ca_name* variable option and a user defined connectivity association key name in hexadecimal format for *ckn* variable option.

A pre-shared key is exchanged between directly-connected links to establish a MACsec-secure link. The pre-shared-key includes the CKN and the CAK. The CKN and CAK must match on both ends of a link to create a MACsec-secured link.

If you configure 128 bit cipher suite, then CAK can be 32 digit hexadecimal number. If you configure 256 bit cipher suite, then CAK can be 64 digit hexadecimal number.

NOTE: To maximize security, we recommend you to configure all 64 digits of a CKN and all 32 digits of a CAK. If you do not configure all 64 digits of a CKN or all 32 digits of a CAK, the system auto-configures all the remaining digits to 0. However, you will receive a warning message when you commit the configuration.

After the successful exchange and verification of the pre-shared keys by both ends of the link, the MACsec Key Agreement (MKA) protocol enables and manages the secure link. The MKA protocol then elects one of the two directly-connected devices as the key server. The key server then shares a random security with the other device over the MACsec-secure point-to-point link. The key server continues to periodically create and share a random security key with the other device over the MACsec-secured point-to-point link as long as MACsec is enabled.

For example, ypu can configure a CKN of `37c9c2c45ddd012aa5bc8ef284aa23ff6729ee2e4acb66e91fe34ba2cd9fe311` and CAK of `228ef255aa23ff6729ee664acb66e91f` on connectivity association.

RELATED DOCUMENTATION

- Understanding Media Access Control Security (MACsec)

Configure MACsec

IN THIS SECTION

We can configure MACsec to secure point-to-point Ethernet links connecting your device with MACsec-capable MICs. Each point-to-point Ethernet link that you want to secure using MACsec must be configured independently. We can enable MACsec on device-to-device links using static connectivity association key (CAK) security mode.

You can configure different interface rates such as 40G, 100G, and 10G in port mode and specific interface rates such as 100G, 40G, and 10G in pic mode. In pic mode you can configure only one type of interface speed.

Customizing Time

To customize time, disable NTP and set the date.

1. Disable NTP.

```
[edit]
security-administrator@hostname:fips# deactivate groups global system ntp
security-administrator@hostname:fips# deactivate system ntp
security-administrator@hostname:fips# commit
security-administrator@hostname:fips# exit
```

2. Setting date and time. Date and time format is YYYYMMDDHHMM.ss

```
security-administrator@hostname:fips> set date 201803202034.00
security-administrator@hostname:fips> set cli timestamp
```

NOTE: We are not claiming NTP as part of FPT_STM_EXT.1 SFR. However, in our configuration guide we have leveraged activate/deactivate NTP services to validate MACsec tolerance and MACsec key-chain.

Configuring MACsec on a Device Running Junos OS

To configure MACsec on a device running Junos OS:

1. Configure the MACsec security mode as for the connectivity association.

```
[edit]
security-administrator@hostname:fips#  set security macsec connectivity-association
connectivity-association-name exclude-protocol protocol-name
security-administrator@hostname:fips#  set security macsec connectivity-association
connectivity-association-name include-sci
security-administrator@hostname:fips#  set security macsec connectivity-association
connectivity-association-name mka key-server-priority priority-number
security-administrator@hostname:fips#  set security macsec connectivity-association
connectivity-association-name mka transmit-interval interval
security-administrator@hostname:fips#  set security macsec connectivity-association
connectivity-association-name offset offset-number
```

NOTE: Based on your requirement you can configure the *offset-number* at the `set security macsec connectivity-association` *`connectivity-association-name`* `offset` hierarchy level to `0`, `30`, or `50`.

2. Create the pre-shared key by configuring the connectivity association key name (CKN) and connectivity association key (CAK).

```
[edit]
security-administrator@hostname:fips# prompt security macsec connectivity-association
```

```
connectivity-association-name pre-shared-key cak
New cak (secret):
Retype new cak (secret):
security-administrator@hostname:fips# set security macsec connectivity-association
connectivity-association-name pre-shared-key ckn hexadecimal-number
security-administrator@hostname:fips# set security macsec connectivity-association
connectivity-association-name replay-protect replay-window-size number-of-packets
```

NOTE: Based on your requirement you can configure the *number-of-packets* value at the `set security macsec connectivity-association connectivity-association-name replay-protect replay-window-size` hierarchy level from `0` through `65535`.

3. Set the MKA to security mode.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1
security-mode static-cak
```

NOTE: `CA1` is an example of *connectivity-association-name* configured.

4. Assign the configured connectivity association with a specified MACsec interface.

```
[edit]
security-administrator@hostname:fips# set security macsec interfaces interface-name
connectivity-association connectivity-association-name
```

Configuring Static MACsec with Layer 3 Traffic

To configure Static MACsec using ICMP traffic between device R0 and device R1:

In R0:

1. Create the preshared key by configuring the connectivity association key name (CKN) and connectivity association key (CAK)

```
[edit]
security-administrator@hostname:fips#  set security macsec connectivity-association CA1 pre-shared-key ckn 2345678922334455667788992223333444555666777888999222233334444555 5
security-administrator@hostname:fips#  prompt security macsec connectivity-association CA1 pre-shared-key cak
New cak (secret):
Retype new cak (secret):
security-administrator@hostname:fips#  set security macsec connectivity-association CA1 offset 30
```

2. Set the trace option values.

```
[edit]
security-administrator@hostname:fips# set security macsec traceoptions file MACsec.log
security-administrator@hostname:fips# set security macsec traceoptions file size 4000000000
security-administrator@hostname:fips# set security macsec traceoptions flag all
```

3. Assign the trace to an interface.

```
[edit]
security-administrator@hostname:fips# set security macsec interfaces interface-name traceoptions file mka_xe size 1g
security-administrator@hostname:fips# set security macsec interfaces interface-name traceoptions flag all
```

4. Configure the MACsec security mode as static-cak for the connectivity association.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1 security-mode static-cak
```

5. Set the MKA key server priority.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1 mka key-server-priority 1
```

6. Set the MKA transmit interval.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1 mka
transmit-interval 3000
```

7. Enable the MKA secure.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1
include-sci
```

8. Assign the connectivity association to an interface.

```
[edit]
security-administrator@hostname:fips# set security macsec interfaces interface-name
connectivity-association CA1
security-administrator@hostname:fips# set interfaces interface-name unit 0 family inet
address 10.1.1.1/24
```

In R1:

1. Create the preshared key by configuring the connectivity association key name (CKN) and connectivity association key (CAK)

```
[edit]
security-administrator@hostname:fips#  set security macsec connectivity-association CA1 pre-
shared-key ckn 2345678922334455667788992222333444555666777888999222233334444555 5
security-administrator@hostname:fips#  prompt security macsec connectivity-association CA1
pre-shared-key cak
New cak (secret):
Retype new cak (secret):
security-administrator@hostname:fips#  set security macsec connectivity-association CA1
offset 30
```

2. Set the trace option values.

```
[edit]
security-administrator@hostname:fips# set security macsec traceoptions file MACsec.log
```

```
security-administrator@hostname:fips# set security macsec traceoptions file size 4000000000
security-administrator@hostname:fips# set security macsec traceoptions flag all
```

3. Assign the trace to an interface.

```
[edit]
security-administrator@hostname:fips# set security macsec interfaces interface-name
traceoptions file mka_xe size 1g
security-administrator@hostname:fips# set security macsec interfaces interface-name
traceoptions flag all
```

4. Configure the MACsec security mode as static-cak for the connectivity association.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1
security-mode static-cak
```

5. Set the MKA transmit interval.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1 mka
transmit-interval 3000
```

6. Enable the MKA secure.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1
include-sci
```

7. Assign the connectivity association to an interface.

```
[edit]
security-administrator@hostname:fips# set security macsec interfaces interface-name
connectivity-association CA1
security-administrator@hostname:fips# set interfaces interface-name unit 0 family inet
address 10.1.1.2/24
```

Configuring MACsec with keychain using Layer 3 Traffic

Synchronize both macsec endpoint devices to NTP as both device's time should be the same for key start time triggers. To configure MACsec with keychain using ICMP traffic between device R0 and device R1:

In R0:

1. Assign a tolerance value to the authentication key chain.

```
[edit]
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 tolerance 20
```

2. Create the secret password to use. It is a string of hexadecimal digits up to 64 characters long. The password can include spaces if the character string is enclosed in quotation marks. The keychain's secret-data is used as a CAK.

   You can configure upto 64 keys. For example, you can refer the following 4 keys:

```
[edit]
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 0 key-name 2345678922334455667788992223334445556667778889992222333344445551
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 0 start-time 2018-03-20.20:35
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 1 key-name 2345678922334455667788992223334445556667778889992222333344445552
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 1 start-time 2018-03-20.20:37
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 2 key-name 2345678922334455667788992223334445556667778889992222333344445553
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 2 start-time 2018-03-20.20:39
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 3 key-name 2345678922334455667788992223334445556667778889992222333344445554
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 3 start-time 2018-03-20.20:41
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 4 key-name 2345678922334455667788992223334445556667778889992222333344445555
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 4 start-time 2018-03-20.20:43
```

Use the `prompt` command to enter a secret key value. For example, the secret key value is *23456789223344556677889922233341234567892233445566778899222333412345678922334455667788992223334*.

You can configure upto 64 secret keys. For example, you can refer the following 4 secret keys:

```
[edit]
security-administrator@hostname:fips#  prompt security authentication-key-chains key-chain
macsec-kc1 key 0 secret
New cak (secret):
Retype new cak (secret):
security-administrator@hostname:fips#  prompt security authentication-key-chains key-chain
macsec-kc1 key 1 secret
New cak (secret):
Retype new cak (secret):
security-administrator@hostname:fips#  prompt security authentication-key-chains key-chain
macsec-kc1 key 2 secret
New cak (secret):
Retype new cak (secret):
security-administrator@hostname:fips#  prompt security authentication-key-chains key-chain
macsec-kc1 key 3 secret
New cak (secret):
Retype new cak (secret):
security-administrator@hostname:fips#  prompt security authentication-key-chains key-chain
macsec-kc1 key 4 secret
New cak (secret):
Retype new cak (secret):
```

3. Associate the preshared keychain name with the connectivity association.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1 pre-
shared-key-chain macsec-kc1
security-administrator@hostname:fips# set security macsec connectivity-association CA1
offset 50
security-administrator@hostname:fips# set security macsec connectivity-association CA1
cipher-suite gcm-aes-256
```

NOTE: The cipher value can also be set as **cipher-suite gcm-aes-128**.

4. Set the trace option values.

```
[edit]
security-administrator@hostname:fips# set security macsec traceoptions file MACsec.log
security-administrator@hostname:fips# set security macsec traceoptions file size 4000000000
security-administrator@hostname:fips# set security macsec traceoptions flag all
```

5. Assign the trace to an interface.

```
[edit]
security-administrator@hostname:fips# set security macsec interfaces interface-name
traceoptions file mka_xe size 1g
security-administrator@hostname:fips# set security macsec interfaces interface-name
traceoptions flag all
```

6. Configure the MACsec security mode as static-cak for the connectivity association.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1
security-mode static-cak
```

7. Set the MKA key server priority.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1 mka
key-server-priority 1
```

8. Set the MKA transmit interval.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1 mka
transmit-interval 3000
```

9. Enable the MKA secure.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1
include-sci
```

10. Assign the connectivity association to an interface.

```
[edit]
security-administrator@hostname:fips# set security macsec interfaces interface-name
connectivity-association CA1
security-administrator@hostname:fips# set interfaces interface-name unit 0 family inet
address 10.1.1.1/24
```

To configure MACsec with keychain for Layer 3 Traffic:

In R1:

1. Assign a tolerance value to the authentication key chain.

```
[edit]
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 tolerance 20
```

2. Create the secret password to use. It is a string of hexadecimal digits up to 64 characters long. The password can include spaces if the character string is enclosed in quotation marks. The keychain's secret-data is used as a CAK.

   You can configure upto 64 keys. For example, you can refer the following 4 keys:

```
[edit]
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 0 key-name 2345678922334455667788992223334445556667778889992222333344445551
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 0 start-time 2018-03-20.20:35
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 1 key-name 2345678922334455667788992223334445556667778889992222333344445552
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 1 start-time 2018-03-20.20:37
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 2 key-name 2345678922334455667788992223334445556667778889992222333344445553
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 2 start-time 2018-03-20.20:39
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 3 key-name 2345678922334455667788992223334445556667778889992222333344445554
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 3 start-time 2018-03-20.20:41
```

```
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 4 key-name 2345678922334455667788992223334445556667778889992222333344445555
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 4 start-time 2018-03-20.20:43
```

Use the `prompt` command to enter a secret key value. For example, the secret key value is *2345678922334455667788992223334123456789223344556677889922233341*.

You can configure upto 64 secret keys. For example, you can refer the following 4 secret keys:

```
[edit]
security-administrator@hostname:fips#  prompt security authentication-key-chains key-chain
macsec-kc1 key 0 secret
New cak (secret):
Retype new cak (secret):
security-administrator@hostname:fips#  prompt security authentication-key-chains key-chain
macsec-kc1 key 1 secret
New cak (secret):
Retype new cak (secret):
security-administrator@hostname:fips#  prompt security authentication-key-chains key-chain
macsec-kc1 key 2 secret
New cak (secret):
Retype new cak (secret):
security-administrator@hostname:fips#  prompt security authentication-key-chains key-chain
macsec-kc1 key 3 secret
New cak (secret):
Retype new cak (secret):
security-administrator@hostname:fips#  prompt security authentication-key-chains key-chain
macsec-kc1 key 4 secret
New cak (secret):
Retype new cak (secret):
```

3. Associate the preshared keychain name with the connectivity association.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1 pre-
shared-key-chain macsec-kc1
security-administrator@hostname:fips# set security macsec connectivity-association CA1
offset 50
security-administrator@hostname:fips# set security macsec connectivity-association CA1
cipher-suite gcm-aes-256
```

4. **NOTE**:

   - You can use the non-XPN ciphers `AES-GCM-128` and `AES-GCM-256` for 10G/xe interfaces macsec configuration only.
   - You can use the XPN ciphers `AES-GCM-XPN-128` and `AES-GCM-XPN-256` for 40G and 100G rates macsec configuration. You can also use the XPN ciphers `AES-GCM-XPN-128` and `AES-GCM-XPN-256` for 10G/xe interfaces macsec configuration, if it supports.

5. Set the trace option values.

```
[edit]
security-administrator@hostname:fips# set security macsec traceoptions file MACsec.log
security-administrator@hostname:fips# set security macsec traceoptions file size 4000000000
security-administrator@hostname:fips# set security macsec traceoptions flag all
```

6. Assign the trace to an interface.

```
[edit]
security-administrator@hostname:fips# set security macsec interfaces interface-name
traceoptions file mka_xe size 1g
security-administrator@hostname:fips# set security macsec interfaces interface-name
traceoptions flag all
```

7. Configure the MACsec security mode as static-cak for the connectivity association.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1
security-mode static-cak
```

8. Set the MKA key server priority.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1 mka
key-server-priority 1
```

9. Set the MKA transmit interval.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1 mka
transmit-interval 3000
```

10. Enable the MKA secure.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1
include-sci
```

11. Assign the connectivity association to an interface.

```
[edit]
security-administrator@hostname:fips# set security macsec interfaces interface-name
connectivity-association CA1
security-administrator@hostname:fips# set interfaces interface-name unit 0 family inet
address 10.1.1.2/24
```

Configuring Static MACsec for Layer 2 Traffic

To configure static MACsec for Layer 2 traffic between device R0 and device R1:

In R0:

1. Set the MKA key server priority.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1 mka
key-server-priority 1
```

2. Create the secret password to use. It is a string of hexadecimal digits up to 64 characters long. The password can include spaces if the character string is enclosed in quotation marks. The keychain's secret-data is used as a CAK.

```
[edit]
security-administrator@hostname:fips# prompt security authentication-key-chains key-chain
macsec-kc1 key 0 secret
New cak (secret):
Retype new cak (secret):
```

For example, the secret key value is *2345678922334455667788992222333412345678922334455667788992222333 41*.

3. Associate the preshared keychain name with the connectivity association.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1 pre-
shared-key-chain macsec-kc1
security-administrator@hostname:fips# set security macsec connectivity-association CA1
offset 50
security-administrator@hostname:fips# set security macsec connectivity-association CA1
cipher-suite gcm-aes-256
```

4. Set the trace option values.

```
[edit]
security-administrator@hostname:fips# set security macsec traceoptions file MACsec.log
security-administrator@hostname:fips# set security macsec traceoptions file size 4000000000
security-administrator@hostname:fips# set security macsec traceoptions flag all
```

5. Assign the trace to an interface.

```
[edit]
security-administrator@hostname:fips# set security macsec interfaces interface-name
traceoptions file mka_xe size 1g
security-administrator@hostname:fips# set security macsec interfaces interface-name
traceoptions flag all
```

6. Configure the MACsec security mode as static-cak for the connectivity association.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1
security-mode static-cak
```

7. Set the MKA key server priority.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1 mka
key-server-priority 1
```

8. Set the MKA transmit interval.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1 mka
transmit-interval 3000
```

9. Enable the MKA secure.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1
include-sci
```

10. Assign the connectivity association to an interface.

```
[edit]
security-administrator@hostname:fips# set security macsec interfaces interface-name
connectivity-association CA1
```

11. Configure VLAN tagging.

```
[edit]
security-administrator@hostname:fips# set interfaces interface-name1 flexible-vlan-tagging
security-administrator@hostname:fips# set interfaces interface-name1 encapsulation
flexibleethernet-services
security-administrator@hostname:fips# set interfaces interface-name1 unit unit-number
family ethernet-switching interface-mode trunk
security-administrator@hostname:fips# set interfaces interface-name1 unit unit-number
```

```
family ethernet-switching vlan members vlan-number-name
security-administrator@hostname:fips# set vlans vlan-number-name vlan-id vlan-number
```

In R1:

1. Create the secret password to use. It is a string of hexadecimal digits up to 64 characters long. The password can include spaces if the character string is enclosed in quotation marks. The keychain's secret-data is used as a CAK.

   ```
   [edit]
   security-administrator@hostname:fips#  prompt security authentication-key-chains key-chain
   macsec-kc1 key 0 secret
   New cak (secret):
   Retype new cak (secret):
   ```

   For example, the secret key value is 2345678922334455667788992223334123456789223344556677889922233341.

2. Associate the preshared keychain name with the connectivity association.

   ```
   [edit]
   security-administrator@hostname:fips# set security macsec connectivity-association CA1 pre-
   shared-key-chain macsec-kc1
   security-administrator@hostname:fips# set security macsec connectivity-association CA1
   offset 50
   security-administrator@hostname:fips# set security macsec connectivity-association CA1
   cipher-suite gcm-aes-256
   ```

3. Set the trace option values.

   ```
   [edit]
   security-administrator@hostname:fips# set security macsec traceoptions file MACsec.log
   security-administrator@hostname:fips# set security macsec traceoptions file size 4000000000
   security-administrator@hostname:fips# set security macsec traceoptions flag all
   ```

4. Assign the trace to an interface.

   ```
   [edit]
   security-administrator@hostname:fips# set security macsec interfaces interface-name
   traceoptions file mka_xe size 1g
   ```

```
security-administrator@hostname:fips# set security macsec interfaces interface-name
traceoptions flag all
```

5. Configure the MACsec security mode as static-cak for the connectivity association.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1
security-mode static-cak
```

6. Set the MKA key server priority.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1 mka
key-server-priority 1
```

7. Set the MKA transmit interval.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1 mka
transmit-interval 3000
```

8. Enable the MKA secure.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1
include-sci
```

9. Assign the connectivity association to an interface.

```
[edit]
security-administrator@hostname:fips# set security macsec interfaces interface-name
connectivity-association CA1
```

10. Configure VLAN tagging.

```
[edit]
security-administrator@hostname:fips# set interfaces interface-name1 flexible-vlan-tagging
```

```
security-administrator@hostname:fips# set interfaces interface-name1 encapsulation
flexibleethernet-services
security-administrator@hostname:fips# set interfaces interface-name1 unit unit-number
family ethernet-switching interface-mode trunk
security-administrator@hostname:fips# set interfaces interface-name1 unit unit-number
family ethernet-switching vlan members vlan-number-name
security-administrator@hostname:fips# set vlans vlan-number-name vlan-id vlan-number
```

Configuring MACsec with keychain for Layer 2 Traffic

Synchronize both macsec endpoint devices to NTP as both device's time should be the same for key start time triggers. To configure MACsec with keychain for ICMP traffic between device R0 and device R1:

In R0:

1. Assign a tolerance value to the authentication key chain.

```
[edit]
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 tolerance 20
```

2. Create the secret password to use. It is a string of hexadecimal digits up to 64 characters long. The password can include spaces if the character string is enclosed in quotation marks. The keychain's secret-data is used as a CAK.

   You can configure upto 64 keys. For example, you can refer the following 4 keys:

```
[edit]
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 0 key-name 2345678922334455667788992223334445556667778889992222333344445551
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 0 start-time 2018-03-20.20:35
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 1 key-name 2345678922334455667788992223334445556667778889992222333344445552
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 1 start-time 2018-03-20.20:37
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 2 key-name 2345678922334455667788992223334445556667778889992222333344445553
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
```

```
macsec-kc1 key 2 start-time 2018-03-20.20:39
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 3 key-name 2345678922334455667788992223334445556667778889992222333344445554
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 3 start-time 2018-03-20.20:41
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 4 key-name 2345678922334455667788992223334445556667778889992222333344445555
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 4 start-time 2018-03-20.20:43
```

Use the `prompt` command to enter a secret key value. For example, the secret key value is *2345678922334455667788992223334123456789223344556677889922233341*.

You can configure upto 64 secret keys. For example, you can refer the following 4 secret keys:

```
[edit]
security-administrator@hostname:fips#  prompt security authentication-key-chains key-chain
macsec-kc1 key 0 secret
New cak (secret):
Retype new cak (secret):
security-administrator@hostname:fips#  prompt security authentication-key-chains key-chain
macsec-kc1 key 1 secret
New cak (secret):
Retype new cak (secret):
security-administrator@hostname:fips#  prompt security authentication-key-chains key-chain
macsec-kc1 key 2 secret
New cak (secret):
Retype new cak (secret):
security-administrator@hostname:fips#  prompt security authentication-key-chains key-chain
macsec-kc1 key 3 secret
New cak (secret):
Retype new cak (secret):
security-administrator@hostname:fips#  prompt security authentication-key-chains key-chain
macsec-kc1 key 4 secret
New cak (secret):
Retype new cak (secret):
```

3. Associate the preshared keychain name with the connectivity association.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1 pre-
shared-key-chain macsec-kc1
```

```
security-administrator@hostname:fips# set security macsec connectivity-association CA1
cipher-suite gcm-aes-256
```

4. Set the trace option values.

```
[edit]
security-administrator@hostname:fips# set security macsec traceoptions file MACsec.log
security-administrator@hostname:fips# set security macsec traceoptions file size 4000000000
security-administrator@hostname:fips# set security macsec traceoptions flag all
```

5. Assign the trace to an interface.

```
[edit]
security-administrator@hostname:fips# set security macsec interfaces interface-name
traceoptions file mka_xe size 1g
security-administrator@hostname:fips# set security macsec interfaces interface-name
traceoptions flag all
```

6. Configure the MACsec security mode as static-cak for the connectivity association.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1
security-mode static-cak
```

7. Set the MKA key server priority.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1 mka
key-server-priority 1
```

8. Set the MKA transmit interval.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1 mka
transmit-interval 3000
```

9. Enable the MKA secure.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1
include-sci
```

10. Assign the connectivity association to an interface.

```
[edit]
security-administrator@hostname:fips# set security macsec interfaces interface-name
connectivity-association CA1
```

11. Configure VLAN tagging.

```
[edit]
security-administrator@hostname:fips# set interfaces interface-name1 flexible-vlan-tagging
security-administrator@hostname:fips# set interfaces interface-name1 encapsulation
flexibleethernet-services
security-administrator@hostname:fips# set interfaces interface-name1 unit unit-number
family ethernet-switching interface-mode trunk
security-administrator@hostname:fips# set interfaces interface-name1 unit unit-number
family ethernet-switching vlan members vlan-number-name
security-administrator@hostname:fips# set vlans vlan-number-name vlan-id vlan-number
```

In R1:

1. Assign a tolerance value to the authentication key chain.

```
[edit]
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 tolerance 20
```

2. Create the secret password to use. It is a string of hexadecimal digits up to 64 characters long. The password can include spaces if the character string is enclosed in quotation marks. The keychain's secret-data is used as a CAK.

   You can configure upto 64 keys. For example, you can refer the following 4 keys:

```
[edit]
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
```

```
macsec-kc1 key 0 key-name 2345678922334455667788992223334445556667778889992222333344445551
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 0 start-time 2018-03-20.20:35
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 1 key-name 2345678922334455667788992223334445556667778889992222333344445552
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 1 start-time 2018-03-20.20:37
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 2 key-name 2345678922334455667788992223334445556667778889992222333344445553
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 2 start-time 2018-03-20.20:39
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 3 key-name 2345678922334455667788992223334445556667778889992222333344445554
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 3 start-time 2018-03-20.20:41
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 4 key-name 2345678922334455667788992223334445556667778889992222333344445555
security-administrator@hostname:fips#  set security authentication-key-chains key-chain
macsec-kc1 key 4 start-time 2018-03-20.20:43
```

Use the `prompt` command to enter a secret key value. For example, the secret key value is *2345678922334455667788992223334123456789223344556677889922233341*.

You can configure upto 64 secret keys. For example, you can refer the following 4 secret keys:

```
[edit]
security-administrator@hostname:fips#  prompt security authentication-key-chains key-chain
macsec-kc1 key 0 secret
New cak (secret):
Retype new cak (secret):
security-administrator@hostname:fips#  prompt security authentication-key-chains key-chain
macsec-kc1 key 1 secret
New cak (secret):
Retype new cak (secret):
security-administrator@hostname:fips#  prompt security authentication-key-chains key-chain
macsec-kc1 key 2 secret
New cak (secret):
Retype new cak (secret):
security-administrator@hostname:fips#  prompt security authentication-key-chains key-chain
macsec-kc1 key 3 secret
New cak (secret):
Retype new cak (secret):
```

```
security-administrator@hostname:fips#  prompt security authentication-key-chains key-chain
macsec-kc1 key 4 secret
New cak (secret):
Retype new cak (secret):
```

3. Associate the preshared keychain name with the connectivity association.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1 pre-
shared-key-chain macsec-kc1
security-administrator@hostname:fips# set security macsec connectivity-association CA1
cipher-suite gcm-aes-256
```

4. Set the trace option values.

```
[edit]
security-administrator@hostname:fips# set security macsec traceoptions file MACsec.log
security-administrator@hostname:fips# set security macsec traceoptions file size 4000000000
security-administrator@hostname:fips# set security macsec traceoptions flag all
```

5. Assign the trace to an interface.

```
[edit]
security-administrator@hostname:fips# set security macsec interfaces interface-name
traceoptions file mka_xe size 1g
security-administrator@hostname:fips# set security macsec interfaces interface-name
traceoptions flag all
```

6. Configure the MACsec security mode as static-cak for the connectivity association.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1
security-mode static-cak
```

7. Set the MKA key server priority.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1 mka
key-server-priority 1
```

8. Set the MKA transmit interval.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1 mka
transmit-interval 3000
```

9. Enable the MKA secure.

```
[edit]
security-administrator@hostname:fips# set security macsec connectivity-association CA1
include-sci
```

10. Assign the connectivity association to an interface.

```
[edit]
security-administrator@hostname:fips# set security macsec interfaces interface-name
connectivity-association CA1
```

11. Configure VLAN tagging.

```
[edit]
security-administrator@hostname:fips# set interfaces interface-name1 flexible-vlan-tagging
security-administrator@hostname:fips# set interfaces interface-name1 encapsulation
flexibleethernet-services
security-administrator@hostname:fips# set interfaces interface-name1 unit unit-number
family ethernet-switching interface-mode trunk
security-administrator@hostname:fips# set interfaces interface-name1 unit unit-number
family ethernet-switching vlan members vlan-number-name
security-administrator@hostname:fips# set vlans vlan-number-name vlan-id vlan-number
```

Disable and Restart MACsec Sessions

To disable and restart the MACsec sessions use the following configurations:

- To disable and enable the MACsec session:

```
user@host# deactivate security macsec
user@host# activate security macsec
```

- To restart the MACsec session:

```
user@host# run restart dot1x-protocol
```

CHAPTER 6

Configuring Event Logging

IN THIS CHAPTER

Event Logging Overview

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

In addition, Junos OS can:

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

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

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

In addition, Juniper Networks recommends that logging also:

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

Interpret Event Messages

The following output shows a sample event message.

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

Table 4 on page 67 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 4: Fields in Event Messages

Field	Description	Examples
timestamp	Time when the message was generated, in one of two representations: • *MMM-DD HH:MM:SS.MS+/-HH:MM,* is the month, day, hour, minute, second and millisecond in local time. The hour and minute that follows the plus sign (+) or minus sign (-) is the offset of the local time zone from Coordinated Universal Time (UTC). • *YYYY-MM-DDTHH:MM:SS.MSZ* is the year, month, day, hour, minute, second and millisecond in UTC.	`Feb 27 02:33:04` is the timestamp expressed as local time in the United States. `2012-02-27T09:17:15.719Z` is `2:33 AM UTC on 27 Feb 2012.`
hostname	Name of the host that originally generated the message.	`router1`
process	Name of the Junos OS process that generated the message.	`mgd`
processID	UNIX process ID (PID) of the Junos OS process that generated the message.	`4153`

Table 4: Fields in Event Messages *(Continued)*

Field	Description	Examples
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]

Log Changes to Secret Data

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

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

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

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

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
```

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
```

CHAPTER 7

Performing Self-Tests on a Device

IN THIS CHAPTER

Understanding FIPS Self-Tests

IN THIS SECTION

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 140-3 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:

- `kernel_kats`—KAT for kernel cryptographic routines
- `md_kats`—KAT for libmd and libc
- `macsec_kats`—KAT for MACsec cryptographic implementation
- `openssl_kats`—KAT for OpenSSL cryptographic implementation
- `openssl-102_kats`—KAT for OpenSSL-102 cryptographic implementation
- `quicksec_kats`—KAT for QuickSec Toolkit cryptographic implementation

NOTE: For MACsec qualifications, the LC KATs has to perform on AES-GCM-128 and AESGCM-256.

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

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:

NOTE: The output is part of `/var/log/messages` that displays the known answer test results.

```
user@host>file show /var/log/messages
mgd: Running FIPS Self-tests
mgd: Testing kernel KATS:
mgd:   NIST 800-90 HMAC DRBG Known Answer Test:         Passed
mgd:   DES3-CBC Known Answer Test:                      Passed
mgd:   HMAC-SHA1 Known Answer Test:                     Passed
mgd:   HMAC-SHA2-256 Known Answer Test:                 Passed
mgd:   SHA-2-384 Known Answer Test:                     Passed
mgd:   SHA-2-512 Known Answer Test:                     Passed
mgd:   AES128-CMAC Known Answer Test:                   Passed
mgd:   AES-CBC Known Answer Test:                       Passed
mgd: Testing MACSec KATS:
mgd:   AES128-CMAC Known Answer Test:                   Passed
mgd:   AES256-CMAC Known Answer Test:                   Passed
mgd:   AES-ECB Known Answer Test:                       Passed
mgd:   AES-KEYWRAP Known Answer Test:                   Passed
mgd:   KBKDF Known Answer Test:                         Passed
mgd: Testing libmd KATS:
mgd:   HMAC-SHA1 Known Answer Test:                     Passed
mgd:   HMAC-SHA2-256 Known Answer Test:                 Passed
mgd:   SHA-2-512 Known Answer Test:                     Passed
mgd: Testing OpenSSL v1.0.2 KATS:
mgd:   FIPS ECDSA Known Answer Test:                    Passed
mgd:   FIPS ECDH 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:   RSA-ENC Known Answer Test:                          Passed
mgd:   RSA-SIGN Known Answer Test:                         Passed
mgd:   ECDSA-SIGN Known Answer Test:                       Passed
mgd:   KDF-IKE-V1 Known Answer Test:                       Passed
mgd:   KDF-SSH-SHA256 Known Answer Test:                   Passed
mgd:   KAS-ECC-EPHEM-UNIFIED-NOKC Known Answer Test:       Passed
mgd:   KAS-FFC-EPHEM-NOKC Known Answer Test:               Passed
mgd: Testing OpenSSL KATS:
mgd:   FIPS ECDSA Known Answer Test:                       Passed
mgd:   FIPS ECDH 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:   RSA-ENC Known Answer Test:                          Passed
mgd:   RSA-SIGN Known Answer Test:                         Passed
mgd:   ECDSA-SIGN Known Answer Test:                       Passed
mgd:   KDF-IKE-V1 Known Answer Test:                       Passed
mgd:   KDF-SSH-SHA256 Known Answer Test:                   Passed
mgd:   KAS-ECC-EPHEM-UNIFIED-NOKC Known Answer Test:       Passed
mgd:   KAS-FFC-EPHEM-NOKC Known Answer Test:               Passed
mgd: Testing QuickSec 7.0 KATS:
mgd:   NIST 800-90 HMAC DRBG Known Answer Test:            Passed
mgd:   DES3-CBC Known Answer Test:                         Passed
mgd:   HMAC-SHA1 Known Answer Test:                        Passed
mgd:   HMAC-SHA2-224 Known Answer Test:                    Passed
mgd:   HMAC-SHA2-256 Known Answer Test:                    Passed
mgd:   HMAC-SHA2-384 Known Answer Test:                    Passed
mgd:   HMAC-SHA2-512 Known Answer Test:                    Passed
mgd:   AES-CBC Known Answer Test:                          Passed
mgd:   AES-GCM Known Answer Test:                          Passed
mgd:   SSH-RSA-ENC Known Answer Test:                      Passed
mgd:   SSH-RSA-SIGN Known Answer Test:                     Passed
mgd:   SSH-ECDSA-SIGN Known Answer Test:                   Passed
mgd:   KDF-IKE-V1 Known Answer Test:                       Passed
mgd:   KDF-IKE-V2 Known Answer Test:                       Passed
mgd: Testing QuickSec KATS:
mgd:   NIST 800-90 HMAC DRBG Known Answer Test:            Passed
mgd:   DES3-CBC Known Answer Test:                         Passed
```

```
mgd:   HMAC-SHA1 Known Answer Test:                    Passed
mgd:   HMAC-SHA2-224 Known Answer Test:                Passed
mgd:   HMAC-SHA2-256 Known Answer Test:                Passed
mgd:   HMAC-SHA2-384 Known Answer Test:                Passed
mgd:   HMAC-SHA2-512 Known Answer Test:                Passed
mgd:   AES-CBC Known Answer Test:                      Passed
mgd:   AES-GCM Known Answer Test:                      Passed
mgd:   SSH-RSA-ENC Known Answer Test:                  Passed
mgd:   SSH-RSA-SIGN Known Answer Test:                 Passed
mgd:   KDF-IKE-V1 Known Answer Test:                   Passed
mgd:   KDF-IKE-V2 Known Answer Test:                   Passed
mgd: Testing SSH IPsec KATS:
mgd:   NIST 800-90 HMAC DRBG Known Answer Test:        Passed
mgd:   DES3-CBC Known Answer Test:                     Passed
mgd:   HMAC-SHA1 Known Answer Test:                    Passed
mgd:   HMAC-SHA2-256 Known Answer Test:                Passed
mgd:   AES-CBC Known Answer Test:                      Passed
mgd:   SSH-RSA-ENC Known Answer Test:                  Passed
mgd:   SSH-RSA-SIGN Known Answer Test:                 Passed
mgd:   KDF-IKE-V1 Known Answer Test:                   Passed
mgd: Testing file integrity:
mgd:   File integrity Known Answer Test:               Passed
mgd: Testing crypto integrity:
mgd:   Crypto integrity Known Answer Test:             Passed
```

8

CHAPTER

Operational Commands

IN THIS CHAPTER

request system zeroize

IN THIS SECTION

Syntax

request system zeroize

Description

Remove all configuration information on the Routing Engines and reset all key values. If the device has dual Routing Engines, the command is broadcast to both Routing Engines on the device. The command removes all data files, including customized configuration and log files, by unlinking the files from their directories. The command removes all user-created files from the system including all plain-text passwords, secrets, and private keys for SSH, local encryption, local authentication, IPsec, RADIUS, TACACS+, and SNMP.

This command reboots the device and sets it to the factory-default configuration. After the reboot, you cannot access the device through the management Ethernet interface. Log in through the console as the root user and start the Junos OS CLI by typing cli at the prompt.

Options

none—Zeroize the Routing Engine in Junos OS in FIPS mode. You must confirm the request by typing **yes** to proceed. This command is restricted to Crypto Officers because the `maintenance` permission bit is one of the permission bits, along with `secret` and `control`, that distinguishes Crypto Officers from other FIPS users.

Required Privilege Level

maintenance

Output Fields

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

Sample Output

request system zeroize (FIPS)

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

Release Information

Command introduced in Junos OS Release 18.1