

Junos® OS

Common Criteria Evaluated Configuration Guide for MX240, MX480, MX960, EX9204, EX9208 and EX9214 Devices

Published
2026-06-18

RELEASE
24.4R2

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

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

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

Junos® OS Common Criteria Evaluated Configuration Guide for MX240, MX480, MX960, EX9204, EX9208 and EX9214 Devices
24.4R2

Copyright © 2025 Juniper Networks, Inc. All rights reserved.

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

About This Guide | vi

1

Overview

Common Criteria Evaluated Configuration Overview | 2

Overview of Junos OS in FIPS Mode | 4

Overview of FIPS Terminology and Supported Cryptographic Algorithms | 5

Identify Secure Product Delivery | 9

Management Interfaces Overview | 11

2

Configure Roles and Authentication Methods

Overview of Roles and Services for Junos OS | 13

Overview of the Operational Environment for Junos OS in FIPS Mode | 16

Download Software Packages from Juniper Networks | 20

Install Junos OS Software Packages | 21

Overview of Zeroization to Clear System Data for FIPS Mode | 24

Zeroize the System For FIPS Mode | 26

Enable FIPS Mode | 27

3

Configure Administrative Credentials and Privileges

Services Available Prior to Authentication | 30

Configure Password Rules for an Authorized Administrator | 30

Configure a Network Device Collaborative Protection Profile Authorized Administrator | 33

Configuring Network Time Protocol | 36

Customize Time in FIPS Mode | 37

Inactivity Timeout Period Configuration, and Local and Remote Idle Session Termination | 38

Configure Session Termination | 38

Sample Output for Local Administrative Session Termination | 40

Sample Output for Remote Administrative Session Termination | 40

Sample Output for User Initiated Termination | 41

4

Configure SSH and Console Connection

Configure System Login Message and Announcement | 43

Configure SSH on the Evaluated Configuration | 44

SSH Host Keys | 47

Limit the Number of User Login Attempts for SSH Sessions | 48

5

Configure the Remote Syslog Server

Sample Syslog Server Configuration on a Linux System | 52

6

Configure Audit Log Options

Configure Audit Log Options in FIPS Mode | 60

Configure Audit Log Options on Device in FIPS Mode | 60

Junos OS Log File Management and Storage Behavior | 61

Sample Code Audits of Configuration Changes | 62

7

Configure Event Logging

Event Logging Overview | 66

Interpret Event Messages | 103

Log Changes to Secret Data | 104

Login and Logout Events Using SSH | 105

Logging of Audit Startup | 105

8

Configure MACsec

Media Access Control Security (MACsec) in FIPS Mode Overview | 108

Configure MACsec | 110

Configuring MACsec on a Device Running Junos OS | 111

- Configuring Static MACsec with Layer 3 Traffic | 113
- Configuring MACsec with keychain using Layer 3 Traffic | 116
- Configuring Static MACsec for Layer 2 Traffic | 122
- Configuring MACsec with keychain for Layer 2 Traffic | 128
- Disable and Restart MACsec Sessions | 135

9

Perform Self-Tests on a Device

- FIPS Self-Tests Overview | 137

10

Operational Commands

- request vmhost zeroize no-forwarding | 141

About This Guide

Use this guide to configure and evaluate MX240, MX480, MX960, EX9204, EX9208, and EX9214 devices for Common Criteria (CC) compliance. Common Criteria for information technology is an international agreement signed by several countries that permit the evaluation of security products against a common set of standards.

RELATED DOCUMENTATION

| [Common Criteria and FIPS Certifications](#)

1

CHAPTER

Overview

IN THIS CHAPTER

- Common Criteria Evaluated Configuration Overview | 2
 - Overview of Junos OS in FIPS Mode | 4
 - Overview of FIPS Terminology and Supported Cryptographic Algorithms | 5
 - Identify Secure Product Delivery | 9
 - Management Interfaces Overview | 11
-

Common Criteria Evaluated Configuration Overview

IN THIS SECTION

- [Common Criteria Overview | 2](#)
- [Product Functionality Not Included in the Scope of the Evaluation | 2](#)
- [Supported Platforms | 3](#)

This document describes the steps required to duplicate the configuration of the device running Junos OS when the device is evaluated. This is referred to as the evaluated configuration. The following list describes the standards to which the device has been evaluated:

- NDcPPv3.0e—<https://www.niap-ccevs.org/protectionprofiles/482>
- MOD_MACSEC_V1.0—https://www.niap-ccevs.org/static_html/protection-profile/480/MACsec/index.html

Common Criteria Overview

Common Criteria for information technology is an international agreement signed by several countries that permits the evaluation of security products against a common set of standards. In the Common Criteria Recognition Arrangement (CCRA) at <https://www.commoncriteriaportal.org/ccra/index.cfm>, the participants agree to mutually recognize evaluations of products performed in other countries. All evaluations are performed using a common methodology for information technology security evaluation.

For more information on Common Criteria, see <https://www.commoncriteriaportal.org/>.

Target of Evaluation (TOE) is a device or system subjected to evaluation based on Collaborative Protection Profile (cPP).

Product Functionality Not Included in the Scope of the Evaluation

The following product functionalities are not included in the CC evaluation:

- Use of telnet, since it violates the Trusted Path requirement set
- Use of FTP, since it violates the Trusted Path requirement set
- Use of SNMP, since it violates the Trusted Path requirement set
- Use of SSL, including management via J-Web, JUNOScript and JUNOScope, since it violates the Trusted Path requirement set
- Use of CLI account super-user and Linux root account.

Security Functions Provided by the TOE

The TOE provides the security functions required by the Collaborative Protection Profile for Network Devices, hereafter referred to as NDcPP v3.0e or NDcPP. The TOE also provides the security functions required by the Functional Package for SSH, hereafter referred to as PKG_SSH_V1.0 and the PP-Module for MACsec Ethernet Encryption, Version 1.0, hereafter referred to as MOD_MACsec_V1.0. Each of these security functionalities are listed in more detail in the sections below.

Security Audit

The TOE generates audit events for all start-up and shutdown functions as well as all auditable events specified in Tables 12 and 13 of the ST. Auditable events are stored in the syslog files on the appliance and can be sent to an external log server (via Netconf over SSH). Auditable events include start-up and shutdown of the audit functions, authentication events, and all SFR-specific events required by the applicable Protection Profiles, Packages and Modules. Audit records include the date and time, event category, event type, username, and the outcome of the event (success or failure). Local syslog storage limits are configurable and monitored. If the storage limit is reached the oldest logs will be overwritten.

Cryptographic Support

The TOE implements an SSH server to support protected communications for administrators to establish secure sessions and to connect to external syslog servers. The TOE requires that applications exchanging information with it are successfully authenticated prior to any exchange (i.e. applications connecting over SSH). Layer 2 communication over point-to-point Ethernet links between the TOE and compliant peers can be secured using MACsec. The TOE includes cryptographic modules that implement the underlying cryptographic services, including key management and protection of stored keys, algorithms, random bit generation and crypto administration. The cryptographic modules provide confidentiality and integrity services for authentication and for protecting communications with connecting applications.

Identification And Authentication

The TOE supports Role Based Access Control. All users must be authenticated to the TOE prior to being granted access to any management actions. The TOE supports password-based authentication and public key-based authentication. Based on the assigned role, a user is granted a set of privileges to access the system. Administrative users must provide unique identification and authentication data before any administrative access to the system is granted. Authentication data entered and stored on the TOE is protected.

Security Management

The TOE provides a Security Administrator role that is responsible for

- Ability to administer the TOE remotely

- Ability to configure the access banner
- Ability to configure the remote session inactivity time before session termination
- Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates
- Ability to start and stop services
- Ability to configure local audit behaviour
- Ability to modify the behaviour of the transmission of audit data to an external IT entity
- Ability to manage the cryptographic keys
- Ability to configure the cryptographic functionality
- Ability to configure thresholds for SSH rekeying
- Ability to re-enable an Administrator account
- Ability to configure the local session inactivity time before session termination or locking
- Ability to configure the authentication failure parameters for FIA_AFL.1
- Ability to set the time which is used for timestamps
- Ability to configure NTP
- Ability to administer the TOE locally
- Ability to manage the trusted public keys database
- Ability to manage a PSK-based CAK and install it in the device
- Ability to manage the Key Server to create, delete, and activate MKA participants using the CLI commands
- Ability to specify the lifetime of a CAK
- Ability to enable, disable, or delete a PSK-based CAK using CLI commands.

The devices are managed through a Command Line Interface (CLI). The CLI is accessible through local (serial) console connection or remote administrative (SSH) session.

Protection Of The TSF

The TOE protects all passwords, pre-shared keys, symmetric keys and private keys from unauthorized disclosure. Passwords are stored using sha256 or sha512. The TOE executes self-tests during initial start-up to ensure correct operation and enforcement of its security functions. An administrator can install software updates to TOE. The TOE allows manual setting of time by the administrator and is also capable of syncing time to an NTP server.

TOE Access

The TOE displays a customizable banner before any administrative session can be established with it. The TOE will terminate local or remote interactive sessions after a specified period of session inactivity configured by an administrator. An administrator can terminate their own interactive local or remote sessions.

Trusted Path/Channels

The TOE supports SSHv2 for secure communications with authorized IT entities such as syslog servers. The TOE supports SSHv2 (remote CLI) for secure remote administration. The TOE also supports MACsec for securing data at Layer 2 between TOE and MACsec supporting peer device.

Supported Platforms

For the features described in this document, the following platforms are supported to qualify NDcPPv3.0e:

Model	RE	RE CPU	MACsec Linecard	MIC-3D-10GE-SGP-E within MPC3E-3D-NG
MX240	RE-S-X6-128G	Intel HASWELL-EP	MPC10-10C and MPC10E-15C, with JNPR Penta Silicon MACsec ASIC	BMC82756 MACsec ASIC with CAVP num AES4550
MX480	RE-S-X6-64G	Xeon E5-2608L V3		
MX960				
EX9204	EX9200-RE2	Intel HASWELL-EP	EX9200-15C, with JNPR Penta Silicon MACsec ASIC	NA
EX9208		Xeon E5-2608L V3		
EX9214				

RELATED DOCUMENTATION

| [Identify Secure Product Delivery](#) | 9

Overview of Junos OS in FIPS Mode

IN THIS SECTION

- [About the Cryptographic Boundary on Your Device | 4](#)
- [How FIPS Mode Differs from Non-FIPS Mode | 4](#)
- [Validated Version of Junos OS in FIPS Mode | 5](#)

Federal Information Processing Standards (FIPS) 140-3 defines security levels for hardware and software that perform cryptographic functions. Operating the security devices in a FIPS 140-3 Level 1 environment requires enabling and configuring FIPS mode on the devices from the Junos OS command-line interface (CLI).

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

About the Cryptographic Boundary on Your 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.



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

How FIPS Mode Differs from Non-FIPS Mode

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, remote, or unencrypted management connections must not be configured. However, TOE allows local and un-encrypted console access across all modes of operation.
- Passwords must be encrypted with strong one-way algorithms that do not permit decryption.
- Junos-FIPS administrator passwords must be at least 10 characters long.
- Cryptographic keys must be encrypted before transmission.

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

| [Identify Secure Product Delivery](#) | 9

Overview of FIPS Terminology and Supported Cryptographic Algorithms

IN THIS SECTION

- [Terminology](#) | 6
- [Supported Cryptographic Algorithms](#) | 7

Use the definitions of FIPS terms, and supported algorithms to help the TOE's administrator understand Junos OS in FIPS mode.

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 "Overview of 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.
Security Administrator	Person with appropriate permissions who is responsible for securely enabling, configuring, monitoring, and maintaining Junos OS in FIPS mode of operation on a device. For details, see "Overview of Junos OS in FIPS Mode" on page 4.
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.	
Hashing	A message authentication method that applies a cryptographic technique iteratively to a message of arbitrary length and produces a hash <i>message digest</i> or <i>signature</i> of fixed length that is appended to the message when sent.
KATs	Known answer tests. System self-tests that validate the output of cryptographic algorithms approved for FIPS and test the integrity of some Junos OS modules. For details, see "FIPS Self-Tests Overview" on page 137.
NDcPPv3.0e	Collaborative Protection Profile for Network Devices.
SSH	A protocol that uses strong authentication and encryption for remote access across a non-secure network. SSH provides remote login, remote program execution, file copy, and other functions. It is intended as a secure replacement for <code>rlogin</code> , <code>rsh</code> , and <code>rcp</code> 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 devices for non-FIPS operation. The Crypto Officer can zeroize the system with a CLI operational command.

Supported Cryptographic Algorithms

Table 1 on page 8 summarizes the high level protocol algorithm support.



WARNING: For FIPS 140-3 compliance, use only FIPS-approved cryptographic algorithms in Junos OS in FIPS mode. The Cryptographic Algorithms referred to in Chapters "[Configure SSH and Console Connection](#)" on page 44 and "[Configure MACsec](#)" on page 110 have been tested for Common Criteria Evaluation of the device. Use of other cryptographic implementations was not evaluated nor tested.

Table 1: 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 • ECDSA P-384 • ECDSA P-521 • SSH-RSA • RSA-SHA2-256 • RSA-SHA2-512 Client (user): • ECDSA P-256 • ECDSA P-384 • ECDSA P-521 • SSH-RSA • RSA-SHA2-256 • RSA-SHA2-512	• AES CTR 128 • AES CTR 256 • AES CBC 128 • AES CBC 256 • aes128-gcm@openssh.com • aes256-gcm@openssh.com	• HMAC-SHA-256 • HMAC-SHA-512

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

- AES** The Advanced Encryption Standard (AES), defined in FIPS PUB 197. The AES algorithm uses keys of 128 or 256 bits to encrypt and decrypt data using CBC, CTR, and GCM modes.
- DRBG** Deterministic Random Bit Generator. The DRBG implemented is not configurable. It is always the HMAC DRBG using SHA-512. The DRBG is seed with 448 bits of entropy, which exceed the 384 required by the FIPS standard. The DRBG is seeded with multiple entropy sources generated within the Junos OS kernel. The designated primary entropy source for FIPS purposes that determines when the DRBG is considered fully seeded and operational is bits 2-10 of the timestamp associated with kernel software interrupts.



NOTE: DRBG requires no configuration and runs automatically at boot.

ECDH	Elliptic Curve Diffie-Hellman. A variant of the Diffie-Hellman key exchange algorithm that uses cryptography based on the algebraic structure of elliptic curves over finite fields. ECDH allows two parties, each having an elliptic curve public-private key pair, to establish a shared secret over an insecure channel. The shared secret can be used either as a key or to derive another key for encrypting subsequent communications using a symmetric key cipher.
ECDSA	Elliptic Curve Digital Signature Algorithm. A variant of the Digital Signature Algorithm (DSA) that uses cryptography based on the algebraic structure of elliptic curves over finite fields. The bit size of the elliptic curve determines the difficulty of decrypting the key. The public key believed to be needed for ECDSA is about twice the size of the security level, in bits. ECDSA using the P-256, P-384, and P-521 curves can be configured under OpenSSH.
HMAC	Defined as “Keyed-Hashing for Message Authentication” in RFC 2104, HMAC combines hashing algorithms with cryptographic keys for message authentication. For Junos OS in FIPS mode, HMAC uses the iterated cryptographic hash functions SHA-1, SHA-256, and SHA-512 along with a secret key.
SHA-1, SHA-384, SHA-256, and SHA-512	Secure hash algorithms (SHA) belonging to the SHA-2 standard defined in FIPS PUB 180-2. SHA-1 produces a 160-bit hash, SHA-256 produces a 256-bit hash digest, SHA-384 produces a 384-bit hash digest, and SHA-512 produces a 512-bit hash digest.

RELATED DOCUMENTATION

[FIPS Self-Tests Overview | 137](#)

[Overview of Zeroization to Clear System Data for FIPS Mode | 24](#)

Identify 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 an appliance 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, 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 in to the Juniper Networks online customer support portal at <https://www.juniper.net/customers/csc/management> to view the order status. Compare the carrier tracking number or the Juniper Networks order number listed in the Juniper Networks shipment notification with the tracking number on the package received.

Management Interfaces Overview

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). The TOE's administrator 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. The fxp0 interface is the dedicated out-of-band management port, designed for management traffic only and isolated from in-band forwarding. 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

Configure Roles and Authentication Methods

IN THIS CHAPTER

- Overview of Roles and Services for Junos OS | **13**
 - Overview of the Operational Environment for Junos OS in FIPS Mode | **16**
 - Download Software Packages from Juniper Networks | **20**
 - Install Junos OS Software Packages | **21**
 - Overview of Zeroization to Clear System Data for FIPS Mode | **24**
 - Zeroize the System For FIPS Mode | **26**
 - Enable FIPS Mode | **27**
-

Overview of Roles and Services for Junos OS

IN THIS SECTION

- [Security Administrator Role and Responsibilities | 14](#)
- [FIPS User Role and Responsibilities | 14](#)
- [What Is Expected of All FIPS Users | 15](#)

The Security Administrator is associated with the defined login class security-admin, which has the necessary permission set to permit the administrator to perform all tasks necessary to manage Junos OS. Administrative users (Security Administrator) must provide unique identification and authentication data before any administrative access to the system is granted.

Security Administrator roles and responsibilities are as follows:

1. Ability to administer the TOE remotely
2. Ability to configure the access banner
3. Ability to configure the remote session inactivity time before session termination
4. Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates
5. Ability to start and stop services
6. Ability to configure local audit behaviour (changes to storage locations for audit; changes to behaviour when local audit storage space is full, changes to local audit storage size)
7. Ability to modify the behaviour of the transmission of audit data to an external IT entity
8. Ability to manage the cryptographic keys
9. Ability to configure the cryptographic functionality
10. Ability to configure thresholds for SSH rekeying
11. Ability to re-enable an Administrator account
12. Ability to configure the local session inactivity time before session termination or locking
13. Ability to configure the authentication failure parameters for FIA_AFL.1
14. Ability to set the time which is used for time-stamps

15. Ability to configure NTP
16. Ability to administer the TOE locally
17. Ability to manage the trusted public keys database.

The Juniper Networks Junos operating system (Junos OS) running in non-FIPS mode allows a wide range of capabilities for users, and authentication is identity-based.

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

Security Administrator Role and Responsibilities

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

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

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

- Set the initial root password. The length of the password should be at least 10 characters.
- Reset user passwords with FIPS-approved algorithms.
- 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 who are part of operator/read-only/superuser or super-user class, including the Security Administrator, can view the configuration. Only the user assigned as the Security Administrator can modify the configuration.

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

What Is Expected of All FIPS Users

All FIPS users, including the Security Administrator, must observe security guidelines at all times.

All FIPS users must:

- Keep all passwords confidential.
- Store 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

[Zeroize the System For FIPS Mode](#) | 26

Overview of the Operational Environment for Junos OS in FIPS Mode

IN THIS SECTION

- [Hardware Environment for Junos OS in FIPS Mode | 16](#)
- [Software Environment for Junos OS in FIPS Mode | 16](#)
- [TOE Environmental Components | 17](#)
- [Critical Security Parameters | 18](#)

A Juniper Networks device running the Juniper Networks Junos operating system (Junos OS) in FIPS mode forms a special type of hardware and software operational environment that is different from the environment of 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. There are two types of hardware with cryptographic boundaries in Junos OS in FIPS mode: one for each Routing Engine and one for entire chassis.

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 nonmodifiable 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 in FIPS mode 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 Security Administrator successfully enables FIPS mode on a device. The Junos OS image that includes FIPS mode is available on the Juniper Networks website and can be installed on a functioning device.

For FIPS 140-3 compliance, the recommendation is that the TOE's administrator 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, the TOE's administrator 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.

The TOE's administrator can use only SSH as a remote access service.

All passwords established for users after the upgrade to Junos OS in FIPS mode must conform to the specifications for Junos OS in FIPS mode. For more information, see "[Configure Password Rules for an Authorized Administrator](#)" on page 30.



NOTE: Do not attach the device to a network until the Security Administrator completes configuration from the local console connection.

TOE Environmental Components

[Table 2 on page 18](#) lists the environmental components that are required to operate the TOE in the evaluated configuration.

Table 2: TOE Environmental Components

Components	Description
Local Management Console	Any management workstation (computer) that is directly (serially) connected to the TOE's console port may be used by the TOE administrator for local administration of the TOE.
Remote Management Workstation	Any management workstation (computer) with a SSHv2 client installed that may be used by the TOE administrator for remote administration of the TOE through SSH protected channel.
Syslog Server	A syslog server, used for remote storage of audit records that have been generated by and transmitted from the TOE securely using SSH tunnel (SSHv2).
NTP Server	A NTPv4 server, used to provide reliable timestamps to the TOE.
MACsec Peer	A MACsec Peer, used for establishing MACsec communication for securing Layer 2 data using MACsec functionality.

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	Zeroize	Use
SSHv2 private host key	ECDSA / RSA key used to identify the host, generated the first time SSH is configured.	Zeroize command.	Used to identify the host.

Table 3: Critical Security Parameters (Continued)

CSP	Description	Zeroize	Use
SSHv2 session keys	Session key used with SSHv2 and as a Diffie-Hellman private key. Encryption: AES-128, AES-256, aes128-gcm@openssh.com, and aes256-gcm@openssh.com. MACs: HMAC-SHA2-256, 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: SHA256, SHA512.	Zeroize command.	Used to authenticate a user to the cryptographic module.
Crypto Officer authentication key	Hash of the Crypto Officer's password: SHA256, SHA512.	Zeroize command.	Used to authenticate the Security Administrator to the cryptographic module.
HMAC DRBG seed	Seed for deterministic random bit generator (DRBG).	Seed is not stored by the cryptographic module.	Used for seeding DRBG.
HMAC DRBG V value	The value (V) of output block length (outlen) in bits, which is updated each time another outlen bits of output are produced.	Power cycle.	A critical value of the internal state of DRBG.
HMAC DRBG key value	The current value of the outlen-bit key, which is updated at least once each time that the DRBG mechanism generates pseudorandom bits.	Power cycle.	A critical value of the internal state of DRBG.

Table 3: Critical Security Parameters (Continued)

CSP	Description	Zeroize	Use
NDRNG entropy	The NDRNG provides 448 bits of entropy collected per NIST SP 800-90B. 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.

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

Local passwords are hashed with the SHA256 or SHA512 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

[Overview of Zeroization to Clear System Data for FIPS Mode](#) | 24

Download Software Packages from Juniper Networks

The TOE's administrator can download the Junos OS software package from the Juniper Networks website. Before the TOE's administrator begin to download the software, ensure that the TOE's administrator 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/](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

| [Installation and Upgrade Guide](#)

Install Junos OS Software Packages

The administrator can use this procedure to upgrade Junos OS on the device.



NOTE: Junos OS is delivered in signed packages with manifests which validate the immutability of the contents. There is also a signature of the manifest that can be validated with public keys that are packaged. During install of the software packages, Junos OS validates the signature, and the hashes of the contents present in the manifest. If the image fails the signature check, then the image is deleted from the device and no upgrade occurs, with the appropriate error visible on the CLI. Successful update is only initiated when the signature verification of the TOE passes. Logs are generated in both cases. Software update performed in FIPS mode is similar to that in non-FIPS mode for the functionalities available on the device. TOE functionalities are unavailable only during the reboot following the upgrade. Junos OS does not support delayed activation while performing software updates.

To install software upgrades on the device:

1. Download the software package as described in "[Download Software Packages from Juniper Networks](#)" on page 20.
2. If the TOE's administrator has 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. Copy the software package to the device. The best practice is to use SFTP to copy the file to the `/var/ tmp/` directory.
4. Install the new package on the device:

```
user@host> request vmhost software add package
```

Replace ***package*** with local directory on the device where the software package is copied. For example, `/var/tmp/package.tgz`.



NOTE: If one needs to stop the installation, do not reboot the device. Instead, complete the package installation as seen in Step 4 and then issue the command “**request system software delete <package.tgz>**”. This is the last opportunity to cancel the installation.

5. Reboot the device to load the installation:

```
user@host> request vmhost reboot
```

6. Once the system completes rebooting, log in and use the show version command to verify the successful installation of the new software version.

```
user@host> show version
Hostname: hostname
Model: mx240
Family: junos
Junos: 24.4R2.9
JUNOS OS Kernel 64-bit [20250529.3e76435_builder_bsd15_244]
JUNOS OS libs [20250529.3e76435_builder_bsd15_244]
JUNOS OS libs compat32 [20250529.3e76435_builder_bsd15_244]
JUNOS OS vmguest [20250529.3e76435_builder_bsd15_244]
JUNOS OS pkgrs [20250529.3e76435_builder_bsd15_244]
JUNOS modules [20250613.010225_builder_junos_244_r2]
JUNOS OS 32-bit compatibility [20250529.3e76435_builder_bsd15_244]
JUNOS OS runtime [20250529.3e76435_builder_bsd15_244]
JUNOS OS crypto [20250529.3e76435_builder_bsd15_244]
JUNOS OS boot-ve files [20250529.3e76435_builder_bsd15_244]
JUNOS mx libs [20250613.010225_builder_junos_244_r2]
JUNOS OS time zone information [20250529.3e76435_builder_bsd15_244]
JUNOS network stack and utilities [20250613.010225_builder_junos_244_r2]
JUNOS SDN Software Suite [20250613.010225_builder_junos_244_r2]
JUNOS libs [20250613.010225_builder_junos_244_r2]
JUNOS py extensions [20250613.010225_builder_junos_244_r2]
JUNOS py base [20250613.010225_builder_junos_244_r2]
JUNOS OS package [20250407.212945_builder_main]
JUNOS jail runtime [20250529.3e76435_builder_bsd15_244]
JUNOS libs compat32 [20250613.010225_builder_junos_244_r2]
JUNOS daemons [20250613.010225_builder_junos_244_r2]
JUNOS vmguest (MTX) [20250613.010225_builder_junos_244_r2]
JUNOS mtx network modules [20250613.010225_builder_junos_244_r2]
JUNOS mx daemons [20250613.010225_builder_junos_244_r2]
JUNOS OS network modules [20250529.3e76435_builder_bsd15_244]
JUNOS vmguest [20250613.010225_builder_junos_244_r2]
JUNOS mx libs compat32 [20250613.010225_builder_junos_244_r2]
JUNOS runtime [20250613.010225_builder_junos_244_r2]
JUNOS mx runtime [20250613.010225_builder_junos_244_r2]
```

JUNOS mx modules [20250613.010225_builder_junos_244_r2]
 JUNOS Services Telemetry [20250613.010225_builder_junos_244_r2]
 JUNOS Services TCP-LOG [20250613.010225_builder_junos_244_r2]
 JUNOS Services SSL [20250613.010225_builder_junos_244_r2]
 JUNOS Services SOFTWARE [20250613.010225_builder_junos_244_r2]
 JUNOS Services Stateful Firewall [20250613.010225_builder_junos_244_r2]
 JUNOS Services RTCOM [20250613.010225_builder_junos_244_r2]
 JUNOS Services RPM [20250613.010225_builder_junos_244_r2]
 JUNOS Services PCEF package [20250613.010225_builder_junos_244_r2]
 JUNOS Services NAT [20250613.010225_builder_junos_244_r2]
 JUNOS Services Mobile Subscriber Service Container package
 [20250613.010225_builder_junos_244_r2]
 JUNOS Services MobileNext Software package [20250613.010225_builder_junos_244_r2]
 JUNOS Services Logging Report Framework package [20250613.010225_builder_junos_244_r2]
 JUNOS Services Jflow Container package [20250613.010225_builder_junos_244_r2]
 JUNOS Services Deep Packet Inspection package [20250613.010225_builder_junos_244_r2]
 JUNOS Services IPSec [20250613.010225_builder_junos_244_r2]
 JUNOS Services IDS [20250613.010225_builder_junos_244_r2]
 JUNOS Services HTTP Content Management package [20250613.010225_builder_junos_244_r2]
 JUNOS Services DNS Filter package (i386) [20250613.010225_builder_junos_244_r2]
 JUNOS Services Crypto [20250613.010225_builder_junos_244_r2]
 JUNOS Services Captive Portal and Content Delivery Container package
 [20250613.010225_builder_junos_244_r2]
 JUNOS Services COS [20250613.010225_builder_junos_244_r2]
 JUNOS Appld Services [20250613.010225_builder_junos_244_r2]
 JUNOS Services Application Level Gateways [20250613.010225_builder_junos_244_r2]
 JUNOS Extension Toolkit [20250613.010225_builder_junos_244_r2]
 JUNOS Phone-home [20250613.010225_builder_junos_244_r2]
 JUNOS Packet Forwarding Engine Support (wrlinux9) [20250613.010225_builder_junos_244_r2]
 JUNOS Packet Forwarding Engine Support (MX/EX92XX Common)
 [20250613.010225_builder_junos_244_r2]
 JUNOS Packet Forwarding Engine FIPS Support [24.4R2.9]
 JUNOS Packet Forwarding Engine Support (M/T Common) [20250613.010225_builder_junos_244_r2]
 JUNOS Packet Forwarding Engine Support (aft) [20250613.010225_builder_junos_244_r2]
 JUNOS Packet Forwarding Engine Support (MX Common) [20250613.010225_builder_junos_244_r2]
 JUNOS Juniper Malware Removal Tool (JMRT) [1.0.0+24.4R2.9]
 JUNOS J-Insight [20250613.010225_builder_junos_244_r2]
 JUNOS jfirmware [20250529.211134_builder_junos_244_r2]
 JUNOS Online Documentation [20250613.010225_builder_junos_244_r2]
 JUNOS FIPS mode utilities [20250613.010225_builder_junos_244_r2]
 JUNOS dsa [20250613.010225_builder_junos_244_r2]
 JUNOS SSH Tunnel Daemon [20250613.010225_builder_junos_244_r2]
 JUNOS sflow mx [20250613.010225_builder_junos_244_r2]

JUNOS na telemetry [24.4R2.9]
 JUNOS full sysmond [20250613.010225_builder_junos_244_r2]
 JUNOS support scripts [20250613.010225_builder_junos_244_r2]
 JUNOS Security Intelligence [20250613.010225_builder_junos_244_r2]
 Junos scheduler tracing [20250613.010225_builder_junos_244_r2]
 JUNOS RPD Telemetry Application [24.4R2.9]
 JUNOS python routing scripts for consistency check in RIB/FIB/PFE
 [20250613.010225_builder_junos_244_r2]
 JUNOS Routing mpls-oam-basic [20250613.010225_builder_junos_244_r2]
 JUNOS Routing mpls-oam-advanced [20250613.010225_builder_junos_244_r2]
 JUNOS Routing lsys [20250613.010225_builder_junos_244_r2]
 JUNOS Routing controller-internal [20250613.010225_builder_junos_244_r2]
 JUNOS Routing controller-external [20250613.010225_builder_junos_244_r2]
 JUNOS Routing 32-bit Compatible Version [20250613.010225_builder_junos_244_r2]
 JUNOS Routing aggregated [20250613.010225_builder_junos_244_r2]
 JUNOS probe utility [20250613.010225_builder_junos_244_r2]
 JUNOS common platform support [20250613.010225_builder_junos_244_r2]
 JUNOS Openconfig [24.4R2.9]
 JUNOS L2 RSI Scripts [20250613.010225_builder_junos_244_r2]
 JUNOS Key Manager [20250613.010225_builder_junos_244_r2]
 JUNOS SQL Sync Daemon [20250613.010225_builder_junos_244_r2]
 JUNOS mtx Data Plane Crypto Support [20250613.010225_builder_junos_244_r2]
 JUNOS Broadband Edge User Plane Apps [24.4R2.9]
 Junos Remote Attestation package [1.0.0+20250613.010225_builder_junos_244_r2]
 JUNOS appidd-mx application-identification daemon [20250613.010225_builder_junos_244_r2]
 JUNOS Common BIOS [20250613.010225_builder_junos_244_r2]
 JUNOS Services URL Filter package [20250613.010225_builder_junos_244_r2]
 JUNOS Services TLB Service PIC package [20250613.010225_builder_junos_244_r2]
 JUNOS Juniper Malware Removal Tool (JMRT) Test [1.0.0+24.4R2.9]

Overview of Zeroization to Clear System Data for FIPS Mode

IN THIS SECTION

 [Why Zeroize? | 25](#)

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.

Security Administrator initiates the zeroization process by entering the request `vmhost zeroize no-forwarding` operational command.

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



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



CAUTION: There are no configurations that do not conform to the key destruction requirement.

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, the TOE's administrator must zeroize the system to remove sensitive information before disabling FIPS mode on the device.

When to Zeroize?

As Security Administrator, perform zeroization in the following situations:

- **Before enabling FIPS mode of operation:** To prepare your 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 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.

Zeroize the System For FIPS Mode

Follow the below procedure to zeroize your device:

1. Login to the device as a security-admin user from CLI, then enter:

```
security-admin@TOE> request vmhost zeroize no-forwarding
VMHost Zeroization : Erase all data, including configuration and log files ? [yes,no] (no)
yes
```

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

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

```
warning: Vmhost will reboot and may not boot without configuration
```

```
warning: Proceeding with vmhost zeroize
```

```
Zeroise secondary internal disk ...
```

```
Proceeding with zeroize on secondary disk
```

```
Mounting device in preparation for zeroize...
```

```
Cleaning up target disk for zeroize ...
```

```
Zeroize done on target disk.
```

```
Zeroize of secondary disk completed
```

```
Zeroize primary internal disk ...
```

```
Proceeding with zeroize on primary disk
```

```
/etc/ssh/ssh_host_ecdsa_key.pub
```

```
/etc/ssh/ssh_host_rsa_key.pub
```

```
/etc/ssh/ssh_host_ecdsa_key
```

```
/etc/ssh/ssh_host_dsa_key
```

```
/etc/ssh/ssh_host_dsa_key.pub
```

```
/etc/ssh/ssh_host_rsa_key
```

```
Mounting device in preparation for zeroize...
```

```

Cleaning up target disk for zeroize ...
Zeroize done on target disk.
Zeroize of primary disk completed
Zeroize done
warning: Proceeding with vmhost reboot
Initiating vmhost reboot...

```

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

Enable FIPS Mode

The Security Administrator must establish a root password conforming to the FIPS password requirements in ["Configure Password Rules for an Authorized Administrator" on page 30](#). When the TOE's administrator enables FIPS mode in Junos OS on the device, they cannot configure passwords unless they meet this standard.

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

To enable FIPS mode in Junos OS on the device:

1. Zeroize the device to delete all CSPs before entering FIPS mode. Refer to ["Overview of Zeroization to Clear System Data for FIPS Mode" on page 24](#) section for details.
2. After the device comes up in 'Amnesiac mode', login using username root and password "" (blank).

```

FreeBSD/amd64 (Amnesiac) (ttyu0)
login: root
--- JUNOS 24.4R2.9 Kernel 64-bit  JNPR-15.0-20250529.3e76435_buil
root@TOE:~ # cli
root@TOE>

```

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

```

root@TOE > edit
Entering configuration mode
[edit]

```

```

root@TOE # set system root-authentication plain-text-password
New password:
Retype new password:
[edit]
root@TOE # commit
commit complete

```

4. Load configuration onto device and commit new configuration.
5. The fips-mode and jpf-fips are optional packages needed for enabling FIPS. These packages are part of Junos OS software. To enable these packages, use below commands:

```

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

```

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

```

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

```

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

```

[edit]
root@TOE # commit
[edit]
system reboot is required to transition to FIPS level 1
commit complete

```

8. Reboot the device:

```

[edit]
root@TOE # run request vmhost reboot

```

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

```

root@TOE:fips>

```

3

CHAPTER

Configure Administrative Credentials and Privileges

IN THIS CHAPTER

- Services Available Prior to Authentication | 30
 - Configure Password Rules for an Authorized Administrator | 30
 - Configure a Network Device Collaborative Protection Profile Authorized Administrator | 33
 - Configuring Network Time Protocol | 36
 - Customize Time in FIPS Mode | 37
 - Inactivity Timeout Period Configuration, and Local and Remote Idle Session Termination | 38
-

Services Available Prior to Authentication

The Junos OS in FIPS mode of operation allows a wide range of capabilities for users, and authentication is identity-based.

Prior to authentication, the only Junos OS managed responses provided to the administrator are:

- Display of the access banner
- ICMP echo responses (for remote management terminals).

Configure Password Rules for an Authorized Administrator

Ensure that the device is in FIPS mode before the TOE’s administrator configure the security administrator or any users. All passwords established for users by the security administrator must conform to Junos OS in FIPS mode requirements in [Table 4 on page 30](#). Attempts to configure passwords that do not conform to the following specifications result in an error.

Table 4: Password Specifications and Guidelines

Requirements	Details
Length	Passwords must contain at least 15 characters.
Character set	Passwords must contain at least three of the following five character sets: • Uppercase letters • Lowercase letters • Digits • Punctuation marks • Keyboard characters are not included in the other four sets. These characters are the percent sign (%) and the ampersand (&). NOTE: Avoid control characters in passwords.

Table 4: Password Specifications and Guidelines (Continued)

Requirements	Details
Password encryption	To change the default encryption method (SHA512), include the format statement at the [edit system login password] hierarchy level.

Configure Password Rules for an Authorized Administrator

Authentication data for fixed password authentication is a case-sensitive, value containing a combination of alphanumeric and the following special characters: "!", "@", "#", "\$", "%", "^", "&", "*", "(", ")", "?", "~", ",", ".", "/", ":", ";", "_", "+", "-", "=", "{", "}", "[", "]", "|", "<", ">", " ", "'", "\"", "\\", "`", "~". The password complexity requirements must be manually configured by the administrator through CLI using the set system login password configuration hierarchy as per the following specifications:

- Configure the minimum password length as a value within the range [6, 20] characters. The default value is 10 in FIPS mode if not explicitly configured. A minimum length of 15 characters is recommended when used in CC configuration.

[edit]

```
security-administrator@host:fips# set system login password minimum-length 15
```

- Password must be configured to contain at least one character from each of the character sets (uppercase, lowercase, numeric, and special characters):

[edit]

```
security-administrator@host:fips# set system login password minimum-upper-case 1
security-administrator@host:fips# set system login password minimum-lower-case 1
security-administrator@host:fips# set system login password minimum-numeric 1
security-administrator@host:fips# set system login password minimum-punctuations 1
```

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

[edit]

```
security-administrator@host:fips# set system login password format (sha256 | sha512)
```

- Commit the configuration:

[edit]

```
security-administrator@host:fips# commit
```



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

The new hash algorithm applies only to those passwords that are generated after committing this configuration.

Guidelines for Strong Passwords and Characteristics of Weak Passwords

Table 5 on page 32 summarizes the guidelines for strong passwords and the characteristics of weak passwords.

Table 5: Guidelines for Strong Passwords and Characteristics of Weak Passwords

Guidelines for Strong Passwords	Characteristics of Weak Passwords
The TOE's administrator can create strong and reusable passwords by using letters from a favorite phrase or word and concatenating these letters with unrelated words, digits, and punctuation marks.	Weak passwords typically exhibit several key characteristics that make the password easy to guess or crack, thereby compromising the security of an account or system. Avoid using the weak passwords.
Strong passwords are made up of alphanumeric characters and punctuation. For FIPS compliance, include at least one change of case, one or more digits, and one or more punctuation marks in the password.	Words that might be found in or exist as a permuted form in a system file such as <code>/etc/passwd</code> .

Table 5: Guidelines for Strong Passwords and Characteristics of Weak Passwords (Continued)

Guidelines for Strong Passwords	Characteristics of Weak Passwords
Strong passwords are easy to remember so that the TOE's administrator is not tempted to write it down.	The hostname of the system (always a first guess)
The TOE's administrator must change the passwords periodically	Any word or phrase that appears in a dictionary or a well-known source, including dictionaries and thesaurus in languages other than English; works by classical or popular writers; or common words and phrases from sports, sayings, movies, or television shows. Permutations of any words or phrases mentioned above. For example, a dictionary word with letters replaced with digits (r00t) or with digits added at the end of the word.
The TOE's administrator must not disclose the passwords to anyone To protect user credentials, the login system masks characters during password input, obscuring feedback effectively. This is the default behavior and requires no additional configuration.	Any machine-generated password. Algorithms reduce the search space of password-guessing programs, and the TOE's administrator must not use machine-generated password.

Configure a Network Device Collaborative Protection Profile Authorized Administrator

An account for root is always present in a configuration and is not intended for use in normal operation. In the evaluated configuration, the root account is restricted to the initial installation and configuration of the evaluated device.

An NDcPPv3.0e authorized administrator must have all permissions, including the ability to change the device configuration.

To configure an authorized administrator:

1. Create a login class named security-admin with all permissions.

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

2. Configure the hashed algorithm SHA256 or SHA512 for plain-text passwords. SHA512 is the default hashing algorithm.

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

3. Commit the changes.

```
[edit]
security-administrator@host:fps# commit
```

4. Define the NDcPPv3.0e user authorized administrator using the command below. The same command is used to change the password.

```
[edit]
security-administrator@host:fps# set system login user NDcPPv3-user class security-admin authentication encrypted-password
```

or

```
[edit]
security-administrator@host:fps# set system login user NDcPPv3-user class security-admin authentication plain-text-password
```

To configure public key authentication:

```
[edit]
security-administrator@host:fps# set system login user NDcPPv3-user class security-admin authentication ssh ecdsa <ecdsa-public-key>
security-administrator@host:fps# set system login user NDcPPv3-user class security-admin authentication ssh rsa <rsa-public-key>
```



NOTE: ssh-ed25519 is not supported in FIPS mode although it is shown as a configurable option.

To delete a configured login credential, use the following command:

[edit]

```
security-administrator@host:fips# delete system login user NDcPPv3-user class security-admin authentication
```

The set commands used to configure the credentials as shown above can be repeated to overwrite the currently configured credentials.

The Keyboard-Interactive Based authentication for SSH is supported by default and needs no additional configuration apart from a password being configured for the user. Providing multifactor authentication mechanism would require the use of an external AAA server, which is outside the CC scope, as a result of which the keyboard-interactive authentication method works similarly to the password-based method in the evaluated configuration.

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

[edit]

```
security-administrator@host:fips# set system services ssh log-key-changes
```



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

6. Commit the changes.

```
[edit]
security-administrator@host:fps# commit
```

For details on how to start with shell mode, see [Overview for Junos OS Guide](#).



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

Configuring Network Time Protocol

The device can be configured to sync with a Network Time Protocol (NTP) server. It supports time updates using NTP version 4. The device authenticates updates using an administrator-configured SHA-1 or SHA-256 key. The device rejects broadcast and multicast time updates by default without requiring any configuration. It does not place a limit on the number of NTP time sources that can be configured.

To configure the device in client mode, include the server statement and other statements at the `[edit system ntp]` hierarchy level:

```
[edit system ntp]
security-administrator@hostname:fps# server address key <key-number> version 4 prefer
security-administrator@hostname:fps# authentication-key <key-number> type sha1|sha256 value
<key value>
security-administrator@hostname:fps# trusted-key trusted <key-number>
```

The above commands specify the address of the system acting as the time server. One specifies an address, not a hostname. The same command can be used to configure multiple NTP servers.

It also configures the authentication key sent in all messages sent to the time server, using the key option. The key corresponds to the key number specified in the authentication-key statement. By default, the device sends NTP version 4 packets to the time server. If more than one time server is configured, one server can be marked as preferred by including the prefer option.

The following example shows how to configure the device to operate in client mode:

```
[edit system ntp]
security-administrator@hostname:fips# authentication-key 12 type sha256 value "$9$TQFn/
9t0OlcYwY4oGU9At"
security-administrator@hostname:fips# server 10.1.1.1 key 12 prefer
security-administrator@hostname:fips# trusted-key 12
```

By default, NTP operates in an entirely unauthenticated manner. If a malicious attempt to influence the accuracy of a router or switch's clock succeeds, it could have negative effects on system logging, make troubleshooting and intrusion detection more difficult, and impede other management functions.

For common criteria compliance, use trusted authentication using SHA1 or SHA256 as the message digest algorithm(s) to make sure that the NTP peer is trusted.

For IP version 4 (IPv4), one can specify the source address the TOE will use to access the network when it is sending NTP requests to the server.

To configure the specific source address that the request will always use, include the *source-address* statement at the [edit system ntp] hierarchy level. The source-address is a valid IP address configured on one of the router or switch interfaces.

```
[edit system ntp]
security-administrator@hostname:fips# set source-address source-address
```

For example:

```
[edit system ntp]
security-administrator@hostname:fips# set source-address 10.1.4.3
```

Customize Time in FIPS Mode

To customize time, disable NTP and then set the date and time.

1. Disable NTP from the configuration mode.

```
[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. Set the date and time from the operational mode. Date and time format is YYYYMMDDHHMM.ss.

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

Inactivity Timeout Period Configuration, and Local and Remote Idle Session Termination

IN THIS SECTION

- [Configure Session Termination | 38](#)
- [Sample Output for Local Administrative Session Termination | 40](#)
- [Sample Output for Remote Administrative Session Termination | 40](#)
- [Sample Output for User Initiated Termination | 41](#)

Inactivity timeout period configuration refers to the settings that determine how long your device wait while detecting no user activity before automatically log out and lock the session. This is a security feature.

Configure Session Termination

Terminate the session after the security administrator specifies inactive timeout period. The inactive timeout period applies to both local console sessions as well as the remote SSH sessions.

1. Set the idle timeout.

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

Specify the idle timeout period in minutes. The configurable idle timeout period range is 0 through 4294967295 minutes.

2. Configure the login access privileges.

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

3. Commit the configuration.

```
[edit]
security-administrator@host:fps# commit

commit complete
```

4. Set the password for the user.

```
[edit]
security-administrator@host:fps# set system login user NDcPPv3-user authentication plain-text-password
New password:
Retype new password:
```

5. Define login class for the user.

```
[edit]
security-administrator@host:fps# set system login user NDcPPv3-user class security-admin
```

6. Commit the configuration.

```
[edit]
security-administrator@host:fps# commit

commit complete
```

Sample Output for Local Administrative Session Termination

```

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

Type the hot key to suspend the connection: <CTRL>Z
FreeBSD/amd64 (host) (ttyu0)
login: NDcPPv3-user
Password:
Last login: Sun Nov 23 22:42:27 from 10.224.33.70

--- JUNOS 24.4R2.9 Kernel 64-bit JNPR-15.0-20250529.3e76435_buil
NDcPPv3-user@host> Warning: session will be closed in 1 minute if there is no activity
Warning: session will be closed in 10 seconds if there is no activity
Idle timeout exceeded: closing session

FreeBSD/amd64 (host) (ttyu0)

```

For password authentication (both remote and local), login interacts with a user to request a username and password to establish and verify the user's identity. The username entered by the administrator at the username prompt is reflected to the screen, but no feedback to screen is provided while the entry made by the administrator at the password prompt until the Enter key is pressed, following which either access to the CLI is provided (correct password) or the password prompt is presented again (incorrect password). This is the default behavior and does not require any configuration.



NOTE: Local console sessions display the banner FreeBSD/amd64 (hostname) (ttyu0) before the login prompt. This message is not shown during remote SSH access. Administrators should use this difference to verify whether the session is local or remote.

Sample Output for Remote Administrative Session Termination

```

ssh NDcPPv3-user@host
Password:
Last login: Sun Nov 23 22:48:05 2019

```

```

--- JUNOS 24.4R2.9 Kernel 64-bit JNPR-15.0-20250529.3e76435_buil
NDcPPv3-user@host> exit

Connection to host closed.
ssh NDcPPv3-user@host
Password:
Last login: Sun Nov 23 22:50:50 2019 from 10.224.33.70
--- JUNOS 24.4R2.9 Kernel 64-bit JNPR-15.0-20250529.3e76435_buil
NDcPPv3-user@host> Warning: session will be closed in 1 minute if there is no activity
Warning: session will be closed in 10 seconds if there is no activity
Idle timeout exceeded: closing session

Connection to host closed.

```

Sample Output for User Initiated Termination

Local console session and the remote SSH session users can use this method to terminate the session.

This is a LOGIN message from MX 240:
Authorized users only !!!

FreeBSD/amd64 (MX240) (ttyu0)

login: admin

Password:

Last login: Fri Feb 20 09:11:31 from 10.1.2.146

--- JUNOS 24.4R2-S2.2 Kernel 64-bit JNPR-15.0-20251006.0b8e28c_buil

admin@MX240:fips>

admin@MX240:fips>

admin@MX240:fips> exit

acumensec@TestVM3:~\$

acumensec@TestVM3:~\$ ssh [admin@10.1.2.80](#)

This is a LOGIN message for MX 240.

Authorized users only !!!

Password:

Last login: Fri Feb 20 09:11:21 2026 from 10.1.2.146

--- JUNOS 24.4R2-S2.2 Kernel 64-bit JNPR-15.0-20251006.0b8e28c_buil

admin@MX240:fips>

admin@MX240:fips>

admin@MX240:fips> exit

Connection to 10.1.2.80 closed.

acumensec@TestVM3:~\$

acumensec@TestVM3:~\$

acumensec@TestVM3:~\$

4

CHAPTER

Configure SSH and Console Connection

IN THIS CHAPTER

- [Configure System Login Message and Announcement | 43](#)
 - [Configure SSH on the Evaluated Configuration | 44](#)
 - [SSH Host Keys | 47](#)
 - [Limit the Number of User Login Attempts for SSH Sessions | 48](#)
-

Configure System Login Message and Announcement

A system login message appears before the user logs in and a system login announcement appears after the user logs in. By default, no login message or announcement is displayed on the device.

To configure a system login message for local console and SSH management interfaces, use the following command:

```
[edit]  
security-administrator@host:fps# set system login message login-message-banner-text
```

To configure system announcement, use the following command:

```
[edit]  
security-administrator@host:fps# set system login announcement system-announcement-text
```

Commit the configuration:

```
[edit]  
security-administrator@host:fps# commit
```



NOTE:

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

- \-Backslash

Configure SSH on the Evaluated Configuration

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

To configure SSH on the TOE:

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

[edit]

```
security-administrator@host:fips# set system services ssh hostkey-algorithm-list ecdsa-sha2-nistp256
```

```
security-administrator@host:fips# set system services ssh hostkey-algorithm-list ecdsa-sha2-nistp384
```

```
security-administrator@host:fips# set system services ssh hostkey-algorithm-list ecdsa-sha2-nistp521
```

```
security-administrator@host:fips# set system services ssh hostkey-algorithm-list rsa
```



NOTE: Although the last hostkey algorithm option mentioned above only mentions RSA, it covers all the claimed RSA algorithms, that is SSH-RSA, RSA-SHA2-256, and RSA-SHA2-512.

2. Specify the SSH key-exchange for Elliptic Curve 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-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
security-administrator@host:fips# set system services ssh ciphers aes128-gcm@openssh.com
security-administrator@host:fips# set system services ssh ciphers aes256-gcm@openssh.com
```

5. Commit the changes:

[edit]

```
security-administrator@host:fips# commit
```



NOTE: To disable SSH service, you can deactivate and commit the SSH configurations:

```
security-administrator@host:fips# deactivate system services ssh
```



NOTE: To disable Netconf service, you can deactivate and commit the netconf configurations:

```
security-administrator@host:fips# deactivate system services netconf ssh
```

Supported SSH host-key algorithm:

```
ecdsa-sha2-nistp256
ecdsa-sha2-nistp384
ecdsa-sha2-nistp521
rsa
```

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 MACs algorithm:

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

Supported SSH ciphers algorithm:

```
aes128-cbc          128-bit AES with Cipher Block Chaining
aes128-ctr          128-bit AES with Counter Mode
aes256-cbc          256-bit AES with Cipher Block Chaining
aes256-ctr          256-bit AES with Counter Mode
aes128-gcm@openssh.com 128-bit AES with Galois/Counter Mode
aes256-gcm@openssh.com 256-bit AES with Galois/Counter Mode
```

Sample output of Logging in via SSH (password):

```
This is a LOGIN message for MX 480. Authorized users only !!!  
  
FreeBSD/amd64 (MX480_TOE) (ttyu0)  
  
login: acumensec  
  
Password:  
  
Last login: Thu Sep 4 11:13:14 on ttyu0  
  
--- JUNOS 24.4R1.9 Kernel 64-bit JNPR-15.0-20241104.1ed86e6_buil  
acumensec@MX480_TOE:fips>
```

Sample output of Logging in via SSH (pubkey):

```
acumensec@mx480-1:~$ ssh tester@10.1.2.158 -i ~/.ssh/id_rsa_256  
  
This is a LOGIN message for MX 480.  
  
Authorized users only !!!  
  
Last login: Mon Sep 8 09:44:44 2025 from 10.1.5.84  
  
--- JUNOS 24.4R1.9 Kernel 64-bit JNPR-15.0-20241104.1ed86e6_buil  
  
tester@MX480_TOE:fips>
```

Sample output of Logging in via local authentication:

```
This is a LOGIN message for MX 480. Authorized users only !!!  
  
FreeBSD/amd64 (MX480_TOE) (ttyu0)  
  
login: acumensec  
  
Password:  
  
Last login: Thu Sep 4 11:13:14 on ttyu0  
  
--- JUNOS 24.4R1.9 Kernel 64-bit JNPR-15.0-20241104.1ed86e6_buil  
  
acumensec@MX480_TOE:fips>
```

SSH Host Keys

SUMMARY

Learn how to generate and delete SSH host keys.

IN THIS SECTION

- [Delete SSH Keys | 47](#)
- [Generate a New SSH Host Key | 47](#)

The TOE generates the SSH host keys automatically when it is in FIPS mode and reboot. The SSH host keys located in the following files:

- `/etc/ssh/fips_ssh_host_ecdsa_key`
- `/etc/ssh/fips_ssh_host_rsa_key`

Delete SSH Keys

If, for any reason, it becomes necessary to delete one or both of SSH host keys, issue the command from the shell prompt for the selected key.

```
rm /etc/ssh/<key-name>
```

Generate a New SSH Host Key

To generate a new SSH host key, issue one of the following commands from the shell prompt, selecting the appropriate key size:

- `ssh-keygen -t ecdsa -b [256|384|521] -f /etc/ssh/ssh_host_ecdsa_key`
- `ssh-keygen -t rsa -b [2048|3072|4096] -f /etc/ssh/ssh_host_rsa_key`

Limit the Number of User Login Attempts for SSH Sessions

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

The TOE's administrator configures the amount of time the device gets locked after failed attempts. The amount of time in minutes before the user can attempt to log in to the device after being locked out due to the number of failed login attempts specified in the `tries-before-disconnect` statement. When a user fails to correctly login after the number of allowed attempts specified by the `tries-before-disconnect` statement, the user must wait for the configured number of minutes before attempting to log in to the device again. During this lockout-period the remote session user still have access to the TOE through the console as the root user.

The lockout-period must be greater than zero. The range at which the TOE's administrator can configure the lockout-period is one through 43,200 minutes.

```
[edit system login]
security-administrator@host:fips# set retry-options lockout-period number
```

The TOE's administrator can configure the device to limit the number of attempts to enter a password while logging through SSH. Using the following command.

```
[edit system login]
security-administrator@host:fips# set retry-options tries-before-disconnect number
```

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

The local administrator's access will be maintained even if the remote administration is made permanently or temporarily unavailable due to the multiple failed login attempts. The console login for local administration will be available to the users during the lockout period.

The TOE's administrator can also configure a delay, in seconds, before a user can try to enter a password after a failed attempt.

```
[edit system login]
security-administrator@host:fips# set retry-options backoff-threshold number
```

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

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

```
[edit system login]
security-administrator@host:fips# set retry-options backoff-factor number
```

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

To unlock a locked user account, use the following command from operational mode:

```
security-administrator@host:fips> clear system login logout user username
```

An administrator uses the above command to manually unlock a user before their lockout period expires.

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

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

The SSH2 protocol provides secure terminal sessions utilizing secure encryption. The SSH2 protocol enforces running the key-exchange phase and changing the encryption and integrity keys for the session. Key exchange is done periodically, after specified seconds or after specified bytes of data have passed over the connection. The TSF ensures that within the SSH connections the same session keys

are used for a threshold of no longer than one hour, and no more than one gigabyte of the transmitted data. When either of the thresholds are reached, a rekey must be performed.

```
[edit system]
security-administrator@host:fips# set services ssh rekey time-limit number
```

Time limit before renegotiating session keys is 1 through 1440 minutes.

```
[edit system]
security-administrator@host:fips# set services ssh rekey data-limit number
```

Data limit before renegotiating session keys is 51200 through 4294967295 byte.



NOTE: If the SSH connection to the TOE is unintentionally broken, the administrator should verify both physical and logical connectivity to the TOE. Once connectivity is confirmed or restored, the administrator must manually re-initiate the SSH connection to log back into the TOE.

5

CHAPTER

Configure the Remote Syslog Server

IN THIS CHAPTER

- [Sample Syslog Server Configuration on a Linux System | 52](#)
-

Sample Syslog Server Configuration on a Linux System

A secure Junos OS environment requires auditing of events and storing them in a local audit file. The recorded events are simultaneously sent to an external syslog server. A syslog server receives the syslog messages streamed from the device. The syslog server must have an SSHv2 client with NETCONF 1.0 support configured to receive the streamed syslog messages. Junos OS supports NETCONF as defined by RFC6241 (NETCONF) and RFC6242 (Using NETCONF protocol over SSH).

Use the configuration details and establish a session between the target of evaluation (TOE) and the audit server. Examine the traffic that passes between the audit server and the TOE during several activities, and the generated audit data to be transferred to the audit server.

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

1. Generate an RSA public key on the remote syslog server. The TOE's administrator can also use ECDSA keys on the syslog server.

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

The TOE's administrator will be prompted to enter the desired pass phrase. The storage locations for the syslog-monitor key pair is displayed.

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

```
[edit system login]
security-administrator@host:fps# set class monitor permissions trace
```

3. Create a user named syslog-mon with the class monitor, and with public key-based or password-based authentication.

For public key-based authentication:

```
[edit system login]
security-administrator@host:fps# set user syslog-mon class monitor authentication ssh-rsa
"public-key"
```

For password-based authentication:

```
[edit system login]
security-administrator@host:fps# set user syslog-mon class monitor authentication (plain-
text-password | encrypted-password)
```

4. Set up NETCONF with SSH.

```
[edit system services]
security-administrator@host:fps# set netconf ssh
```

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

```
[edit system]
security-administrator@host:fps# set syslog file file-name any any
commit
```

6. To configure syslog in year format:

```
[edit system]
security-administrator@host:fps# syslog time-format year
commit
```

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

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

8. On the remote syslog server, add the *syslog-monitor* key pair to the *ssh-agent*.

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

The TOE's administrator will be prompted to enter the desired passphrase. Enter the same passphrase used in Step 1.

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

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

10. If the session becomes disconnected, first verify and restore physical and network connectivity with the syslog server. Then, repeat the command in Step 9 to re-establish the NETCONF connection.
11. After NETCONF is established, configure a system log events message stream. This RPC will cause the NETCONF service to start transmitting messages over the SSH connection that is established.


```
<rpc><get-syslog-events><stream>messages</stream></get-syslog-events></rpc>
```
12. The examples for syslog messages are listed below. Monitor the event log generated for admin actions on TOE are received on syslog server. Examine the traffic that passes between the audit server and the TOE, observing that these data are not viewed during this transfer, and that they are successfully received by the audit server. Match the logs between local event logging and remote event logged in syslog server and record the particular software (name, version) used on the audit server during testing.

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

```
root@host:~ #ssh-keygen -t ecdsa -f $HOME/.ssh/id_ssh_toby_ecdsa_521 -N "" -b 521
Generating public/private ecdsa key pair.
/root/.ssh/id_ssh_toby_ecdsa_521 already exists.
Overwrite (y/n)? Your identification has been saved in /root/.ssh/id_ssh_toby_ecdsa_521.
Your public key has been saved in /root/.ssh/id_ssh_toby_ecdsa_521.pub.
The key fingerprint is:
SHA256:QotJZkrdOAXn9VCpDc/2S1rF+KPJW239WfQhj9sEhVA root@host.englab.juniper.net
The key's randomart image is:
+---[ECDSA 521]---+
|  ..o o..o.E  |
|  . * ..O. . . |
|  . B + * . + . |
|  . = = .. = . + |
|  . o o S. . = ..|
|      .   + Bo+|
|      = =.+*|
|      . =.+.*|
|      .o o.|
+----[SHA256]-----+
[security-admin@TOE ~]# cat
$HOME/.ssh/id_ssh_toby_ecdsa_521.pub ecdsa-sha2-
nistp521
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAABmlzdHA1MjEAAACFBAC2+AZ7Gklc8Y9PZNZosY7vUnSR
```

```

Mxu5l3aXMtodhIYns66WwI7U/rjQsKosqwkvizep2wUtQ49DuQIXO0vc3mPNaa1DA== root@host.englab.juniper.net
[security-admin@TOE ~]# eval `ssh-agent -s`
Agent pid 5978
[security-admin@TOE ~]# ssh-add ~/.ssh/id_ssh_toby_ecdsa_521
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@          WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0755 for '/root/' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Identity added: .ssh/id_ssh_toby_ecdsa_521 (.ssh/id_ssh_toby_ecdsa_521)

```

Net configuration channel

```

root@host ~]# ssh syslog-mon@nms-mx10003-a -s netconf
<!-- No zombies were killed during the creation of this user interface -->
<!-- user syslog-mon, class j-super-user -->
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>urn:ietf:params:netconf:base:1.0</capability>
    <capability>urn:ietf:params:netconf:capability:candidate:1.0</capability>
    <capability>urn:ietf:params:netconf:capability:confirmed-commit:1.0</capability>
    <capability>urn:ietf:params:netconf:capability:validate:1.0</capability>
    <capability>urn:ietf:params:netconf:capability:url:1.0?scheme=http,ftp,file</capability>
    <capability>urn:ietf:params:xml:ns:netconf:base:1.0</capability>
    <capability>urn:ietf:params:xml:ns:netconf:capability:candidate:1.0</capability>
    <capability>urn:ietf:params:xml:ns:netconf:capability:confirmed-commit:1.0</capability>
    <capability>urn:ietf:params:xml:ns:netconf:capability:validate:1.0</capability>
    <capability>urn:ietf:params:xml:ns:netconf:capability:url:1.0?scheme=http,ftp,file</
  capability>
    <capability>urn:ietf:params:xml:ns:yang:ietf-yang-metadata?module=ietf-yang-
metadata&revision=2016-08-05</capability>
    <capability>urn:ietf:params:xml:ns:yang:ietf-netconf-monitoring</capability>
    <capability>http://xml.juniper.net/netconf/junos/1.0</capability>
    <capability>http://xml.juniper.net/dmi/system/1.0</capability>
    <capability>http://yang.juniper.net/junos/jcmd?module=junos-configuration-
metadata&revision=2021-09-01&...
  </capabilities>
  <session-id>80506</session-id>
</hello>
]]>]]>
<rpc><get-syslog-events><stream>messages</stream></get-syslog-events></rpc>

```

```
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns:junos="http://xml.juniper.net/
junos/26.1I-20251125_dev_common.0.1234/junos">
<syslog-events>
<syslog>
Dec 4 13:49:03 2025 nms-mx10003-a-test mgd[65827]: UI_COMMIT: User 'root' requested 'commit'
operation (comment: none)
</syslog>
<syslog>
Dec 4 13:49:03 2025 nms-mx10003-a-test ffp: "dynamic-profiles": No change to profiles
</syslog>
<syslog>
Dec 4 13:49:04 2025 nms-mx10003-a-test mgd[65827]: UI_CONFIGURATION_REVISION_UPDATED: New
database revision 're0-1764836343-29' and old database revision 're0-1764835976-28'
</syslog>
<syslog>
Dec 4 13:49:04 2025 nms-mx10003-a-test mgd[65827]: UI_COMMIT_COMPLETED: : commit complete
</syslog>
```

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

```
<190>1 2025-12-04T13:04:42.472+05:30 nms-mx10003-a-test mgd 72697 UI_AUTH_EVENT
[junos@2636.1.1.1.2.139 username="syslog-mon" authentication-level="j-super-user"] Authenticated
user 'syslog-mon' assigned to class 'j-super-user'
<190>1 2025-12-04T13:04:42.472+05:30 nms-mx10003-a-test mgd 72697 UI_LOGIN_EVENT
[junos@2636.1.1.1.2.139 username="syslog-mon" class-name="j-super-user" local-peer=""
pid="72697" ssh-connection="10.56.212.248 37647 10.209.6.136 22" client-mode="cli"] User 'syslog-
mon' login, class 'j-super-user' [72697], ssh-connection '10.56.212.248 37647 10.209.6.136 22',
client-mode 'cli'
```

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

Local:

```
<38>1 2025-12-04T14:41:44.514+05:30 nms-mx10003-a-test sshd 83264 - - Accepted publickey for
syslog-mon from 10.56.212.248 port 24927 ssh2: ECDSA SHA256:QotJZkrdOAXn9VCpDc/2S1rF
+KPJW239WfQhj9sEhVA
<190>1 2025-12-04T14:41:45.461+05:30 nms-mx10003-a-test mgd 83268 UI_AUTH_EVENT
[junos@2636.1.1.1.2.139 username="syslog-mon" authentication-level="j-super-user"] Authenticated
user 'syslog-mon' assigned to class 'j-super-user'
<190>1 2025-12-04T14:41:45.461+05:30 nms-mx10003-a-test mgd 83268 UI_LOGIN_EVENT
[junos@2636.1.1.1.2.139 username="syslog-mon" class-name="j-super-user" local-peer=""
pid="83268" ssh-connection="10.56.212.248 24927 10.209.6.136 22" client-mode="cli"] User 'syslog-
```

```

mon' login, class 'j-super-user' [83268], ssh-connection '10.56.212.248 24927 10.209.6.136 22',
client-mode 'cli'
<190>1 2025-12-04T14:41:47.549+05:30 nms-mx10003-a-test mgd 83268 UI_CMDLINE_READ_LINE
[junos@2636.1.1.1.2.139 username="syslog-mon" command="edit "] User 'syslog-mon', command 'edit '
<189>1 2025-12-04T14:41:47.550+05:30 nms-mx10003-a-test mgd 83268 UI_DBASE_LOGIN_EVENT
[junos@2636.1.1.1.2.139 username="syslog-mon"] User 'syslog-mon' entering configuration mode
<190>1 2025-12-04T14:41:51.753+05:30 nms-mx10003-a-test mgd 83268 UI_CMDLINE_READ_LINE
[junos@2636.1.1.1.2.139 username="syslog-mon" command="commit "] User 'syslog-mon', command
'commit '
<189>1 2025-12-04T14:41:51.754+05:30 nms-mx10003-a-test mgd 83268 UI_COMMIT
[junos@2636.1.1.1.2.139 username="syslog-mon" command="commit" message="none"] User 'syslog-mon'
requested 'commit' operation (comment: none)
<190>1 2025-12-04T14:42:50.331+05:30 nms-mx10003-a-test mgd 83251 UI_CMDLINE_READ_LINE
[junos@2636.1.1.1.2.139 username="root" command="show log abc | grep syslog-mon "] User 'root',
command 'show log abc | grep syslog-mon '

```

Remote:

```

root@host ~]# ssh syslog-mon@nms-mx10003-a -s netconf
<!-- No zombies were killed during the creation of this user interface -->
<!-- user syslog-mon, class j-super-user -->
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>urn:ietf:params:netconf:base:1.0</capability>
    <capability>urn:ietf:params:netconf:capability:candidate:1.0</capability>
    <capability>urn:ietf:params:netconf:capability:confirmed-commit:1.0</capability>
    <capability>urn:ietf:params:netconf:capability:validate:1.0</capability>
    <capability>urn:ietf:params:netconf:capability:url:1.0?scheme=http,ftp,file</capability>
    <capability>urn:ietf:params:xml:ns:netconf:base:1.0</capability>
    <capability>urn:ietf:params:xml:ns:netconf:capability:candidate:1.0</capability>
    <capability>urn:ietf:params:xml:ns:netconf:capability:confirmed-commit:1.0</capability>
    <capability>urn:ietf:params:xml:ns:netconf:capability:validate:1.0</capability>
    <capability>urn:ietf:params:xml:ns:netconf:capability:url:1.0?scheme=http,ftp,file</
  capability>
    <capability>urn:ietf:params:xml:ns:yang:ietf-yang-metadata?module=ietf-yang-
  metadata&revision=2016-08-05</capability>
    <capability>urn:ietf:params:xml:ns:yang:ietf-netconf-monitoring</capability>
    <capability>http://xml.juniper.net/netconf/junos/1.0</capability>
    <capability>http://xml.juniper.net/dmi/system/1.0</capability>
    <capability>http://yang.juniper.net/junos/jcmd?module=junos-configuration-
  metadata&revision=2021-09-01&...
  </capabilities>

```

```

    <session-id>80506</session-id>
  </hello>
]]>]]>
<rpc><get-syslog-events><stream>messages</stream></get-syslog-events></rpc>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns:junos="http://xml.juniper.net/
junos/26.1I-20251125_dev_common.0.1234/junos">
  <syslog-events>
    <syslog>
      Dec 4 13:49:03 2025 nms-mx10003-a-test mgd[65827]: UI_COMMIT: User 'syslog-mon' requested
      'commit' operation (comment: none)
    </syslog>
    <syslog>
      Dec 4 13:49:03 2025 nms-mx10003-a-test ffp: "dynamic-profiles": No change to profiles
    </syslog>
    <syslog>
      Dec 4 13:49:04 2025 nms-mx10003-a-test mgd[65827]: UI_CONFIGURATION_REVISION_UPDATED: New
      database revision 're0-1764836343-29' and old database revision 're0-1764835976-28'
    </syslog>
    <syslog>
      Dec 4 13:49:04 2025 nms-mx10003-a-test mgd[65827]: UI_COMMIT_COMPLETED: : commit complete
    </syslog>
  </syslog-events>
</rpc-reply>

```

6

CHAPTER

Configure Audit Log Options

IN THIS CHAPTER

- [Configure Audit Log Options in FIPS Mode](#) | 60
-

Configure Audit Log Options in FIPS Mode

SUMMARY

Learn to configure audit log options in FIPS mode.

IN THIS SECTION

- [Configure Audit Log Options on Device in FIPS Mode | 60](#)
- [Junos OS Log File Management and Storage Behavior | 61](#)
- [Sample Code Audits of Configuration Changes | 62](#)

The syslog functionality on MX and EX starts up during the system bootup. The syslog service cannot be started or stopped by user configuration.

The local logs are automatically overwritten according to configurable limits on storage volume. The default maximum size is 1 MB, which can be modified by the user, using the “size” argument for the “set system syslog file <filename> archive” CLI command.

The Junos OS defines an active log file and a number of “archive” files (10 by default, but configurable from 1 to 1000). When the active log file reaches its maximum size, the logging utility closes the file, compresses it, and names the compressed archive file ‘logfile.0.gz’. The logging utility then opens and writes to a new active log file. When the new active log file reaches the configured maximum size ‘logfile.0.gz’ is renamed ‘logfile.1.gz’, and the active log file is closed, compressed, and renamed ‘logfile.0.gz’. When the maximum number of archive files is reached and when the size of the active file reaches the configured maximum size, the contents of the oldest archived file are deleted so the current active file can be archived.

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

Configure Audit Log Options on Device in FIPS Mode

Only authenticated administrators are authorized to delete locally stored audit data.

To configure audit log options:

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

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

2. Specify the file in which to log data.

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

- Specify the size of files, in bytes, to be archived. Note: The size can also be specified in shorthand form, for example, `10m` for 10 MB and `1g` for 1 GB.

```
[edit system syslog]
security-administrator@host:fps# set file syslog archive size 10000000
```

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

```
[edit system syslog]
security-administrator@host:fps# set file syslog explicit-priority
```

- Log system messages in a structured format.

```
[edit system syslog]
security-administrator@host:fps# set file syslog structured-data
```

If 'structured-data' option is configured, the year field is included in the audit log messages.

- Commit the changes:

```
[edit]
security-administrator@host:fps# commit
```

- View the local audit data

```
[edit]
security-administrator@host:fps# show log syslog
```

- Clear the local audit data

```
[edit]
security-administrator@host:fps# clear log syslog
```

Junos OS Log File Management and Storage Behavior

IN THIS SECTION

- Storage Management for Syslog Files | 62
- Storage Exhaustion Management | 62

The Junos OS maintains logs through active log file and a set of archived log files (10 files by default, but configurable 1 through 1000 files). When the active file log reaches its maximum file size (1 GB by default, but configurable 65536 to 1073741824 bytes, that is 64 KB to 1 GB), the logging utility performs the following steps:

1. Archiving the Active File:

- When the active log file reaches its maximum size the logging utility:
 - Closes and compresses the log file
 - Saves the file as logfile.0.gz.
 - Creates an active log file for ongoing logging.

2. Managing Older Archives:

- When the new active file log reaches the maximum size, the existing logfile.0.gz is renamed to logfile.1.gz.
- The current active log file is then closed, compressed, and renamed to logfile.0.gz.

3. Managing Archive Limits:

- When the maximum number of archived files is reached and the active log file reaches its size limit, the oldest archived file is deleted.
- This ensures space for the newest archive file while maintaining the configured number of backups.

Storage Management for Syslog Files

A 1 GB syslog file takes approximately 0.25 GB of storage when archived. Syslog files can consume all allocated storage in to /var file, which is platform specific.

When the filesystem reaches 92% storage capacity an event is raised to the administrator. However, the event process continues using the reserved storage blocks to ensure uninterrupted logging till the administrator frees the storage.

Storage Exhaustion Management

When the /var file storage exhausted, the system logs a final entry reporting No space left on device and terminates the logging. The appliance continues to operate in the event of exhaustion of audit log storage space.

Sample Code Audits of Configuration Changes

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

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

```

    }
}

```

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

```

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

```

Example: The System Logging of Configuration Changes

This example shows a sample configuration and makes changes to users and secret data. It then shows the information sent to the audit server when the secret data is added to the original configuration and committed with the load command.

```

[edit system]
location {
    country-code US;
    building B1;
}
...
login {
    message "UNAUTHORIZED USE OF THIS ROUTER\n\tIS STRICTLY PROHIBITED!";
    user admin {
        uid 2000;
        class super-user;
        authentication {
            encrypted-password "$ABC123";
            # SECRET-DATA
        }
    }
}
radius-server 192.0.2.15 {

```

```

    secret "$ABC123" # SECRET-DATA
}
services {
    ssh;
}
syslog {
    user *{
        any emergency;
    }
    file messages {
        any notice;
        authorization info;
    }
    file interactive-commands {
        interactive-commands any;
    }
}
...
...

```

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

```

security-administrator@host:fips# show | compare
[edit system login user admin authentication]
-   encrypted-password "$ABC123"; # SECRET-DATA
+   encrypted-password "$ABC123"; # SECRET-DATA
[edit system login]
+   user admin2 {
+       uid 2001;
+       class operator;
+       authentication {
+           encrypted-password "$ABC123";
+           # SECRET-DATA
+       }
+   }
[edit system radius-server 192.0.2.15]
-   secret "$ABC123"; # SECRET-DATA
+   secret "$ABC123"; # SECRET-DATA

```

7

CHAPTER

Configure Event Logging

IN THIS CHAPTER

- [Event Logging Overview | 66](#)
 - [Interpret Event Messages | 103](#)
 - [Log Changes to Secret Data | 104](#)
 - [Login and Logout Events Using SSH | 105](#)
 - [Logging of Audit Startup | 105](#)
-

Event Logging Overview

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

In addition, Junos OS can:

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

The logging for the evaluated configuration must capture the events. The logging events are listed below:

[Table 6 on page 67](#) shows sample for syslog auditing for NDcPPv3.0e:

Table 6: Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
FAU_GEN.1	None	None	- Start-up and shut-down of the audit functions; Note: There is no manual startup/shutdown of the local audit function, which is tied to startup/shutdown of the TOE itself, logs for which implicitly indicate the audit function stopping and starting as well. TOE Shutdown: <pre><45>1 2025-07-04T23:12:32.753Z MX480_TOE eventd 20463 SYSTEM_SHUTDOWN [junos@2636.1.1.1.2.25 type="shutdown" username="admin" time="Fri Jul 4 23:08:54 2025" message="no message"] System shutdown by admin at Fri Jul 4 23:08:54 2025: no message</pre> TOE Startup: <pre><45>1 2025-07-04T23:12:32.754Z MX480_TOE eventd 20463 SYSTEM_OPERATIONAL - System is operational</pre> - All auditable events for the not specified level of audit; - All administrative actions comprising: - Administrative login and logout (name of Administrator account shall be logged if individual accounts are required for Administrators). Login: <pre><38>1 2025-07-09T12:06:43.690Z MX480_TOE sshd 23064 - - Accepted keyboard-interactive/pam for acumensec from 10.1.5.84 port 35624 ssh2</pre> <pre><190>1 2025-07-09T12:06:43.780Z MX480_TOE mgd 23070 UI_AUTH_EVENT [junos@2636.1.1.1.2.25 username="acumensec" authentication-level="j- security-admin"] Authenticated user 'acumensec' assigned to class 'j-security-admin'</pre>

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
			<190>1 2025-07-09T12:06:43.780Z MX480_TOE mgd 23070 UI_LOGIN_EVENT [junos@2636.1.1.1.2.25 username="acumensec" class-name="j-security-admin" local-peer="" pid="23070" ssh-connection="10.1.5.84 35624 10.1.2.158 22" client-mode="cli"] User 'acumensec' login, class 'j-security-admin' [23070], ssh-connection '10.1.5.84 35624 10.1.2.158 22', client-mode 'cli' Logout <38>1 2025-07-09T12:08:55.986Z MX480_TOE sshd 23068 - - Received disconnect from 10.1.5.84 port 35624:11: disconnected by user <38>1 2025-07-09T12:08:55.986Z MX480_TOE sshd 23068 - - Disconnected from user acumensec 10.1.5.84 port 35624 - Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed). <182>1 2025-07-09T11:11:54.326Z MX480_TOE mgd 22519 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.25 username="admin" action="set" pathname="[system syslog file audit_file any\]" delimiter="" data="unconfigured" value="any"] User 'admin' set: [system syslog file audit_file any] unconfigured -- "any" <190>1 2025-07-09T11:11:54.326Z MX480_TOE mgd 22519 UI_CMDLINE_READ_LINE [junos@2636.1.1.1.2.25 username="admin" command="set system syslog file audit_file any any "] User 'admin', command 'set system syslog file audit_file any any ' - Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
			Generation of cryptographic keys (SSH): <pre><190>1 2026-04-30T09:27:37.676Z MX480_TOE csh 77709 - - UI_SHELL_READ_LINE: User 'acumensec', command 'ssh-keygen '</pre> <pre><38>1 2026-04-30T09:27:45.183Z MX480_TOE ssh- keygen 77711 - - Generated SSH key file /var/home/acumensec/.ssh/id_rsa.pub with fingerprint SHA256:LjNI2dWDZXupxW5Nrvn/9Rhykd5sCFUrZcU osrDIsv4</pre> Import of cryptographic keys (SSH): <pre><182>1 2025-08-12T10:54:36.309Z MX480_TOE mgd 21496 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.25 username="admin" action="set" pathname="[system login user cctester authentication ssh-rsa /* SECRET-DATA */\]" delimiter="" value=""] User 'admin' set: [system login user cctester authentication ssh-rsa /* SECRET-DATA */]</pre> <pre><190>1 2025-08-12T10:54:36.309Z MX480_TOE mgd 21496 UI_CMDLINE_READ_LINE [junos@2636.1.1.1.2.25 username="admin" command="set system login user cctester authentication ssh-rsa /* SECRET-DATA */ "] User 'admin', command 'set system login user cctester authentication ssh-rsa /* SECRET-DATA */ ' Deletion of cryptographic keys (SSH):</pre> <pre><190>1 2025-08-12T10:57:13.866Z MX480_TOE mgd 21496 UI_CMDLINE_READ_LINE [junos@2636.1.1.1.2.25 username="admin" command="delete system login user cctester authentication ssh-rsa /* SECRET-DATA */ "] User 'admin', command 'delete system login user cctester authentication ssh-rsa /* SECRET-DATA */ ' <182>1 2025-08-12T10:57:13.866Z MX480_TOE mgd 21496 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.25 username="admin" action="delete" pathname="[system login user cctester authentication ssh-rsa /* SECRET-DATA */\]" delimiter="" value=""] User 'admin' delete: [system login user cctester authentication ssh-rsa /* SECRET- DATA */]</pre> • [Resetting passwords (name of related

			Administrator account shall be logged));
--	--	--	--

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
			**NOTE: The logs mention data="unconfigured" as the old value even when resetting an existing password to mask the sensitive information. <pre> <182>1 2025-07-09T12:39:20.230Z MX480_TOE mgd 22148 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.25 username="admin" action="set" pathname="[system login user cctester authentication\]" delimiter="" data="unconfigured" value="plain-text-password"] User 'admin' set: [system login user cctester authentication] unconfigured -- "plain-text-password" <190>1 2025-07-09T12:39:32.340Z MX480_TOE mgd 22148 UI_CMDLINE_READ_LINE [junos@2636.1.1.1.2.25 username="admin" command="set system login user cctester authentication plain-text-password "] User 'admin', command 'set system login user cctester authentication plain-text-password ' </pre>
FAU_GEN.2	None	None	
FAU_STG_EXT.1	Configuration of local audit settings.	Identity of account making changes to the audit configuration.	Configuration of local audit settings. <pre> <182>1 2025-07-09T11:11:54.326Z MX480_TOE mgd 22519 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.25 username="admin" action="set" pathname="[system syslog file audit_file any\]" delimiter="" data="unconfigured" value="any"] User 'admin' set: [system syslog file audit_file any] unconfigured -- "any" <190>1 2025-07-09T11:11:54.326Z MX480_TOE mgd 22519 UI_CMDLINE_READ_LINE [junos@2636.1.1.1.2.25 username="admin" command="set system syslog file audit_file any any "] User 'admin', command 'set system syslog file audit_file any any ' </pre>

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
FCS_CKM.1	None	None	
FCS_CKM.2	None	None	
FCS_CKM.4	None	None	
FCS_COP.1/ DataEncryption	None	None	
FCS_COP.1/ SigGen	None	None	
FCS_COP.1/ Hash	None	None	
FCS_COP.1/ KeyedHash	None	None	
FCS_RBG_EXT.1	None	None	
FCS_MACSEC_ EXT.1	Session establishment	Secure Channel Identifier (SCI)	<30>1 2025-09-17T14:19:21.580Z MX240 secure-dot1xd 23083 DOT1XD_MKA_SECURE_CHANNEL_CREATED [junos@2636.1.1.1.2.29 mac-address="7c:25:86:ab:28:40" interface-name="ge-0/0/0"] Macsec receive secure channel created for 7c:25:86:ab:28:40 on interface ge-0/0/0 <28>1 2025-09-17T14:19:31.043Z MX240 secure-dot1xd 23083 DOT1XD_MACSEC_SC_CAK_ACTIVATED [junos@2636.1.1.1.2.29 interface-name="ge-0/0/0" sc-id0="5800BB0A680C0001" sc-id1="7C2586AB28400001" pre-shared-key="1234567890"] ifd: ge-0/0/0 sci-out:5800BB0A680C0001 sci-in:7C2586AB28400001 ckn: 1234567890

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
FCS_MACSEC_EXT.3	Creation and update of SAK	Creation and update times	Creation of SAK: <pre><30>1 2025-10-14T11:24:42.053Z MX240 secure-dot1xd 21596 DOT1XD_MKA_SECURE_CHANNEL_CREATED [junos@2636.1.1.1.2.29 mac-address="7c:25:86:ab:28:40" interface-name="ge-0/0/0"] Macsec receive secure channel created for 7c:25:86:ab:28:40 on interface ge-0/0/0</pre> Update of SAK: <pre><30>1 2025-09-29T13:26:29.994Z MX240 secure-dot1xd 23083 DOT1XD_MKA_SAK_REKEY_EVENT [junos@2636.1.1.1.2.29 interface-name="ge-0/0/0"] MKA sak-rekey event started for the interface: ge-0/0/0</pre> <pre><30>1 2025-09-29T13:26:29.994Z MX240 secure-dot1xd 23083 DOT1XD_MKA_SA_KEY_ROLLOVER [junos@2636.1.1.1.2.29 interface-name="ge-0/0/0"] Macsec secure association key rolled over on interface ge-0/0/0</pre>

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
FCS_MACSEC_EXT.4	Creation of CA	Connectivity Association Key Names (CKNs)	<30>1 2025-10-14T11:24:42.053Z MX240 secure-dot1xd 21596 DOT1XD_MKA_SECURE_CHANNEL_CREATED [junos@2636.1.1.1.2.29 mac-address="7c:25:86:ab:28:40" interface-name="ge-0/0/0"] Macsec receive secure channel created for 7c:25:86:ab:28:40 on interface ge-0/0/0 <30>1 2025-10-14T11:24:42.601Z MX240 secure-dot1xd 21596 DOT1XD_MKA_SECURE_ASSOCIATION_ESTABLISHED [junos@2636.1.1.1.2.29 sequence-number="0" interface-name="ge-0/0/0"] Macsec secure association established with an:0 on interface ge-0/0/0 <28>1 2025-10-14T11:24:42.601Z MX240 secure-dot1xd 21596 DOT1XD_MACSEC_SC_PRIMARY_CAK_IN_USE [junos@2636.1.1.1.2.29 interface-name="ge-0/0/0" pre-shared-key="ABCDEF0123456789ABCDEF0123456789"] ifd: ge-0/0/0 primary ckn: ABCDEF0123456789ABCDEF0123456789 is in-use <28>1 2025-10-14T11:24:48.281Z MX240 secure-dot1xd 21596 DOT1XD_MACSEC_SC_CAK_ACTIVATED [junos@2636.1.1.1.2.29 interface-name="ge-0/0/0" sc-id0="5800BB0A680C0001" sc-id1="7C2586AB28400001" pre-shared-key="ABCDEF0123456789ABCDEF0123456789"] ifd: ge-0/0/0 sci-out:5800BB0A680C0001 sci-in:7C2586AB28400001 ckn: ABCDEF0123456789ABCDEF0123456789
FCS_RBG_EXT.1	None	None	

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
FCS_SSH_EXT.1	Failure to establish SSH connection	Reason for failure and Non-TOE endpoint of attempted connection (IP Address)	Failure to establish SSH connection Unsupported cipher <38>1 2025-08-12T11:53:11.090Z MX480_TOE sshd 30530 - - Unable to negotiate with 10.1.2.65 port 49874: no matching cipher found. Their offer: aes192-ctr [preauth] Unsupported hashing algorithm <38>1 2025-08-12T12:03:26.860Z MX480_TOE sshd 24607 - - Unable to negotiate with 10.1.2.65 port 55976: no matching MAC found. Their offer: hmac-md5 [preauth] Unsupported key exchange method <38>1 2025-08-12T12:05:48.942Z MX480_TOE sshd 24672 - - Unable to negotiate with 10.1.2.65 port 59712: no matching key exchange method found. Their offer: diffie-hellman-group14-sha1,ext-info-c,kex-strict-c-v00@openssh.com [preauth]

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
	Establishment of SSH connection	Non-TOE endpoint of attempted connection (IP Address)	Establishment of SSH connection <pre><38>1 2025-07-09T12:06:43.690Z MX480_TOE sshd 23064 - - Accepted keyboard-interactive/pam for acumensec from 10.1.5.84 port 35624 ssh2</pre> <pre><190>1 2025-07-09T12:06:43.780Z MX480_TOE mgd 23070 UI_AUTH_EVENT [junos@2636.1.1.1.2.25 username="acumensec" authentication-level="j-security-admin"] Authenticated user 'acumensec' assigned to class 'j-security-admin'</pre> <pre><190>1 2025-07-09T12:06:43.780Z MX480_TOE mgd 23070 UI_LOGIN_EVENT [junos@2636.1.1.1.2.25 username="acumensec" class-name="j-security-admin" local-peer="" pid="23070" ssh-connection="10.1.5.84 35624 10.1.2.158 22" client-mode="cli"] User 'acumensec' login, class 'j-security-admin' [23070], ssh-connection '10.1.5.84 35624 10.1.2.158 22', client-mode 'cli'</pre>
	Termination of SSH connection session	Non-TOE endpoint of attempted connection (IP Address)	Termination of SSH connection session <pre><38>1 2025-07-09T12:08:55.986Z MX480_TOE sshd 23068 - - Received disconnect from 10.1.5.84 port 35624:11: disconnected by user</pre> <pre><38>1 2025-07-09T12:08:55.986Z MX480_TOE sshd 23068 - - Disconnected from user acumensec 10.1.5.84 port 35624</pre>

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
	Dropping of packet(s) outside defined size limits	Packet Size	<38>1 2025-09-30T11:01:46.335Z MX480_TOE sshd 65440 - - Accepted password for admin from 10.1.5.84 port 44272 ssh2 <38>1 2025-09-30T11:01:46.339Z MX480_TOE sshd 65442 - - Potential replay attack detected on SSH connection initiated from 10.1.5.84:44272 <37>1 2025-09-30T11:01:46.339Z MX480_TOE sshd - SSH_MSG_REPLAY_DETECT [junos@2636.1.1.1.2.25 source-address="10.1.5.84" source-port="44272"] Potential replay attack detected on SSH connection initiated from 10.1.5.84:44272 <38>1 2025-09-30T11:01:46.340Z MX480_TOE sshd 65442 - - Bad packet length 262145. <28>1 2025-09-30T11:01:46.341Z MX480_TOE inetd 21046 - - /usr/sbin/sshd[65440]: exited, status 255
FCS_SSHS_EXT.1	No events specified	None	None

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
FCS_NTP_EXT.1	- Configuration of a new time server - Removal of configured time server	Identity of new/removed time server	- Configuration of a new time server <pre><182>1 2025-07-24T10:41:28.618Z MX480_TOE mgd 21755 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.25 username="admin" action="set" pathname="[system ntp server 10.1.5.84\]" delimiter="" value=""] User 'admin' set: [system ntp server 10.1.5.84]</pre> <pre><182>1 2025-07-24T10:41:28.618Z MX480_TOE mgd 21755 UI_CFG_AUDIT_SET_SECRET [junos@2636.1.1.1.2.25 username="admin" action="set" pathname="[system ntp server 10.1.5.84 key\]" User 'admin' set: [system ntp server 10.1.5.84 key]</pre> <pre><182>1 2025-07-24T10:41:28.618Z MX480_TOE mgd 21755 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.25 username="admin" action="set" pathname="[system ntp server 10.1.5.84 version\]" delimiter="" data="unconfigured" value="4"] User 'admin' set: [system ntp server 10.1.5.84 version] unconfigured -- "4"</pre> <pre><190>1 2025-07-24T10:41:28.618Z MX480_TOE mgd 21755 UI_CMDLINE_READ_LINE [junos@2636.1.1.1.2.25 username="admin" command="set system ntp server 10.1.5.84 key /* SECRET-DATA */ version 4 "] User 'admin', command 'set system ntp server 10.1.5.84 key /* SECRET-DATA */ version 4 '</pre> - Removal of configured time server <pre><190>1 2025-07-24T10:43:05.455Z MX480_TOE mgd 21755 UI_CMDLINE_READ_LINE [junos@2636.1.1.1.2.25 username="admin" command="delete system ntp server 10.1.5.84 "] User 'admin', command 'delete system ntp server 10.1.5.84 '</pre>

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
			<182>1 2025-07-24T10:43:05.455Z MX480_TOE mgd 21755 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.25 username="admin" action="delete" pathname="[system ntp server 10.1.5.84\]" delimiter="" value=""] User 'admin' delete: [system ntp server 10.1.5.84]

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
FIA_UIA_EXT.1	All use of identification and authentication mechanism	Origin of the attempt (e.g., IP address)	All use of identification and authentication mechanism Local Successful Login <37>1 2025-07-11T16:17:50.080Z MX480_TOE login 76412 - - Login attempt for user acumensec from host [unknown] <38>1 2025-07-11T16:17:53.680Z MX480_TOE login 76412 LOGIN_INFORMATION [junos@2636.1.1.1.2.25 username="acumensec" hostname="[unknown\]" tty-name="ttyu0"] User acumensec logged in from host [unknown] on device ttyu0 <190>1 2025-07-11T16:17:53.726Z MX480_TOE mgd 76415 UI_AUTH_EVENT [junos@2636.1.1.1.2.25 username="acumensec" authentication-level="j-security-admin"] Authenticated user 'acumensec' assigned to class 'j-security-admin' <190>1 2025-07-11T16:17:53.726Z MX480_TOE mgd 76415 UI_LOGIN_EVENT [junos@2636.1.1.1.2.25 username="acumensec" class-name="j-security-admin" local-peer="" pid="76415" ssh-connection="" client-mode="cli"] User 'acumensec' login, class 'j-security-admin' [76415], ssh-connection "", client-mode 'cli' Local Unsuccessful Login <37>1 2025-07-11T16:05:45.358Z MX480_TOE login 75983 - - Login attempt for user acumensec from host [unknown] <35>1 2025-07-11T16:05:46.548Z MX480_TOE login 75983 PAM_UNIX_LOC_PASSWD_AUTH [junos@2636.1.1.1.2.25 username="acumensec" result="failed"] local password authentication of user 'acumensec' failed

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
			<35>1 2025-07-11T16:05:46.549Z MX480_TOE login 75983 LOGIN_PAM_AUTHENTICATION_ERROR [junos@2636.1.1.1.2.25 username="acumensec"] Failed password for user acumensec <37>1 2025-07-11T16:05:46.549Z MX480_TOE login 75983 LOGIN_FAILED [junos@2636.1.1.1.2.25 username="acumensec" source-address="ttyu0"] Login failed for user acumensec from host ttyu0 Remote Successful Password-Based Login <38>1 2025-08-04T11:00:37.144Z MX480_TOE sshd 86747 - - Accepted password for acumensec from 10.1.5.84 port 36318 ssh2 <190>1 2025-08-04T11:00:37.235Z MX480_TOE mgd 86751 UI_AUTH_EVENT [junos@2636.1.1.1.2.25 username="acumensec" authentication-level="j-security-admin"] Authenticated user 'acumensec' assigned to class 'j-security-admin' <190>1 2025-08-04T11:00:37.235Z MX480_TOE mgd 86751 UI_LOGIN_EVENT [junos@2636.1.1.1.2.25 username="acumensec" class-name="j-security-admin" local-peer="" pid="86751" ssh-connection="10.1.5.84 36318 10.1.2.158 22" client-mode="cli"] User 'acumensec' login, class 'j-security-admin' [86751], ssh-connection '10.1.5.84 36318 10.1.2.158 22', client-mode 'cli' Remote Unsuccessful Password-Based Login <35>1 2025-07-11T16:39:14.888Z MX480_TOE sshd - PAM_UNIX_LOC_PASSWD_AUTH [junos@2636.1.1.1.2.25 username="acumensec" result="failed"] local password authentication of user 'acumensec' failed <15>1 2025-07-11T16:39:14.888Z MX480_TOE sshd - PAM_USER_LOCK_USER [junos@2636.1.1.1.2.25 event-function-name="pam_sm_authenticate"

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
			username="acumensec"] (pam_sm_authenticate): DEBUG: PAM_USER: acumensec <15>1 2025-07-11T16:39:14.889Z MX480_TOE sshd - PAM_USER_LOCK_UPD_LOCK_ATTEMPTS [junos@2636.1.1.1.2.25 event-function- name="pam_sm_authenticate" username="acumensec" num-msgs-forward="1"] (pam_sm_authenticate): DEBUG: Updating lock-attempts of user: acumensec attempts: 1 <35>1 2025-07-11T16:39:14.889Z MX480_TOE sshd 77211 - - error: PAM: Authentication error for acumensec from 10.1.5.84 <37>1 2025-07-11T16:39:14.890Z MX480_TOE sshd - SSHD_LOGIN_FAILED [junos@2636.1.1.1.2.25 username="acumensec" source-address="10.1.5.84"] Login failed for user 'acumensec' from host '10.1.5.84' Remote Successful Public Key-Based Login <38>1 2025-07-14T20:06:49.571Z MX480_TOE sshd 40869 - - Accepted publickey for admin from 10.1.5.84 port 39202 ssh2: RSA SHA256:z1HjGXyPNrVziK39ieCsdzP99cDVXpZIMvPt uAiTrps <190>1 2025-07-14T20:06:49.680Z MX480_TOE mgd 40873 UI_AUTH_EVENT [junos@2636.1.1.1.2.25 username="admin" authentication-level="j-security- admin"] Authenticated user 'admin' assigned to class 'j- security-admin' <190>1 2025-07-14T20:06:49.680Z MX480_TOE mgd 40873 UI_LOGIN_EVENT [junos@2636.1.1.1.2.25 username="admin" class- name="j-security-admin" local-peer="" pid="40873" ssh-connection="10.1.5.84 39202 10.1.2.158 22" client-mode="cli"] User 'admin' login, class 'j-security- admin' [40873], ssh-connection '10.1.5.84 39202 10.1.2.158 22', client-mode 'cli'

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
			Remote Unsuccessful Public Key-Based Login <pre><38>1 2025-09-04T09:44:20.435Z MX480_TOE sshd 93275 - - Connection closed by authenticating user tester 10.1.5.84 port 55022 [preauth]</pre> <pre><28>1 2025-09-04T09:44:20.436Z MX480_TOE inetd 20984 - - /usr/sbin/sshd[93275]: exited, status 255</pre>

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded	Origin of the attempt (e.g., IP address)	Unsuccessful login attempts limit is met or exceeded Aug 15 18:05:17 2025 MX480_TOE sshd[94713]: error: PAM: Authentication error for tester from 10.1.5.84 Aug 15 18:05:17 2025 MX480_TOE sshd: SSHD_LOGIN_FAILED: Login failed for user 'tester' from host '10.1.5.84' Aug 15 18:05:18 2025 MX480_TOE sshd[94713]: error: PAM: Authentication error for tester from 10.1.5.84 Aug 15 18:05:18 2025 MX480_TOE sshd: SSHD_LOGIN_FAILED: Login failed for user 'tester' from host '10.1.5.84' Aug 15 18:05:25 2025 MX480_TOE sshd: LIBJNX_LOGIN_ACCOUNT_LOCKED: Account for user 'tester' has been locked out from logins Aug 15 18:05:25 2025 MX480_TOE sshd: PAM_USER_LOCK_LOGIN_REQUESTS_DENIED: Login requests from host '10.1.5.84' are denied Aug 15 18:05:25 2025 MX480_TOE sshd[94713]: error: PAM: Authentication error for tester from 10.1.5.84 Aug 15 18:05:25 2025 MX480_TOE sshd: SSHD_LOGIN_FAILED: Login failed for user 'tester' from host '10.1.5.84' Aug 15 18:05:40 2025 MX480_TOE sshd: SSHD_LOGIN_ATTEMPTS_THRESHOLD: Threshold for unsuccessful authentication attempts (3) reached by user 'tester' Aug 15 18:05:40 2025 MX480_TOE sshd[94713]: Disconnecting authenticating user tester 10.1.5.84 port 48596: Too many password failures for tester [preauth]

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
			Aug 15 18:05:40 2025 MX480_TOE sshd[94714]: Disconnecting authenticating user tester 10.1.5.84 port 48596: Too many password failures for tester Aug 15 18:05:40 2025 MX480_TOE inetd[23345]: /usr/sbin/sshd[94713]: exited, status 255
FIA_PMG_EXT.1	None	None	
FIA_UAU.7	None	None	
FMT_MOF.1/ ManualUpdate	Any attempt to initiate a manual update	None	Any attempt to initiate a manual update <190>1 2025-08-11T05:41:24.812Z MX480_TOE mgd 49536 UI_CHILD_START [junos@2636.1.1.1.2.25 command="/usr/libexec/ui/package"] Starting child '/usr/libexec/ui/package' <29>1 2025-08-11T05:41:24.814Z MX480_TOE mgd 49536 - - /usr/libexec/ui/package -X update /var/tmp/junos-vmhost-install-mx-x86-64-24.4R1.9.tgz
FMT_MOF.1/ Functions	None	None	
FMT_MOF.1/ Services	None	None	
FMT_MTD.1/ CoreData	None	None	
FMT_MTD.1/ CryptoKeys	None	None	

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
FMT_SMF.1	All management activities of TSF data.	None	Ability to administer the TOE remotely <pre><38>1 2025-07-09T12:06:43.690Z MX480_TOE sshd 23064 - - Accepted keyboard-interactive/pam for acumensec from 10.1.5.84 port 35624 ssh2</pre> <190>1 2025-07-09T12:06:43.780Z MX480_TOE mgd 23070 UI_AUTH_EVENT [junos@2636.1.1.1.2.25 username="acumensec" authentication-level="j- security-admin"] Authenticated user 'acumensec' assigned to class 'j-security-admin' <190>1 2025-07-09T12:06:43.780Z MX480_TOE mgd 23070 UI_LOGIN_EVENT [junos@2636.1.1.1.2.25 username="acumensec" class- name="j-security-admin" local-peer="" pid="23070" ssh-connection="10.1.5.84 35624 10.1.2.158 22" client-mode="cli"] User 'acumensec' login, class 'j- security-admin' [23070], ssh-connection '10.1.5.84 35624 10.1.2.158 22', client-mode 'cli' Ability to configure the access banner <pre><182>1 2025-08-04T05:48:50.806Z MX480_TOE mgd 69167 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.25 username="admin" action="set" pathname="[system login message\]" delimiter="" data="unconfigured" value="This is a LOGIN message for MX 480.\nAuthorized users only !!!"] User 'admin' set: [system login message] unconfigured -- "This is a LOGIN message for MX 480.\nAuthorized users only !!!"</pre> <190>1 2025-08-04T05:48:50.806Z MX480_TOE mgd 69167 UI_CMDLINE_READ_LINE [junos@2636.1.1.1.2.25 username="admin" command="set system login message \"This is a LOGIN messagefor MX 480.\nAuthorized users only !!!\" "] User 'admin', command 'set system login message "This is a LOGIN message for MX 480.\nAuthorized users only !!!" '

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
			Ability to configure the remote session inactivity time before session termination <pre><182>1 2025-08-04T10:35:29.803Z MX480_TOE mgd 71233 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.25 username="admin" action="set" pathname="[system login class security- admin idle-timeout\]" delimiter="" data="unconfigured" value="1"] User 'admin' set: [system login class security-admin idle-timeout] unconfigured -- "1"</pre> <pre><190>1 2025-08-04T10:35:29.804Z MX480_TOE mgd 71233 UI_CMDLINE_READ_LINE [junos@2636.1.1.1.2.25 username="admin" command="set system login class security-admin idle- timeout 1 "] User 'admin', command 'set system login class security-admin idle-timeout 1 '</pre> Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates <pre><190>1 2025-08-11T05:41:24.812Z MX480_TOE mgd 49536 UI_CHILD_START [junos@2636.1.1.1.2.25 command="/usr/libexec/ui/package"] Starting child '/usr/libexec/ui/package'</pre> <pre><29>1 2025-08-11T05:41:24.814Z MX480_TOE mgd 49536 - - /usr/libexec/ui/package -X update /var/tmp/ junos-vmhost-install-mx-x86-64-24.4R1.9.tgz</pre> <pre><190>1 2025-08-11T05:48:16.808Z MX480_TOE mgd 49536 UI_CHILD_STATUS [junos@2636.1.1.1.2.25 command="/usr/libexec/ui/ package" pid="71662" status-code="0"] Cleanup child '/usr/libexec/ui/package', PID 71662, status 0</pre> <pre><118>1 2025-08-11T05:57:17.200Z MX480_TOE kernel - - - Verified os-kernel-prd-x86-64-20241104 signed by PackageProductionECP256_2024 method ECDSA256+SHA256</pre>

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
			<118>1 2025-08-11T05:57:17.200Z MX480_TOE kernel - - - Verified os-libs-15-x86-64-20241104 signed by PackageProductionECP256_2024 method ECDSA256+SHA256 <118>1 2025-08-11T05:57:17.200Z MX480_TOE kernel - - - Verified os-runtime-x86-64-20241104 signed by PackageProductionECP256_2024 method ECDSA256+SHA256 <118>1 2025-08-11T05:57:17.200Z MX480_TOE kernel - - - Verified os-package-20241014 signed by Package ProductionECP256_2024 method ECDSA256+SHA256 Ability to start and stop services Starting services <182>1 2025-10-09T09:32:27.377Z MX480_TOE mgd 12714 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.25 username="admin" action="set" pathname="[system services netconf ssh \]" delimiter="" value=""] User 'admin' set: [system services netconf ssh] <190>1 2025-10-09T09:32:27.377Z MX480_TOE mgd 12714 UI_CMDLINE_READ_LINE [junos@2636.1.1.1.2.25 username="admin" command="set system services netconf ssh "] User 'admin', command 'set system services netconf ssh ' Stopping services <190>1 2025-10-09T09:34:59.262Z MX480_TOE mgd 12714 UI_CMDLINE_READ_LINE [junos@2636.1.1.1.2.25 username="admin" command="delete system services netconf ssh "] User 'admin', command 'delete system services netconf ssh ' <182>1 2025-10-09T09:34:59.262Z MX480_TOE mgd 12714 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.25 username="admin"

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
			action="delete" pathname="[system services netconf ssh\]" delimiter="" value="" User 'admin' delete: [system services netconf ssh] Ability to configure local audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full, changes to local audit storage size) <182>1 2025-07-14T09:48:54.261Z MX480_TOE mgd 57387 UI_CFG_AUDIT_SET [junos@263 6.1.1.1.2.25 username="admin" action="set" pathname="[system syslog file syslog archive size\]" delimiter="" data="10m" value="11m"] User 'admin' set: [system syslog file syslog archive size] "10m -- "11m" <190>1 2025-07-14T09:48:54.261Z MX480_TOE mgd 57387 UI_CMDLINE_READ_LINE [junos @2636.1.1.1.2.25 username="admin" command="set system syslog file syslog archive size 11m "] User 'admin', command 'set system syslog file syslog archive size 11m ' Ability to modify the behaviour of the transmission of audit data to an external IT entity <182>1 2025-10-09T09:32:27.377Z MX480_TOE mgd 12714 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.25 username="admin" action="set" pathname="[system services netconf ssh\]" delimiter="" value=""] User 'admin' set: [system services netconf ssh] <190>1 2025-10-09T09:32:27.377Z MX480_TOE mgd 12714 UI_CMDLINE_READ_LINE [junos@2636.1.1.1.2.25 username="admin" command="set system services netconf ssh "] User 'admin', command 'set system services netconf ssh ' Ability to manage the cryptographic keys

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
			<182>1 2025-08-12T10:54:36.309Z MX480_TOE mgd 21496 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.25 username="admin" action="set" pathname="[system login user cctester authentication ssh-rsa /* SECRET-DATA */]" delimiter="" value=""] User 'admin' set: [system login user cctester authentication ssh-rsa /* SECRET-DATA */] <190>1 2025-08-12T10:54:36.309Z MX480_TOE mgd 21496 UI_CMDLINE_READ_LINE [junos@2636.1.1.1.2.25 username="admin" command="set system login user cctester authentication ssh-rsa /* SECRET-DATA */ "] User 'admin', command 'set system login user cctester authentication ssh-rsa /* SECRET-DATA */ ' Ability to configure thresholds for SSH rekeying <182>1 2025-10-09T09:25:56.067Z MX480_TOE mgd 12714 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.25 username="admin" action="set" pathname="[system services ssh rekey time-limit\]" delimiter="" data="unconfigured" value="60"] User 'admin' set: [system services ssh rekey time-limit] unconfigured -- "60" <190>1 2025-10-09T09:25:56.067Z MX480_TOE mgd 12714 UI_CMDLINE_READ_LINE [junos@2636.1.1.1.2.25 username="admin" command="set system services ssh rekey time-limit 60 "] User 'admin', command 'set system services ssh rekey time-limit 60 ' <182>1 2025-10-09T09:26:20.131Z MX480_TOE mgd 12714 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.25 username="admin" action="set" pathname="[system services ssh rekey data-limit\]" delimiter="" data="unconfigured" value="15m"] User 'admin' set: [system services ssh rekey data-limit] unconfigured -- "15m"

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
			<190>1 2025-10-09T09:26:20.131Z MX480_TOE mgd 12714 UI_CMDLINE_READ_LINE [junos@2636.1.1.1.2.25 username="admin" command="set system services ssh rekey data-limit 15m "] User 'admin', command 'set system services ssh rekey data-limit 15m ' Ability to re-enable an Administrator account <190>1 2025-10-09T09:20:21.480Z MX480_TOE mgd 12714 UI_CMDLINE_READ_LINE [junos@2636.1.1.1.2.25 username="admin" command="clear system login lockout user acumensec "] User 'admin', command 'clear system login lockout user acumensec ' <37>1 2025-10-09T09:20:21.481Z MX480_TOE mgd 12714 LIBJNX_LOGIN_ACCOUNT_UNLOCKED [junos@2636.1.1.1.2.25 username="acumensec"] Account for user 'acumensec' has been unlocked for logins Ability to configure the local session inactivity time before session termination or locking <182>1 2025-08-04T10:35:29.803Z MX480_TOE mgd 71233 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.25 username="admin" action="set" pathname="[system login class security-admin idle-timeout\]" delimiter="" data="unconfigured" value="1"] User 'admin' set: [system login class security-admin idle-timeout] unconfigured -- "1" <190>1 2025-08-04T10:35:29.804Z MX480_TOE mgd 71233 UI_CMDLINE_READ_LINE [junos@2636.1.1.1.2.25 username="admin" command="set system login class security-admin idle-timeout 1 "] User 'admin', command 'set system login class security-admin idle-timeout 1 ' Ability to configure the authentication failure parameters for FIA_AFL.1

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
			<182>1 2025-10-09T09:11:05.287Z MX480_TOE mgd 12714 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.25 username="admin" action="set" pathname="[system login retry-options tries-before-disconnect\]" delimiter="" data="3" value="3"] User 'admin' set: [system login retry-options tries-before-disconnect] "3 -- "3" <190>1 2025-10-09T09:11:05.288Z MX480_TOE mgd 12714 UI_CMDLINE_READ_LINE [junos@2636.1.1.1.2.25 username="admin" command="set system login retry-options tries-before- disconnect 3 "] User 'admin', command 'set system login retry-options tries-before-disconnect 3 ' <182>1 2025-10-09T09:11:23.622Z MX480_TOE mgd 12714 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.25 username="admin" action="set" pathname="[system login retry-options lockout-period\]" delimiter="" data="5" value="5"] User 'admin' set: [system login retry-options lockout- period] "5 -- "5" <190>1 2025-10-09T09:11:23.622Z MX480_TOE mgd 12714 UI_CMDLINE_READ_LINE [junos@2636.1.1.1.2.25 username="admin" command="set system login retry-options lockout- period 5 "] User 'admin', command 'set system login retry-options lockout-period 5 ' Ability to set the time which is used for time-stamps <190>1 2025-08-06T06:59:31.596Z MX480_TOE mgd 87699 UI_CMDLINE_READ_LINE [junos@2636.1.1.1.2.25 username="admin" command="set date 202601010808.08 "] User 'admin', command 'set date 202601010808.08 ' <190>1 2025-08-06T06:59:31.598Z MX480_TOE mgd 87699 UI_CHILD_START [junos@2636.1.1.1.2.25 command="/bin/date"] Starting child '/bin/date'

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
			<37>1 2026-01-01T08:08:08.000Z MX480_TOE date 88447 - - date set by root <190>1 2026-01-01T08:08:08.000Z MX480_TOE mgd 87699 UI_CHILD_STATUS [junos@2636.1.1.1.2.25 command="/bin/date" pid="88447" status-code="0"] Cleanup child '/bin/date', PID 88447, status 0 Ability to configure NTP <182>1 2025-07-24T10:41:28.618Z MX480_TOE mgd 21755 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.25 username="admin" action="set" pathname="[system ntp server 10.1.5.84\]" delimiter="" value=""] User 'admin' set: [system ntp server 10.1.5.84] <182>1 2025-07-24T10:41:28.618Z MX480_TOE mgd 21755 UI_CFG_AUDIT_SET_SECRET [junos@2636.1.1.1.2.25 username="admin" action="set" pathname="[system ntp server 10.1.5.84 key\]" User 'admin' set: [system ntp server 10.1.5.84 key] <182>1 2025-07-24T10:41:28.618Z MX480_TOE mgd 21755 UI_CFG_AUDIT_SET [junos@2636.1.1.1.2.25 username="admin" action="set" pathname="[system ntp server 10.1.5.84 version\]" delimiter="" data="unconfigured" value="4"] User 'admin' set: [system ntp server 10.1.5.84 version] unconfigured -- "4" <190>1 2025-07-24T10:41:28.618Z MX480_TOE mgd 21755 UI_CMDLINE_READ_LINE [junos@2636.1.1.1.2.25 username="admin" command="set system ntp server 10.1.5.84 key /* SECRET-DATA */ version 4 "] User 'admin', command 'set system ntp server 10.1.5.84 key /* SECRET-DATA */ version 4 '

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
			Ability to administer the TOE locally<37>1 2025-08-04T10:45:23.451Z MX480_TOE login 86118 - - Login attempt for user acumensec from host [unknown] <38>1 2025-08-04T10:45:27.602Z MX480_TOE login 86118 LOGIN_INFORMATION [junos@2636.1.1.1.2.25 username="acumensec" hostname="[unknown\]" tty-name="ttyu0"] User acumensec logged in from host [unknown] on device ttyu0 <190>1 2025-08-04T10:45:27.646Z MX480_TOE mgd 86163 UI_AUTH_EVENT [junos@2636.1.1.1.2.25 username="acumensec" authentication-level="j-security-admin"] Authenticated user 'acumensec' assigned to class 'j-security-admin' <190>1 2025-08-04T10:45:27.646Z MX480_TOE mgd 86163 UI_LOGIN_EVENT [junos@2636.1.1.1.2.25 username="acumensec" class-name="j-security-admin" local-peer="" pid="86163" ssh-connection="" client-mode="cli"] User 'acumensec' login, class 'j-security-admin' [86163], ssh-connection "", client-mode 'cli' Ability to manage the trusted public keys database <182>1 2025-10-09T08:56:48.726Z MX480_TOE mgd 12101 UI_CFG_AUDIT_OTHER [junos@2636.1.1.1.2.25 username="admin" action="set" pathname="[system login user cctester authentication ssh-rsa /* SECRET-DATA */]" delimiter="" value=""] User 'admin' set: [system login user cctester authentication ssh-rsa /* SECRET-DATA */] <190>1 2025-10-09T08:56:48.726Z MX480_TOE mgd 12101 UI_CMDLINE_READ_LINE [junos@2636.1.1.1.2.25 username="admin" command="set system login user cctester authentication ssh-rsa /* SECRET-DATA */"] User

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
			'admin', command 'set system login user cctester authentication ssh-rsa /* SECRET-DATA */ '
FMT_SMR.2	None	None	
FPT_RPL.1	Detected replay attempt	None	<27>1 2025-10-17T12:24:14.040Z MX240 secure-dot1xd 24097 DOT1XD_MKA_DUPLICATE_OR_DELAYED_PDU_DE TEC TED [junos@2636.1.1.1.2.29 cak- type="PRIMARY" mka-actor="0" interface- name="ge-0/0/0"] MKA PRIMARY actor #0 received duplicate or delayed PDU on interface: ge-0/0/0
FPT_SKP_EXT.1	None	None	
FPT_APW_EXT.1	None	None	
FPT_TST_EXT.1	None	None	

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
FPT_TUD_EXT. 1	Initiation of update; result of the update attempt (success or failure)	None	Initiation of update; result of the update attempt (success or failure) <pre><190>1 2025-08-11T05:41:24.812Z MX480_TOE mgd 49536 UI_CHILD_START [junos@2636.1.1.1.2.25 command="/usr/libexec/ui/package"] Starting child '/usr/libexec/ui/package'</pre> <pre><29>1 2025-08-11T05:41:24.814Z MX480_TOE mgd 49536 - - /usr/libexec/ui/package -X update /var/tmp/ junos-vmhost-install-mx-x86-64-24.4R1.9.tgz</pre> result of the update attempt (success or failure) - Success ** NOTE: status-code of "0", states that the upgrade had been successful** <pre><190>1 2025-08-11T05:41:24.812Z MX480_TOE mgd 49536 UI_CHILD_START [junos@2636.1.1.1.2.25 command="/usr/libexec/ui/package"] Starting child '/usr/libexec/ui/package'</pre> <pre><29>1 2025-08-11T05:41:24.814Z MX480_TOE mgd 49536 - - /usr/libexec/ui/package -X update /var/tmp/ junos-vmhost-install-mx-x86-64-24.4R1.9.tgz</pre> <pre><190>1 2025-08-11T05:48:16.808Z MX480_TOE mgd 49536 UI_CHILD_STATUS [junos@2636.1.1.1.2.25 command="/usr/libexec/ui/ package" pid="71662" status-code="0"] Cleanup child '/usr/libexec/ui/package', PID 71662, status 0</pre> - failure ** NOTE: status-code other than "0", states that the upgrade has failed** <pre><190>1 2025-08-20T05:55:26.865Z MX480_TOE mgd 81904 UI_CHILD_START [junos@2636.1.1.1.2.25 command="/opt/support/vmhost-pkg-support"] Starting child '/opt/support/vmhost-pkg-support'</pre>

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
			<29>1 2025-08-20T05:55:26.867Z MX480_TOE mgd 81904 - - /opt/support/vmhost-pkg-support - c /var/tmp/junos-vmhost-install-mx-x86-64-24.4R1.9_modified.tgz <190>1 2025-08-20T05:56:50.618Z MX480_TOE mgd 81904 UI_CHILD_STATUS [junos@2636.1.1.1.2.25 command="/opt/support/vmhost-pkg-support" pid="82345" status-code="256"] Cleanup child '/opt/support/vmhost-pkg-support', PID 82345, status 0x100 <29>1 2025-08-20T05:56:50.618Z MX480_TOE mgd 81904 UI_CHILD_EXITED [junos@2636.1.1.1.2.25 pid="82345" return-value="1" core-dump-status="" command="/opt/support/vmhost-pkg-support"] Child exited: PID 82345, status 1, command '/opt/support/vmhost-pkg-support'

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
FPT_STM_EXT. 1	Discontinuous changes to time - either Administrator actuated or changed via an automated process	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).	Discontinuous changes to time - either Administrator actuated or changed via an automated process Admin changed time: <pre><190>1 2025-08-06T06:59:31.596Z MX480_TOE mgd 87699 UI_CMDLINE_READ_LINE [junos@2636.1.1.1.2.25 username="admin" command="set date 202601010808.08 "] User 'admin', command 'set date 202601010808.08 '</pre> <pre><190>1 2025-08-06T06:59:31.598Z MX480_TOE mgd 87699 UI_CHILD_START [junos@2636.1.1.1.2.25 command="/bin/date"] Starting child '/bin/date'</pre> <pre><37>1 2026-01-01T08:08:08.000Z MX480_TOE date 88447 - - date set by root</pre> <pre><190>1 2026-01-01T08:08:08.000Z MX480_TOE mgd 87699 UI_CHILD_STATUS [junos@2636.1.1.1.2.25 command="/bin/date" pid="88447" status-code="0"] Cleanup child '/bin/ date', PID 88447, status 0</pre> Time change using NTP: <pre><102>1 2025-11-07T04:29:55.044Z MX480_TOE xntpd 67284 - - kernel reports TIME_ERROR: 0x41: Clock Unsynchronized</pre> <pre><102>1 2025-11-07T04:29:55.044Z MX480_TOE xntpd 67284 - - kernel reports TIME_ERROR: 0x41: Clock Unsynchronized</pre> <pre><103>1 2025-11-07T04:29:55.893Z MX480_TOE xntpd 67284 - - 1 7 0 32 32</pre> <pre><103>1 2025-11-07T04:29:57.895Z MX480_TOE xntpd 67284 - - 1 7 0 32 32</pre> <pre><103>1 2025-11-07T04:29:59.895Z MX480_TOE xntpd 67284 - - 1 7 0 32 32</pre>

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
			<pre> <103>1 2025-11-07T04:30:01.898Z MX480_TOE xntpd 67284 - - 1 7 0 32 32 <14>1 2025-11-07T07:05:24.906Z MX480_TOE xntpd - NTPD_CHANGED_TIME [junos@2636.1.1.1.2.25 rate="9323.007043"] time reset +9323.007043 s <101>1 2025-11-07T07:05:24.906Z MX480_TOE xntpd 67284 - - ntpd: time reset +9323.007043 s admin@MX480_TOE:fips> show ntp associations remote refid auth st t when poll reach delay offset jitter rootdelay rootdisp ===== ===== ===== *10.1.5.97 96.231.54.40 SKEY 2 u 22 64 3 0.451 -0.113 0.139 8.362 27.054 admin@MX480_TOE:fips> </pre>

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
FTA_SSL.3	The termination of a remote session by the session locking mechanism	None	The termination of a remote session by the session locking mechanism <pre><14>1 2025-08-04T11:48:37.181Z MX480_TOE -cli - UI_CLI_IDLE_TIMEOUT [junos@2636.1.1.1.2.25 username="acumensec"] Idle timeout for user 'acumensec' exceeded and session terminated</pre> <pre><190>1 2025-08-04T11:48:37.181Z MX480_TOE mgd 89124 UI_LOGOUT_EVENT [junos@2636.1.1.1.2.25 username="acumensec"] User 'acumensec' logout</pre> <pre><38>1 2025-08-04T11:48:37.183Z MX480_TOE sshd 89122 - - Received disconnect from 10.1.5.84 port 50294:11: disconnected by user</pre> <pre><38>1 2025-08-04T11:48:37.183Z MX480_TOE sshd 89122 - - Disconnected from user acumensec 10.1.5.84 port 50294</pre>
FTA_SSL.4	The termination of an interactive session	None	The termination of an interactive session <pre><190>1 2025-08-04T09:45:46.370Z MX480_TOE mgd 83269 UI_CMDLINE_READ_LINE [junos@2636.1.1.1.2.25 username="acumensec" command="exit "] User 'acumensec', command 'exit '</pre> <pre><190>1 2025-08-04T09:45:46.370Z MX480_TOE mgd 83269 UI_LOGOUT_EVENT [junos@2636.1.1.1.2.25 username="acumensec"] User 'acumensec' logout</pre>

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
FTA_SSL_EXT.1 (if “terminate the session” is selected)	The termination of a local session by the session locking mechanism	None	The termination of a local session by the session locking mechanism <14>1 2025-08-04T10:46:32.246Z MX480_TOE -cli - UI_CLI_IDLE_TIMEOUT [junos@2636.1.1.1.2.25 username="acumensec"] Idle timeout for user 'acumensec' exceeded and session terminated <190>1 2025-08-04T10:46:32.247Z MX480_TOE mgd 86163 UI_LOGOUT_EVENT [junos@2636.1.1.1.2.25 username="acumensec"] User 'acumensec' logout
FTA_TAB.1	None	None	

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
FTP_ITC.1	- Initiation of the trusted channel. - Termination of the trusted channel. - Failure of the trusted channel functions.	- None - None - Reason for failure	- Initiation of the trusted channel. <pre><38>1 2025-10-09T08:21:56.548Z MX480_TOE sshd 11107 - - Accepted publickey for syslog-mon from 10.1.5.84 port 49514 ssh2: ECDSA SHA256:nh0jpMNtA7wsC1Cti+f/VEFD8CjkZvsn+Qi1UDwt7LM</pre> <pre><190>1 2025-10-09T08:21:56.640Z MX480_TOE mgd 11111 UI_AUTH_EVENT [junos@2636.1.1.1.2.25 username="syslog-mon" authentication-level="j-monitor"] Authenticated user 'syslog-mon' assigned to class 'j-monitor'</pre> <pre><190>1 2025-10-09T08:21:56.641Z MX480_TOE mgd 11111 UI_LOGIN_EVENT [junos@2636.1.1.1.2.25 username="syslog-mon" class-name="j-monitor" local-peer="" pid="11111" ssh-connection="10.1.5.84 49514 10.1.2.158 22" client-mode="cli"] User 'syslog-mon' login, class 'j-monitor' [11111], ssh-connection '10.1.5.84 49514 10.1.2.158 22', client-mode 'cli'</pre> - Termination of the trusted channel. <pre><30>1 2025-10-09T08:27:14.238Z MX480_TOE mgd 11110 UI_NETCONF_MONITORING_DELETE [junos@2636.1.1.1.2.25 message="11110"] Netconf session with pid '11110' is being deleted</pre> <pre><190>1 2025-10-09T08:27:14.247Z MX480_TOE mgd 11110 UI_LOGOUT_EVENT [junos@2636.1.1.1.2.25 username="syslog-mon"] User 'syslog-mon' logout</pre> - Failure of the trusted channel functions. <pre><38>1 2025-10-09T08:36:32.385Z MX480_TOE sshd 11646 - - Unable to negotiate with 10.1.5.84 port 47950: no matching MAC found. Their offer: hmac-md5 [preauth]</pre>

Table 6: Auditable Events (Continued)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Records
FTP_TRP.1/ Admin	- Initiation of the trusted path. - Termination of the trusted path. - Failure of the trusted path functions.	- None - None - Reason for failure	- Initiation of the trusted path. <pre><38>1 2025-07-09T12:06:43.690Z MX480_TOE sshd 23064 - - Accepted keyboard-interactive/pam for acumensec from 10.1.5.84 port 35624 ssh2</pre> <pre><190>1 2025-07-09T12:06:43.780Z MX480_TOE mgd 23070 UI_AUTH_EVENT [junos@2636.1.1.1.2.25 username="acumensec" authentication-level="j- security-admin"] Authenticated user 'acumensec' assigned to class 'j-security-admin'</pre> <pre><190>1 2025-07-09T12:06:43.780Z MX480_TOE mgd 23070 UI_LOGIN_EVENT [junos@2636.1.1.1.2.25 username="acumensec" class- name="j-security-admin" local-peer="" pid="23070" ssh-connection="10.1.5.84 35624 10.1.2.158 22" client-mode="cli"] User 'acumensec' login, class 'j- security-admin' [23070], ssh-connection '10.1.5.84 35624 10.1.2.158 22', client-mode 'cli'</pre> - Termination of the trusted path. <pre><38>1 2025-07-09T12:08:55.986Z MX480_TOE sshd 23068 - - Received disconnect from 10.1.5.84 port 35624:11: disconnected by user</pre> <pre><38>1 2025-07-09T12:08:55.986Z MX480_TOE sshd 23068 - - Disconnected from user acumensec 10.1.5.84 port 35624</pre> - Failure of the trusted path functions. <pre><38>1 2025-08-12T11:53:11.090Z MX480_TOE sshd 30530 - - Unable to negotiate with 10.1.2.65 port 49874: no matching cipher found. Their offer: aes192- ctr [preauth]</pre>

In addition, Juniper Networks recommends:

- To capture all changes to the configuration.

- To store logging information remotely.

For more information on log details, see [Specifying Log File Size, Number, and Archiving Properties](#)

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 7 on page 103](#) 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 7: Fields in Event Messages

Field	Description	Examples
<i>timestamp</i>	Time when the message was generated, in one of two representations: • <i>MMM-DD HH:MM:SS.MS+/-HH:MM</i>, is the month, day, hour, minute, second and millisecond in local time. The hour and minute that follows the plus sign (+) or minus sign (-) is the offset of the local time zone from Coordinated Universal Time (UTC). • <i>YYYY-MM-DDTHH:MM:SS.MSZ</i> is the year, month, day, hour, minute, second and millisecond in UTC.	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.
<i>hostname</i>	Name of the host that originally generated the message.	router1
<i>process</i>	Name of the Junos OS process that generated the message.	mgd

Table 7: Fields in Event Messages (Continued)

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

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
```

RELATED DOCUMENTATION

[Interpret Event Messages](#) | 103

Logging of Audit Startup

The audit information logged includes startups of Junos OS. This in turn identifies the startup events of the audit system, which cannot be independently disabled or enabled. For example, if Junos OS is restarted, the audit log contains the following information:

```
Dec 20 23:17:35 bilbo syslogd: exiting on signal 14
Dec 20 23:17:35 bilbo syslogd: restart
Dec 20 23:17:35 bilbo syslogd /kernel: Dec 20 23:17:35 init: syslogd (PID 19128) exited with
status=1
```

```
Dec 20 23:17:42 bilbo /kernel:  
Dec 20 23:17:53 init: syslogd (PID 19200) started
```

RELATED DOCUMENTATION

[Login and Logout Events Using SSH](#) | 105

8

CHAPTER

Configure MACsec

IN THIS CHAPTER

- Media Access Control Security (MACsec) in FIPS Mode Overview | 108
 - Configure MACsec | 110
-

Media Access Control Security (MACsec) in FIPS Mode Overview

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 the TOE's administrator 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.

- AES-CMAC - Advanced Encryption Standard-Cipher-based Message Authentication Code
- AES-ECB - Advanced Encryption Standard-Electronic Codebook
- AES-KEYWRAP - Advanced Encryption Standard-Key Wrapping algorithm
- KBKDF - Key Based Key Derivation Function

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

```
security-administrator@host:fips# prompt security macsec connectivity-association ca_name pre-shared-key cak
```

New cak (secret):
 Retype new cak (secret):

```
security-administrator@host:fps# 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.

To delete an existing CAK, use the following command:

```
security-administrator@host:fps# delete security macsec connectivity association ca_name pre-  
shared-key cak
```

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 is a 64-digit hexadecimal number and the CAK is a 32-digit hexadecimal number. The CKN and CAK must match on both ends of a link to create a MACsec-secured link.

When a 128-bit cipher suite is configured, the CAK and CKN shall each be specified as a hexadecimal number with a minimum length of 1 digit and a maximum length of 32 digits. When a 256-bit cipher suite is configured, the CAK and CKN shall each be specified as a hexadecimal number with a minimum length of 1 digit and a maximum length of 64 digits.



NOTE: To maximize security, the TOE's administrator should 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. As part of its operation, the MKA protocol elects one of the two directly-connected switches as the key server. The election of the key server is determined by comparing the key server priority values configured on each participant: the switch with the highest key server priority value is elected as the key server. If the priorities are equal, further tie-breakers such as the lowest MAC address are used.

The TOE can be configured to act as the key server by manually setting its key server priority to a value higher than that of the peer device using the `key-server-priority` command in the MKA configuration. The key server is responsible for generating and sharing a random secure association key (SAK) with the other device over the MACsec-secure point-to-point link. The key server continues to periodically create and share new random SAKs with the other device over the MACsec-secured point-to-point link for as long as MACsec is enabled.

For example, the TOE's administrator 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

- [Configuring MACsec on a Device Running Junos OS | 111](#)
- [Configuring Static MACsec with Layer 3 Traffic | 113](#)
- [Configuring MACsec with keychain using Layer 3 Traffic | 116](#)
- [Configuring Static MACsec for Layer 2 Traffic | 122](#)
- [Configuring MACsec with keychain for Layer 2 Traffic | 128](#)
- [Disable and Restart MACsec Sessions | 135](#)

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

The TOE's administrator 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 the TOE's administrator can configure only one type of interface speed.

The TOE only allows the following MACsec ethertypes by default and this requires no configuration: 88-8E, 88-E5, 88-08.

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@host:fps# set security macsec connectivity-association connectivity-association-name exclude-protocol protocol-name
security-administrator@host:fps# set security macsec connectivity-association connectivity-association-name include-sci
security-administrator@host:fps# set security macsec connectivity-association connectivity-association-name mka key-server-priority priority-number
security-administrator@host:fps# set security macsec connectivity-association connectivity-association-name mka transmit-interval interval
security-administrator@host:fps# set security macsec connectivity-association connectivity-association-name offset 30
```



NOTE: Based on your requirement you can configure the offset *offset-number* value at the set security macsec connectivity-association *connectivity-association-name* 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@host:fps# prompt security macsec connectivity-association connectivity-association-name pre-shared-key cak
New cak (secret):
Retype new cak (secret):
security-administrator@host:fps# set security macsec connectivity-association connectivity-association-name pre-shared-key ckn hexadecimal-number
security-administrator@host:fps# 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.



NOTE: The ICK is automatically derived from the CAK using AES_CMAC and this requires no separate configuration.

3. Set the MACsec Key Agreement (MKA) secure channel details.

[edit]

```
security-administrator@host:fps# set security macsec connectivity-association connectivity-association-name secure-channel secure-channel-name direction (inbound | outbound)
security-administrator@host:fps# set security macsec connectivity-association connectivity-association-name secure-channel secure-channel-name encryption (MACsec)
security-administrator@host:fps# set security macsec connectivity-association connectivity-association-name secure-channel secure-channel-name id mac-address mac-address
security-administrator@host:fps# set security macsec connectivity-association connectivity-association-name secure-channel secure-channel-name id port-id port-id-number
security-administrator@host:fps# set security macsec connectivity-association connectivity-association-name secure-channel secure-channel-name offset (0|30|50)
security-administrator@host:fps# set security macsec connectivity-association connectivity-association-name secure-channel secure-channel-name security-association security-association-number key key-string
```

4. Set the MKA to security mode.

[edit]

```
security-administrator@host:fps# set security macsec connectivity-association CA1 security-mode security-mode
```



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

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

[edit]

```
security-administrator@host:fps# set security macsec interfaces interface-name connectivity-association connectivity-association-name
```

Configuring Static MACsec with Layer 3 Traffic

To configure Static MACsec using Layer 3 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@host:fps# set security macsec connectivity-association CA1 pre-
shared-key ckn 234567892233445566778899222333444555666777888999222333344445555
security-administrator@host:fps# prompt security macsec connectivity-association CA1 pre-
shared-key cak
New cak (secret):
Retype new cak (secret):
security-administrator@host:fps# set security macsec connectivity-association CA1 offset 30
```

2. Set the trace option values.

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

3. Assign the trace to an interface.

```
[edit]
security-administrator@host:fps# set security macsec interfaces interface-name traceoptions
file mka_xe size 1g
security-administrator@host:fps# 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@host:fps# set security macsec connectivity-association CA1 security-
mode static-cak
```

5. Set the MKA key server priority.

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

6. Set the MKA transmit interval.

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

7. Enable Secure Channel Identifier.

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

8. Assign the connectivity association to an interface.

```
[edit]
security-administrator@host:fps# set security macsec interfaces interface-name connectivity-
association CA1
security-administrator@host:fps# 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@host:fps# set security macsec connectivity-association CA1 pre-
shared-key ckn 234567892233445566778899222333444555666777888999222333344445555
security-administrator@host:fps# prompt security macsec connectivity-association CA1 pre-
shared-key cak
New cak (secret):
Retype new cak (secret):
security-administrator@host:fps# set security macsec connectivity-association CA1 offset 30
```

2. Set the trace option values.

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

3. Assign the trace to an interface.

```
[edit]
security-administrator@host:fps# set security macsec interfaces interface-name traceoptions
file mka_xe size 1g
security-administrator@host:fps# 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@host:fps# set security macsec connectivity-association CA1 security-
mode static-cak
```

5. Set the MKA transmit interval.

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

6. Enable Secure Channel Identifier.

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

7. Assign the connectivity association to an interface.

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

```
security-administrator@host: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, as the time for both devices to trigger the key start time should be the same. To configure MACsec with keychain using Layer 3 traffic between device R0 and device R1:

In R0:

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

```
[edit]
security-administrator@host: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 the Connectivity Association Key (CAK).

The TOE's administrator can configure up to 64 keys within a keychain. In addition to specifying the key material, the TOE's administrator can also configure start-time based on TOE's current time to precisely control the key's lifetime.

The keys can be configured with a start-time in YYYY-MM-DD.HH:MM format to define when the corresponding key becomes active.

When multiple keys are configured with sequential start times, new keys keep becoming active when their start time is reached, effectively configuring the lifetime for each key.

```
[edit]
security-administrator@host:fips# set security authentication-key-chains key-chain macsec-kc1 key 0 key-name 234567892233445566778899222333444555666777888999222333344445551
security-administrator@host:fips# set security authentication-key-chains key-chain macsec-kc1 key 0 start-time 2018-03-20.20:35
security-administrator@host:fips# set security authentication-key-chains key-chain macsec-kc1 key 1 key-name 234567892233445566778899222333444555666777888999222333344445552
security-administrator@host:fips# set security authentication-key-chains key-chain macsec-kc1 key 1 start-time 2018-03-20.20:37
security-administrator@host:fips# set security authentication-key-chains key-chain macsec-kc1 key 2 key-name 234567892233445566778899222333444555666777888999222333344445553
```

```

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

The TOE's administrator can configure up to 64 secret keys. For example, the TOE's administrator can refer the following secret keys:

```

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

```

3. To delete an existing key from a keychain, use the following command:

```

[edit]
security-administrator@host:fips# delete security authentication-key-chains key-chain macsec-kc1 key 0

```

- Associate the preshared keychain name with the connectivity association.

```
[edit]
security-administrator@host:fps# set security macsec connectivity-association CA1 pre-
shared-key-chain macsec-kc1
security-administrator@host:fps# set security macsec connectivity-association CA1 offset 50
security-administrator@host:fps# 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**.

- Set the trace option values.

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

- Assign the trace to an interface.

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

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

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

- Set the MKA key server priority.

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

9. Set the MKA transmit interval.

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

10. Enable Secure Channel Identifier.

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

11. Assign the connectivity association to an interface.

```
[edit]
security-administrator@host:fps# set security macsec interfaces interface-name
connectivity-association CA1
security-administrator@host:fps# 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@host:fps# 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.

The TOE's administrator can configure up to 64 keys. For example, the TOE's administrator can refer the following keys:

```
[edit]
security-administrator@host:fps# set security authentication-key-chains key-chain macsec-
kc1 key 0 key-name 234567892233445566778899222333444555666777888999222333344445551
security-administrator@host:fps# set security authentication-key-chains key-chain macsec-
```

```

kc1 key 0 start-time 2018-03-20.20:35
security-administrator@host:fips# set security authentication-key-chains key-chain macsec-
kc1 key 1 key-name 23456789223344556677889922233344455566777888999222333344445552
security-administrator@host:fips# set security authentication-key-chains key-chain macsec-
kc1 key 1 start-time 2018-03-20.20:37
security-administrator@host:fips# set security authentication-key-chains key-chain macsec-
kc1 key 2 key-name 234567892233445566778899222333444555666777888999222333344445553
security-administrator@host:fips# set security authentication-key-chains key-chain macsec-
kc1 key 2 start-time 2018-03-20.20:39
security-administrator@host:fips# set security authentication-key-chains key-chain macsec-
kc1 key 3 key-name 234567892233445566778899222333444555666777888999222333344445554
security-administrator@host:fips# set security authentication-key-chains key-chain macsec-
kc1 key 3 start-time 2018-03-20.20:41
security-administrator@host:fips# set security authentication-key-chains key-chain macsec-
kc1 key 4 key-name 234567892233445566778899222333444555666777888999222333344445555
security-administrator@host: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.

The TOE's administrator can configure up to 64 secret keys. For example, the TOE's administrator can refer the following secret keys:

```

[edit]
security-administrator@host:fips# prompt security authentication-key-chains key-chain
macsec-kc1 key 0 secret
New cak (secret):
Retype new cak (secret):
security-administrator@host:fips# prompt security authentication-key-chains key-chain
macsec-kc1 key 1 secret
New cak (secret):
Retype new cak (secret):
security-administrator@host:fips# prompt security authentication-key-chains key-chain
macsec-kc1 key 2 secret
New cak (secret):
Retype new cak (secret):
security-administrator@host:fips# prompt security authentication-key-chains key-chain
macsec-kc1 key 3 secret
New cak (secret):
Retype new cak (secret):
security-administrator@host: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@host:fps# set security macsec connectivity-association CA1 pre-
shared-key-chain macsec-kc1
security-administrator@host:fps# set security macsec connectivity-association CA1 offset 50
security-administrator@host:fps# set security macsec connectivity-association CA1 cipher-
suite gcm-aes-256
```



NOTE: You can use the non-XPB ciphers AES-GCM-128 and AES-GCM-256 for 10G/xe interfaces macsec configuration only.

4. Set the trace option values.

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

5. Assign the trace to an interface.

```
[edit]
security-administrator@host:fps# set security macsec interfaces interface-name
traceoptions file mka_xe size 1g
security-administrator@host:fps# 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@host:fps# set security macsec connectivity-association CA1 security-
mode static-cak
```

7. Set the MKA key server priority.

```
[edit]
security-administrator@host:fps# set security macsec connectivity-association CA1 mka key-
server-priority 2
```

8. Set the MKA transmit interval.

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

9. Enable Secure Channel Identifier.

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

10. Assign the connectivity association to an interface.

```
[edit]
security-administrator@host:fps# set security macsec interfaces interface-name
connectivity-association CA1
security-administrator@host:fps# 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@host:fps# set security macsec connectivity-association CA1 mka key-  
server-priority 1
```



NOTE: The configurable range for the key server priority values is 0-255 with 0 meaning highest priority. Also, the TOE must be configured with the lowest priority number to configure it to act as a key server.

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@host:fps# 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.

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

[edit]

```
security-administrator@host:fps# set security macsec connectivity-association CA1 pre-  
shared-key-chain macsec-kc1
```

```
security-administrator@host:fps# set security macsec connectivity-association CA1 offset 50
```

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

4. Set the trace option values.

[edit]

```
security-administrator@host:fps# set security macsec traceoptions file MACsec.log
```

```
security-administrator@host:fps# set security macsec traceoptions file size 4000000000
```

```
security-administrator@host:fps# set security macsec traceoptions flag all
```

5. Assign the trace to an interface.

```
[edit]
security-administrator@host:fps# set security macsec interfaces interface-name
traceoptions file mka_xe size 1g
security-administrator@host:fps# 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@host:fps# set security macsec connectivity-association CA1 security-
mode static-cak
```

7. Set the MKA key server priority.

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

8. Set the MKA transmit interval.

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

9. Enable Secure Channel Identifier.

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

10. Assign the connectivity association to an interface.

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

11. Configure VLAN tagging.

```
[edit]
security-administrator@host:fps# set interfaces interface-name1 flexible-vlan-tagging
security-administrator@host:fps# set interfaces interface-name1 encapsulation flexible-
ethernet-services
security-administrator@host:fps# set interfaces interface-name1 unit 100 encapsulation
vlan-bridge
security-administrator@host:fps# set interfaces interface-name1 unit 100 vlan-id 100
security-administrator@host:fps# set interfaces interface-name2 flexible-vlan-tagging
security-administrator@host:fps# set interfaces interface-name2 encapsulation flexible-
ethernet-services
security-administrator@host:fps# set interfaces interface-name2 unit 100 encapsulation
vlan-bridge
security-administrator@host:fps# set interfaces interface-name2 unit 100 vlan-id 100
```

12. Configure bridge domain.

```
[edit]
security-administrator@host:fps# set bridge-domains BD-110 domain-type bridge
security-administrator@host:fps# set bridge-domains BD-110 vlan-id 100
security-administrator@host:fps# set bridge-domains BD-110 interface interface-name1 100
security-administrator@host:fps# set bridge-domains BD-110 interface interface-name2 100
```



NOTE: The *interface-name1* and *interface-name2* options at the set bridge-domains *BD-110* interface hierarchy level are user defined interfaces which are part of the bridge domain.

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@host:fps# 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@host:fps# set security macsec connectivity-association CA1 pre-
shared-key-chain macsec-kc1
security-administrator@host:fps# set security macsec connectivity-association CA1 offset 50
security-administrator@host:fps# set security macsec connectivity-association CA1 cipher-
suite gcm-aes-256
```

3. Set the trace option values.

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

4. Assign the trace to an interface.

```
[edit]
security-administrator@host:fps# set security macsec interfaces interface-name
traceoptions file mka_xe size 1g
security-administrator@host:fps# 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@host:fps# set security macsec connectivity-association CA1 security-
mode static-cak
```

6. Set the MKA key server priority.

```
[edit]
security-administrator@host:fps# set security macsec connectivity-association CA1 mka key-
server-priority 2
```

7. Set the MKA transmit interval.

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

8. Enable Secure Channel Identifier.

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

9. Assign the connectivity association to an interface.

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

10. Configure VLAN tagging.

```
[edit]
security-administrator@host:fps# set interfaces interface-name1 flexible-vlan-tagging
security-administrator@host:fps# set interfaces interface-name1 encapsulation flexible-
ethernet-services
security-administrator@host:fps# set interfaces interface-name1 unit 100 encapsulation
vlan-bridge
security-administrator@host:fps# set interfaces interface-name1 unit 100 vlan-id 100
security-administrator@host:fps# set interfaces interface-name2 flexible-vlan-tagging
security-administrator@host:fps# set interfaces interface-name2 encapsulation flexible-
ethernet-services
security-administrator@host:fps# set interfaces interface-name2 unit 100 encapsulation
vlan-bridge
security-administrator@host:fps# set interfaces interface-name2 unit 100 vlan-id 100
```

11. Configure bridge domain.

```
[edit]
security-administrator@host:fps# set bridge-domains BD-110 domain-type bridge
```

```
security-administrator@host:fps# set bridge-domains BD-110 vlan-id 100
security-administrator@host:fps# set bridge-domains BD-110 interface interface-name1 100
security-administrator@host:fps# set bridge-domains BD-110 interface interface-name2 100
```

Configuring MACsec with keychain for Layer 2 Traffic

Synchronize both MACsec endpoint devices, as the time for both devices to trigger the key start time should be the same. To configure MACsec with keychain for Layer 3 traffic between device R0 and device R1:

In R0:

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

```
[edit]
security-administrator@host:fps# 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.

The TOE's administrator can configure up to 64 keys. For example, the TOE's administrator can refer the following keys:

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

```

kc1 key 3 start-time 2018-03-20.20:41
security-administrator@host:fips# set security authentication-key-chains key-chain macsec-
kc1 key 4 key-name 23456789223344556677889922233344455566778899922233344445555
security-administrator@host: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.

The TOE's administrator can configure up to 64 secret keys. For example, the TOE's administrator can refer the following secret keys:

```

[edit]
security-administrator@host:fips# prompt security authentication-key-chains key-chain
macsec-kc1 key 0 secret
New cak (secret):
Retype new cak (secret):
security-administrator@host:fips# prompt security authentication-key-chains key-chain
macsec-kc1 key 1 secret
New cak (secret):
Retype new cak (secret):
security-administrator@host:fips# prompt security authentication-key-chains key-chain
macsec-kc1 key 2 secret
New cak (secret):
Retype new cak (secret):
security-administrator@host:fips# prompt security authentication-key-chains key-chain
macsec-kc1 key 3 secret
New cak (secret):
Retype new cak (secret):
security-administrator@host: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@host:fips# set security macsec connectivity-association CA1 pre-
shared-key-chain macsec-kc1
security-administrator@host:fips# set security macsec connectivity-association CA1 cipher-
suite gcm-aes-256

```

4. Set the trace option values.

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

5. Assign the trace to an interface.

```
[edit]
security-administrator@host:fps# set security macsec interfaces interface-name
traceoptions file mka_xe size 1g
security-administrator@host:fps# 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@host:fps# set security macsec connectivity-association CA1 security-
mode static-cak
```

7. Set the MKA key server priority.

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

8. Set the MKA transmit interval.

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

9. Enable Secure Channel Identifier.

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

10. Assign the connectivity association to an interface.

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

11. Configure VLAN tagging.

```
[edit]
security-administrator@host:fps# set interfaces interface-name1 flexible-vlan-tagging
security-administrator@host:fps# set interfaces interface-name1 encapsulation flexible-
ethernet-services
security-administrator@host:fps# set interfaces interface-name1 unit 100 encapsulation
vlan-bridge
security-administrator@host:fps# set interfaces interface-name1 unit 100 vlan-id 100
security-administrator@host:fps# set interfaces interface-name2 flexible-vlan-tagging
security-administrator@host:fps# set interfaces interface-name2 encapsulation flexible-
ethernet-services
security-administrator@host:fps# set interfaces interface-name2 unit 100 encapsulation
vlan-bridge
security-administrator@host:fps# set interfaces interface-name2 unit 100 vlan-id 100
```

12. Configure bridge domain.

```
[edit]
security-administrator@host:fps# set bridge-domains BD-110 domain-type bridge
security-administrator@host:fps# set bridge-domains BD-110 vlan-id 100
security-administrator@host:fps# set bridge-domains BD-110 interface interface-name1 100
security-administrator@host:fps# set bridge-domains BD-110 interface interface-name2 100
```

In R1:

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

```
[edit]
security-administrator@host:fps# 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.

```
[edit]
security-administrator@host:fps#  set security authentication-key-chains key-chain macsec-
kc1 key 0 key-name 234567892233445566778899222333444555667778889992222333344445551
security-administrator@host:fps#  set security authentication-key-chains key-chain macsec-
kc1 key 0 start-time 2018-03-20.20:35
security-administrator@host:fps#  set security authentication-key-chains key-chain macsec-
kc1 key 1 key-name 234567892233445566778899222333444555667778889992222333344445552
security-administrator@host:fps#  set security authentication-key-chains key-chain macsec-
kc1 key 1 start-time 2018-03-20.20:37
security-administrator@host:fps#  set security authentication-key-chains key-chain macsec-
kc1 key 2 key-name 234567892233445566778899222333444555667778889992222333344445553
security-administrator@host:fps#  set security authentication-key-chains key-chain macsec-
kc1 key 2 start-time 2018-03-20.20:39
security-administrator@host:fps#  set security authentication-key-chains key-chain macsec-
kc1 key 3 key-name 234567892233445566778899222333444555667778889992222333344445554
security-administrator@host:fps#  set security authentication-key-chains key-chain macsec-
kc1 key 3 start-time 2018-03-20.20:41
security-administrator@host:fps#  set security authentication-key-chains key-chain macsec-
kc1 key 4 key-name 234567892233445566778899222333444555667778889992222333344445555
security-administrator@host:fps#  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.

The TOE's administrator can configure up to 64 secret keys. For example, the TOE's administrator can refer the following secret keys:

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

```

New cak (secret):
Retype new cak (secret):
security-administrator@host:fips# prompt security authentication-key-chains key-chain
macsec-kc1 key 3 secret
New cak (secret):
Retype new cak (secret):
security-administrator@host: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@host:fips# set security macsec connectivity-association CA1 pre-
shared-key-chain macsec-kc1
security-administrator@host:fips# set security macsec connectivity-association CA1 cipher-
suite gcm-aes-256

```

4. Set the trace option values.

```

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

```

5. Assign the trace to an interface.

```

[edit]
security-administrator@host:fips# set security macsec interfaces interface-name
traceoptions file mka_xe size 1g
security-administrator@host: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@host:fps# set security macsec connectivity-association CA1 security-
mode static-cak
```

7. Set the MKA key server priority.

```
[edit]
security-administrator@host:fps# set security macsec connectivity-association CA1 mka key-
server-priority 2
```

8. Set the MKA transmit interval.

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

9. Enable Secure Channel Identifier.

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

10. Assign the connectivity association to an interface.

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

11. Configure VLAN tagging.

```
[edit]
security-administrator@host:fps# set interfaces interface-name1 flexible-vlan-tagging
security-administrator@host:fps# set interfaces interface-name1 encapsulation flexible-
ethernet-services
security-administrator@host:fps# set interfaces interface-name1 unit 100 encapsulation
```

vlan-bridge

```
security-administrator@host:fps# set interfaces interface-name1 unit 100 vlan-id 100
security-administrator@host:fps# set interfaces interface-name2 flexible-vlan-tagging
security-administrator@host:fps# set interfaces interface-name2 encapsulation flexible-
ethernet-services
security-administrator@host:fps# set interfaces interface-name2 unit 100 encapsulation
vlan-bridge
security-administrator@host:fps# set interfaces interface-name2 unit 100 vlan-id 100
```

12. Configure bridge domain.

[edit]

```
security-administrator@host:fps# set bridge-domains BD-110 domain-type bridge
security-administrator@host:fps# set bridge-domains BD-110 vlan-id 100
security-administrator@host:fps# set bridge-domains BD-110 interface interface-name1 100
security-administrator@host:fps# set bridge-domains BD-110 interface interface-name2 100
```

Disable and Restart MACsec Sessions

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

- To disable the MACsec session:

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

- To restart the MACsec session:

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

or

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

9

CHAPTER

Perform Self-Tests on a Device

IN THIS CHAPTER

- [FIPS Self-Tests Overview | 137](#)
-

FIPS Self-Tests Overview

The cryptographic module enforces security rules to ensure that the Juniper Networks Junos operating system (Junos OS) in FIPS mode 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
- `macsec_kats`—KAT for MACsec cryptographic implementation
- `md_kats`—KAT for libmd and libc
- `openssl_kats`—KAT for OpenSSL cryptographic implementation



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

The device automatically performs the KAT self-tests at startup. The device also performs the conditional self-tests automatically to verify digitally signed software packages, generated random numbers, RSA and ECDSA key pairs, and manually entered keys.

When the device successfully completes the KATs, it updates the log (syslog) file to display the executed tests.

During bootup entropy health test is performed. The system software integrity check is done during bootup. Each software module is verified before being loaded. The messages pertaining to the entropy health check and software integrity checks can be viewed on the console during system bootup.

If one of the self-tests fail, the device panics and reboot continuously. The TOE's administrator can recover the device using USB install as follows:

1. Download the Junos USB installation image and create a bootable USB drive.
2. Insert the bootable USB drive into the Routing Engine USB port.
3. Reboot the device.
4. Access the Boot Manager during startup and select the USB device as the boot source.
5. Allow the USB installation process to start and follow the prompts to complete the installation.
6. Reboot the device for the fresh Junos installation to take effect.

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

```
security-admin@host:fips> request system fips
self-test random: HMAC-DRBG with SHA2-512
chosen
sysctl_warn_reuse: can't re-use a leaf (kern.random.hmac-drbg.hash)!
Testing kernel KATS:
  NIST 800-90 HMAC DRBG Known Answer Test:      Passed
  HMAC-SHA1 Known Answer Test:                  Passed
  HMAC-SHA2-256 Known Answer Test:              Passed
  SHA-2-384 Known Answer Test:                  Passed
```

AES128-CMAC Known Answer Test:	Passed
AES-CBC Known Answer Test:	Passed
Testing MACSec KATS:	
AES128-CMAC Known Answer Test:	Passed
AES256-CMAC Known Answer Test:	Passed
AES-ECB Known Answer Test:	Passed
AES-KEYWRAP Known Answer Test:	Passed
KBKDF Known Answer Test:	Passed
Testing libmd KATS:	
HMAC-SHA1 Known Answer Test:	Passed
HMAC-SHA2-256 Known Answer Test:	Passed
SHA-2-512 Known Answer Test:	Passed
Testing OpenSSL KATS:	
FIPS ECDSA Known Answer Test:	Passed
FIPS ECDH Known Answer Test:	Passed
HMAC-SHA1 Known Answer Test:	Passed
HMAC-SHA2-224 Known Answer Test:	Passed
HMAC-SHA2-256 Known Answer Test:	Passed
HMAC-SHA2-384 Known Answer Test:	Passed
HMAC-SHA2-512 Known Answer Test:	Passed
AES-CBC Known Answer Test:	Passed
AES-GCM Known Answer Test:	Passed
RSA-ENC Known Answer Test:	Passed
RSA-SIGN Known Answer Test:	Passed
KDF-IKE-V1 Known Answer Test:	Passed
KDF-SSH-SHA256 Known Answer Test:	Passed
KDF-TLS12-PRF Known Answer Test:	Passed
KDF-TLS13-KDF-EXTRACT Known Answer Test:	Passed
KDF-TLS13-KDF-EXPAND Known Answer Test:	Passed
KDF-X942 Known Answer Test:	Passed
KDF-X963 Known Answer Test:	Passed
KAS-ECC-EPHEM-UNIFIED-NOKC Known Answer Test:	Passed
KAS-FFC-EPHEM-NOKC Known Answer Test:	Passed
Testing QuickSec 7.0 KATS:	
HMAC-SHA1 Known Answer Test:	Passed
HMAC-SHA2-224 Known Answer Test:	Passed
HMAC-SHA2-256 Known Answer Test:	Passed
HMAC-SHA2-384 Known Answer Test:	Passed
HMAC-SHA2-512 Known Answer Test:	Passed
AES-CBC Known Answer Test:	Passed
AES-GCM Known Answer Test:	Passed
SSH-RSA-ENC Known Answer Test:	Passed
SSH-RSA-SIGN Known Answer Test:	Passed

```

SSH-ECDSA-SIGN Known Answer Test:           Passed
KDF-IKE-V1 Known Answer Test:               Passed
KDF-IKE-V2 Known Answer Test:               Passed
Testing QuickSec KATS:
HMAC-SHA1 Known Answer Test:                Passed
HMAC-SHA2-224 Known Answer Test:            Passed
HMAC-SHA2-256 Known Answer Test:            Passed
HMAC-SHA2-384 Known Answer Test:            Passed
HMAC-SHA2-512 Known Answer Test:            Passed
AES-CBC Known Answer Test:                  Passed
AES-GCM Known Answer Test:                  Passed
SSH-RSA-ENC Known Answer Test:               Passed
SSH-RSA-SIGN Known Answer Test:              Passed
KDF-IKE-V1 Known Answer Test:               Passed
KDF-IKE-V2 Known Answer Test:               Passed
Testing SSH IPsec KATS:
HMAC-SHA1 Known Answer Test:                Passed
HMAC-SHA2-256 Known Answer Test:            Passed
AES-CBC Known Answer Test:                  Passed
SSH-RSA-ENC Known Answer Test:               Passed
SSH-RSA-SIGN Known Answer Test:              Passed
KDF-IKE-V1 Known Answer Test:               Passed
Testing file integrity:
File integrity Known Answer Test:             Passed
Testing crypto integrity:
Crypto integrity Known Answer Test:           Passed
Expect an exec Authentication error...
/sbin/kats/run-tests: /sbin/kats/cannot-exec: Authentication error

```



NOTE: The self-test module tests cryptographic protocols and algorithms that are not utilized in the approved mode of operation. Refer section **Supported Cryptographic Algorithms** for the list of protocols and algorithms that are utilized by the TOE.

10

CHAPTER

Operational Commands

IN THIS CHAPTER

- [request vmhost zeroize no-forwarding](#) | 141
-

request vmhost zeroize no-forwarding

IN THIS SECTION

- [Syntax | 141](#)
- [Description | 141](#)
- [Required Privilege Level | 141](#)
- [Sample Output | 142](#)
- [Release Information | 142](#)

Syntax

```
request vmhost zeroize no-forwarding
```

Description

Remove all configuration information on the Routing Engines and reset all key values. 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, the TOE's administrator 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.

Required Privilege Level

maintenance

Sample Output

request vmhost zeroize no-forwarding

```

user@host> request vmhost zeroize no-forwarding
VMHost Zeroization : Erase all data, including configuration and log files ?
[yes,no] (no) yes
warning: Vmhost will reboot and may not boot without configuration
warning: Proceeding with vmhost zeroize
Zeroize secondary internal disk ...
Proceeding with zeroize on secondary disk
Mounting device in preparation for zeroize...
Cleaning up target disk for zeroize ...
Zeroize done on target disk.
Zeroize of secondary disk completed
Zeroize primary internal disk ...
Proceeding with zeroize on primary disk
/etc/ssh/ssh_host_ecdsa_key.pub
/etc/ssh/ssh_host_rsa_key.pub
/etc/ssh/ssh_host_ecdsa_key
/etc/ssh/ssh_host_dsa_key
/etc/ssh/ssh_host_dsa_key.pub
/etc/ssh/ssh_host_rsa_key
Mounting device in preparation for zeroize...
Cleaning up target disk for zeroize ...
Zeroize done on target disk.
Zeroize of primary disk completed
Zeroize done
warning: Proceeding with vmhost reboot
Initiating vmhost reboot...

```

Release Information

Command introduced in Junos OS Release 15.1F3.