Junos® OS for EX Series Ethernet Switches, Release 14.1R4

FIPS

Release
14.1R4

Published: 2015-03-06
Revision 1

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

Junos® OS for EX Series Ethernet Switches FIPS
Release 14.1R4

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 http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About the Documentation vii

Documentation and Release Notes vii
Supported Platforms vii
Using the Examples in This Manual viii
Merging a Full Example viii
Merging a Snippet ix
Documentation Conventions ix
Documentation Feedback xi
Requesting Technical Support xii
Self-Help Online Tools and Resources xii
Opening a Case with JTAC xii

Part 1 Junos OS in FIPS Mode for EX Series Switches

Chapter 1 Junos OS in FIPS Mode Overview—Environment and Requirements 3

Understanding Junos OS in FIPS Mode 3
About the Cryptographic Boundary on Your EX Series Switch 4
How FIPS Mode Differs from Non-FIPS Mode 5
How Junos FIPS Mode Differs from Junos-FIPS 5
Validated Version of Junos OS in FIPS Mode 5
How to Use FIPS Documentation 5
Verifying Secure Delivery of the Product 6
Verifying Product Integrity 6
Verifying Product Authenticity 6
Applying Tamper-Evident Seals to Switch Management Ports for FIPS Mode 7
General Tamper-Evident Seal Instructions 7
EX9204 Switch Tamper-Evident Seal Application 7
EX9208 Switch Tamper-Evident Seal Application 8
EX9214 Switch Tamper-Evident Seal Application 9
Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms 11
FIPS Terminology 11
Supported Cryptographic Algorithms 13
Understanding Zeroization to Clear System Data for FIPS Mode 14
Why Zeroize? 15
When to Zeroize? 15
Understanding FIPS Self-Tests 15
Understanding FIPS Error States and System Panic 16
FIPS System Panic 16
Memory Allocation Error 17
Error Recovery from Alternate Boot Media 17

Understanding Roles and Services for Junos OS in FIPS Mode 18
Crypto Officer Role and Responsibilities 18
FIPS User Role and Responsibilities 19
What Is Expected of All FIPS Users 19
Understanding the Operational Environment for Junos OS in FIPS Mode 20
Hardware Environment for Junos OS in FIPS Mode 20
Software Environment for Junos OS in FIPS Mode 21
Critical Security Parameters 21
Understanding Requirements for Secure Communication Between Routing Engines in FIPS Mode 23
SA Direction 24
SPI 24
IPsec Keys 24
IPsec Limitations 24
Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode 25
Understanding Remote Access for Junos OS in FIPS Mode 26
Understanding Event Logging for Junos OS in FIPS Mode 27
Understanding Configuration Limitations and Restrictions on Junos OS in FIPS Mode 27
How to Enable and Configure Junos OS in FIPS Mode—Overview 29

Chapter 2 **Enabling and Configuring Junos OS in FIPS Mode 31**

Downloading and Installing Junos Software Packages (FIPS Mode) 31
Downloading Software Packages from Juniper Networks (FIPS Mode) 32
Installing Software on an EX Series Switch with a Single Routing Engine (FIPS Mode) 33
Installing Software on an EX Series Switch with Redundant Routing Engines (FIPS Mode) 35
Preparing the Switch for the Software Installation 36
Installing Software on the Backup Routing Engine 37
Installing Software on the Default Master Routing Engine 38
Returning Routing Control to the Default Master Routing Engine (Optional) 40
Zeroizing the System (FIPS Mode) 40
Setting a Switch to FIPS Mode 41
Establishing Root Password Access (FIPS Mode) 44
Configuring Crypto Officer and FIPS User Identification and Access 45
Configuring Crypto Officer Login Access 45
Configuring FIPS User Login Access 46
Enabling Internal Communications Between Routing Engines (FIPS Mode) 47
Configuring the IPsec SA on the Master Routing Engine 49
Configuring the IPsec SA on the Backup Routing Engine 51
Configuring the Console Port for FIPS Mode 53
Configuring Event Logging for Junos OS in FIPS Mode 54
Configuring Event Logging to a Local File 55
Configuring Event Logging to a Remote Server 56
Disabling FIPS Mode 57

Chapter 3 Administering Junos OS in FIPS Mode on an EX Series Switch 59
Verifying That FIPS Self-Tests Are Taking Place 59
Chapter 4 Configuration Statements for Junos OS in FIPS Mode 61
algorithm (FIPS) 62
authentication (FIPS) 62
direction (FIPS) 63
encryption (FIPS) 64
fips (FIPS) 64
internal (FIPS) 65
ipsec (FIPS) 66
key (FIPS) 67
level (FIPS) 68
manual (FIPS) 69
protocol esp (FIPS) 69
security (FIPS) 70
security-association (FIPS) 71
spi (FIPS) 72
Chapter 5 Operational Commands for Junos OS in FIPS Mode 73
request system zeroize (FIPS) 74

About the Documentation

- Documentation and Release Notes on page vii
- Supported Platforms on page vii
- Using the Examples in This Manual on page viii
- Documentation Conventions on page ix
- Documentation Feedback on page xi
- Requesting Technical Support on page xii

Documentation and Release Notes

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

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

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

Supported Platforms

For the features described in this document, and to operate in accordance with the NDPP certification, Table 1 on page vii shows the platforms that are supported and their install images.

Table 1: Supported Platforms and Install Images

Platform	Install Image
EX9204	jinstall-ex-9200-Junos-14.1R4.n-domestic-signed.tgz
EX9208	jinstall-ex-9200-Junos-14.1R4.n-domestic-signed.tgz
EX9214	jinstall-ex-9200-Junos-14.1R4.n-domestic-signed.tgz

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   system {
     scripts {
       commit {
         file ex-script.xsl;
       }
     }
   }
   interfaces {
     fxp0 {
       disable;
       unit 0 {
         family inet {
           address 10.0.0.1/24;
         }
       }
     }
   }
   ```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

   ```
   [edit]
   user@host# load merge /var/tmp/ex-script.conf
   load complete
   ```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   commit {
     file ex-script-snippet.xsl; }
   ```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

   ```
   [edit]
   user@host# edit system scripts
   [edit system scripts]
   ```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

   ```
   [edit system scripts]
   user@host# load merge relative /var/tmp/ex-script-snippet.conf
   load complete
   ```

For more information about the **load** command, see the *CLI User Guide*.

Documentation Conventions

Table 2 on page x defines notice icons used in this guide.

Table 2: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 3 on page x defines the text and syntax conventions used in this guide.

Table 3: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*

Table 3: Text and Syntax Conventions *(continued)*

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

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

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

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page at the Juniper Networks Technical Documentation site at http://www.juniper.net/techpubs/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at https://www.juniper.net/cgi-bin/docbugreport/.

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

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

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

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/ .
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

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

PART 1

Junos OS in FIPS Mode for EX Series Switches

- Junos OS in FIPS Mode Overview—Environment and Requirements on page 3
- Enabling and Configuring Junos OS in FIPS Mode on page 31
- Administering Junos OS in FIPS Mode on an EX Series Switch on page 59
- Configuration Statements for Junos OS in FIPS Mode on page 61
- Operational Commands for Junos OS in FIPS Mode on page 73

CHAPTER 1

Junos OS in FIPS Mode Overview—Environment and Requirements

- Understanding Junos OS in FIPS Mode on page 3
- Verifying Secure Delivery of the Product on page 6
- Applying Tamper-Evident Seals to Switch Management Ports for FIPS Mode on page 7
- Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms on page 11
- Understanding Zeroization to Clear System Data for FIPS Mode on page 14
- Understanding FIPS Self-Tests on page 15
- Understanding FIPS Error States and System Panic on page 16
- Understanding Roles and Services for Junos OS in FIPS Mode on page 18
- Understanding the Operational Environment for Junos OS in FIPS Mode on page 20
- Understanding Requirements for Secure Communication Between Routing Engines in FIPS Mode on page 23
- Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode on page 25
- Understanding Remote Access for Junos OS in FIPS Mode on page 26
- Understanding Event Logging for Junos OS in FIPS Mode on page 27
- Understanding Configuration Limitations and Restrictions on Junos OS in FIPS Mode on page 27
- How to Enable and Configure Junos OS in FIPS Mode—Overview on page 29

Understanding Junos OS in FIPS Mode

Federal Information Processing Standards (FIPS) 140-2 defines security levels for hardware and software that perform cryptographic functions. By meeting the applicable overall requirements within the FIPS standard, the Juniper Networks RE-1800 Routing Engine on EX9200 switches running the Juniper Networks Junos operating system (Junos OS) in *FIPS mode* comply with the FIPS 140-2 Level 1 standard.

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

The *Crypto Officer* enables FIPS mode in Junos OS and sets up keys and passwords for the system and other *FIPS users* who can view the configuration. Both user types can also perform normal configuration tasks on the switch (such as modify interface types) as individual user configuration allows.

BEST PRACTICE: **Be sure to verify the secure delivery of your switch and apply tamper-evident seals to its vulnerable ports.**

- About the Cryptographic Boundary on Your EX Series Switch on page 4
- How FIPS Mode Differs from Non-FIPS Mode on page 5
- How Junos FIPS Mode Differs from Junos-FIPS on page 5
- Validated Version of Junos OS in FIPS Mode on page 5
- How to Use FIPS Documentation on page 5

About the Cryptographic Boundary on Your EX Series Switch

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

For the Juniper Networks EX Series switches that are certified at FIPS-140-2 Level 1, the cryptographic boundary of the module is determined by the chassis type. For a list of FIPS-certified switches and the cryptographic boundary of each switch, see Table 4 on page 4.

Table 4: Cryptographic Boundaries on FIPS-Certified EX Series Switches

Switch	Chassis Type	Cryptographic Boundary
EX9204 switch with any line card configuration	Modular configuration	Routing Engine
EX9208 switch with any line card configuration	Modular configuration	Routing Engine
EX9214 switch with any line card configuration	Modular configuration	Routing Engine

CAUTION: **Virtual Chassis features are not supported in FIPS mode—they have not been tested by Juniper Networks. Do not configure a Virtual Chassis in FIPS mode.**

To physically secure the cryptographic module, all EX Series switches require a tamper-evident seal on the USB and mini-USB ports.

How FIPS Mode Differs from Non-FIPS Mode

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

- Self-tests of all cryptographic algorithms are performed at startup.
- Self-tests of random number and key generation are performed continuously.
- Weak cryptographic algorithms such as Data Encryption Standard (DES) and Message Digest 5 (MD5) are disabled.
- Weak or unencrypted management connections must not be configured.
- Passwords must be encrypted with strong one-way algorithms that do not permit decryption.
- Administrator passwords must be at least 10 characters long.

For specific configuration limitations and restrictions, see "Understanding Configuration Limitations and Restrictions on Junos OS in FIPS Mode" on page 27.

How Junos FIPS Mode Differs from Junos-FIPS

Junos FIPS mode is a software package that must be installed in order to enable FIPS mode on EX9200 switches. The *Junos-FIPS image* is a separately downloadable Junos OS image available for Juniper Networks SRX Series Services Gateways.

Junos FIPS mode is available only on the EX9200 switches listed in Table 4 on page 4 that are running Junos OS Release 14.1R4.

Validated Version of Junos OS in FIPS Mode

Juniper Networks submits one Junos OS release per year—Junos OS Release 14.1R4, for example—to the National Institute of Standards and Technology (NIST) for validation. To determine whether a Junos OS release is NIST-validated, see the software download page on the Juniper Networks Web site (http://www.juniper.net/) or the National Institute of Standards and Technology site at http://csrc.nist.gov/cryptval/140-1/1401val.htm.

How to Use FIPS Documentation

For configuration and operational tasks that are specific to FIPS mode on EX Series switches, be sure to use the documentation for Junos OS in FIPS mode. Do not use the documentation for Junos-FIPS statements and commands because the syntax and options might not apply to FIPS mode.

For Junos OS configuration and operational tasks that are not specific to FIPS mode, see other EX Series hardware and software documentation at http://www.juniper.net/techpubs/en_US/release-independent/information-products/pathway-pages/ex-series/product/index.html.

Related Documentation

- Verifying Secure Delivery of the Product on page 6
- Applying Tamper-Evident Seals to Switch Management Ports for FIPS Mode on page 7
- Configuration Statements for Junos OS in FIPS Mode on page 61
- Operational Commands for Junos OS in FIPS Mode on page 73

Verifying Secure Delivery of the Product

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

- Verifying Product Integrity on page 6
- Verifying Product Authenticity on page 6

Verifying Product Integrity

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

- Shipping label—Ensure that the shipping label correctly identifies your correct customer name and address as well as the Juniper Networks product you ordered.
- Outside packaging—Inspect the outside shipping box and tape. Ensure that the shipping tape has not been cut or otherwise compromised. Ensure that the box has not been cut or damaged to allow access to the product.
- Inside packaging—Inspect the plastic bag and seal. Ensure that the bag is not cut or removed. Ensure that the seal is intact.

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

Verifying Product Authenticity

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

- Verify that the product was ordered using a purchase order. Juniper Networks products are never shipped without a purchase order.
- When a product is shipped, a shipment notification is sent to the e-mail address provided by the customer when the order is taken. Verify that this e-mail notification was received. Verify that the e-mail contains the following information:
  - Purchase order number
  - Juniper Networks order number used to track the shipment
  - Carrier tracking number used to track the shipment
  - List of items shipped, including serial numbers
  - Address and contacts of both the supplier and the customer

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

Related Documentation

- Applying Tamper-Evident Seals to Switch Management Ports for FIPS Mode on page 7

Applying Tamper-Evident Seals to Switch Management Ports for FIPS Mode

Adhesive seals applied to management ports help secure an EX Series switch. Any damage to a seal provides evidence of physical tampering with the FIPS cryptographic module. Tamper-evident seals are shipped with your switch.

As Crypto Officer, you are responsible for applying the seals to secure the cryptographic module, controlling any unused seals, and directly controlling and observing any changes—such as repairs or booting from an external USB drive—to the cryptographic module that require removing or replacing the seals to maintain the security of the module.

- General Tamper-Evident Seal Instructions on page 7
- EX9204 Switch Tamper-Evident Seal Application on page 7
- EX9208 Switch Tamper-Evident Seal Application on page 8
- EX9214 Switch Tamper-Evident Seal Application on page 9

General Tamper-Evident Seal Instructions

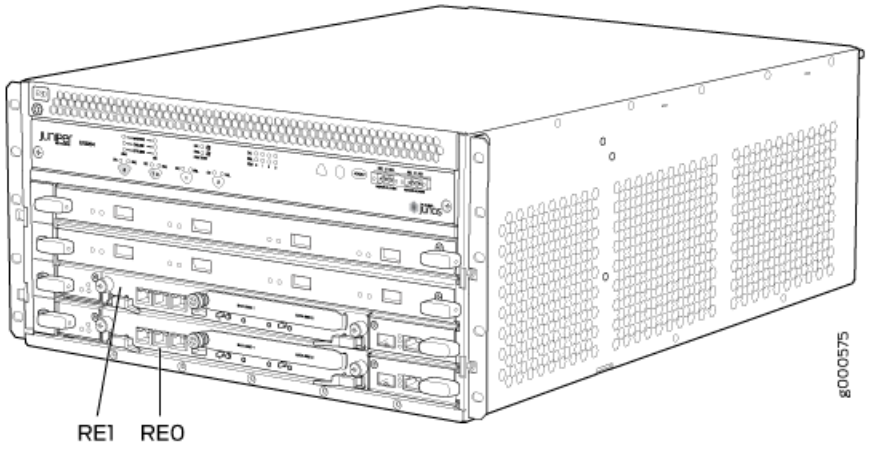
All FIPS-certified switches require a tamper-evident seal on USB ports. While applying seals, follow these general instructions:

- Handle the seals with care. Do not touch the adhesive side. Do not cut or otherwise resize a seal to make it fit.
- Make sure all surfaces to which the seals are applied are clean and dry and clear of any residue.
- Apply the seals with firm pressure across the seal to ensure adhesion. Allow at least 1 hour for the adhesive to cure.

EX9204 Switch Tamper-Evident Seal Application

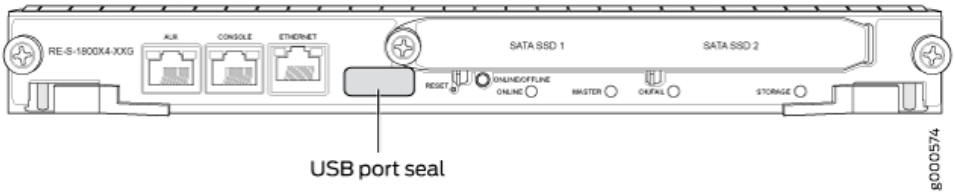
A USB port is located on each RE module in the EX9204 chassis (**RE0** and **RE1** inFigure 1 on page 8). An EX9204 chassis can have a single RE module or two (redundant) RE modules.

Figure 1: EX9204 RE Module Locations



Apply a tamper-evident USB port seal to the USB port on each RE module to secure the EX9204 cryptographic module, as shown in Figure 2 on page 8.

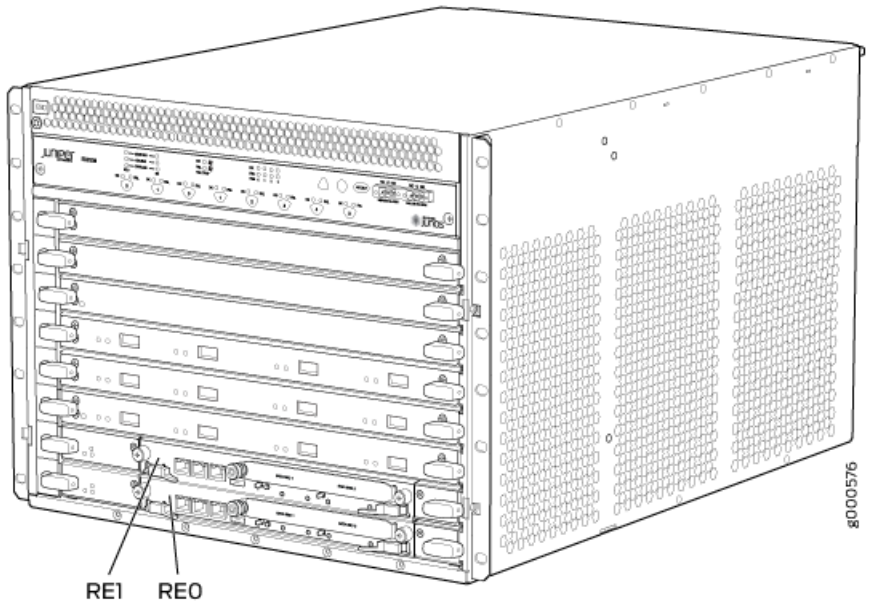
Figure 2: EX9204 Tamper-Evident Seal Location—RE Module



EX9208 Switch Tamper-Evident Seal Application

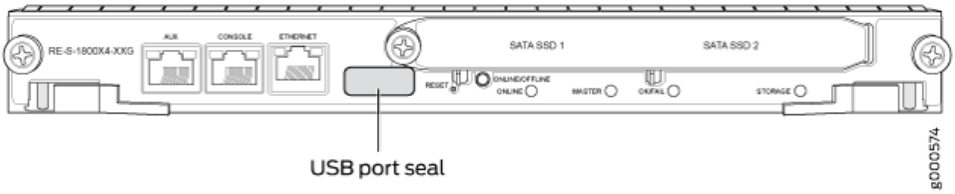
A USB port is located on each RE module in the EX9208 chassis (**RE0** and **RE1** in Figure 3 on page 9). An EX9208 chassis can have a single RE module or two redundant RE modules.

Figure 3: EX9208 RE Module Locations



Apply a tamper-evident seals to the USB port on each RE module to secure the EX9208 cryptographic module, as shown in Figure 4 on page 9.

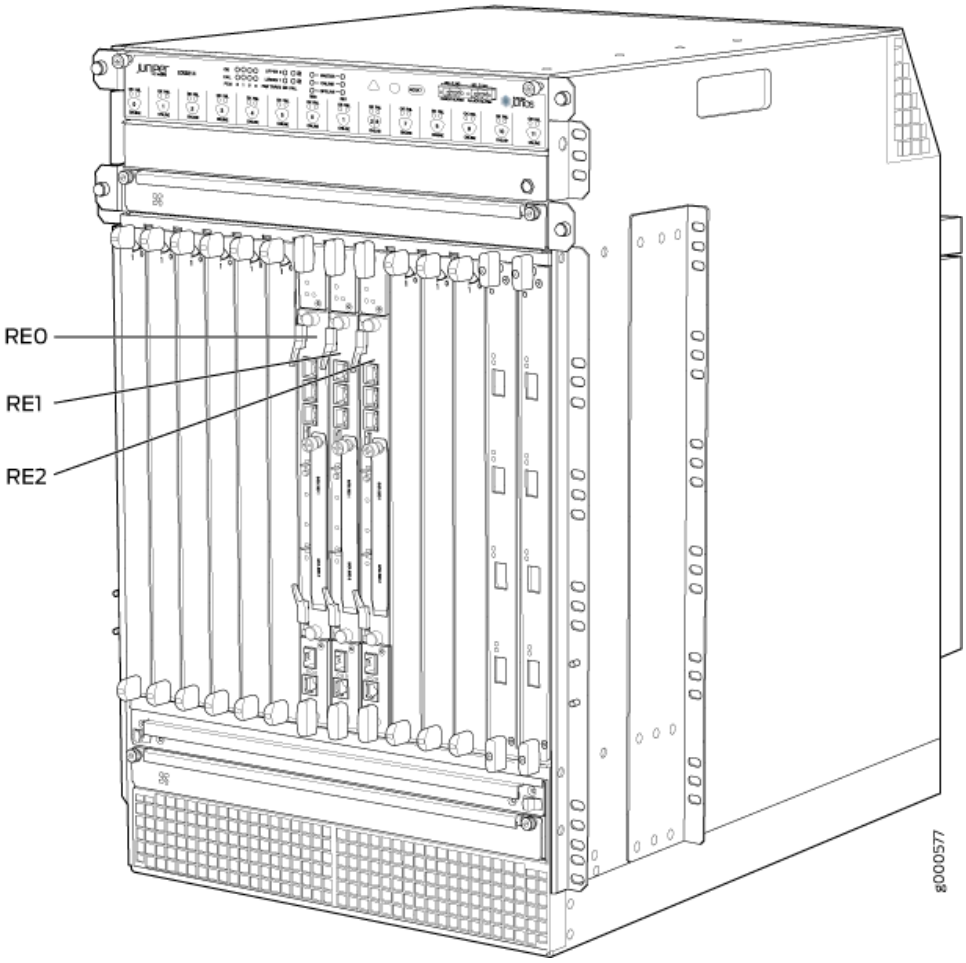
Figure 4: EX9208 Tamper-Evident Seal Location—RE Module



EX9214 Switch Tamper-Evident Seal Application

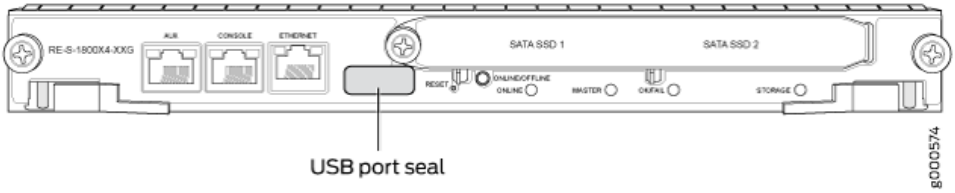
A USB port is located on each RE module in the EX9214 chassis (**RE0**, **RE1**, and **RE2** in Figure 5 on page 10). An EX9214 chassis can have two or three redundant RE modules.

Figure 5: EX9214 RE Module Locations



Apply a tamper-evident USB port seal to the USB port on each RE module to secure the EX9214 cryptographic module, as shown in Figure 6 on page 10.

Figure 6: EX9214 Tamper-Evident Seal Location—RE Module



Related Documentation

- Understanding Junos OS in FIPS Mode on page 3
- Understanding the Operational Environment for Junos OS in FIPS Mode on page 20

Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms

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

- FIPS Terminology on page 11
- Supported Cryptographic Algorithms on page 13

FIPS Terminology

Critical security parameter (CSP)—Security-related information—for example, secret and private cryptographic keys and authentication data such as passwords and personal identification numbers (PINs)—whose disclosure or modification can compromise the security of a cryptographic module or the information it protects. For details, see "Understanding the Operational Environment for Junos OS in FIPS Mode" on page 20.

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. EX Series switches are certified at FIPS 140-2 Level 1. For fixed-configuration switches, the cryptographic module is the switch case. For modular switches, the cryptographic module is the Routing Engine.

Crypto Officer—Person with appropriate permissions who is responsible for securely enabling, configuring, monitoring, and maintaining Junos OS in FIPS mode on a switch. For details, see "Understanding Roles and Services for Junos OS in FIPS Mode" on page 18.

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

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

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

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

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

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

IPsec—The IP Security (IPsec) protocol. A standard way to add security to Internet communications. An IPsec security association (SA) establishes secure communication with another FIPS cryptographic module by means of mutual authentication and encryption.

NOTE: **An IPsec SA is required for switches running Junos OS in FIPS mode for the following reasons:**

- **Because the cryptographic boundary on modular switches is the Routing Engine, an EX9204, EX9208, or EX9214 switch with redundant Routing Engines running Junos OS in FIPS mode requires an internal, manual IPsec security association (SA) between the Routing Engines for secure communication.**

For more information, see "Understanding Requirements for Secure Communication Between Routing Engines in FIPS Mode" on page 23.

KATs—Known answer tests. System self-tests that validate the output of cryptographic algorithms approved for FIPS and test the integrity of some Junos OS modules. For details, see "Understanding FIPS Self-Tests" on page 15.

SA—Security association (SA). A connection between hosts that allows them to communicate securely by defining, for example, how they exchange private keys. As Crypto Officer, you must manually configure an internal SA on switches running Junos OS in FIPS mode. All values, including the keys, must be statically specified in the configuration. On switches with more than one Routing Engine, the configuration must match on both ends of the connection between the Routing Engines. For communication to take place, each Routing Engine must have the same configured options, which need no negotiation and do not expire. For more information, see "Understanding Requirements for Secure Communication Between Routing Engines in FIPS Mode" on page 23.

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

SSH—A protocol that uses strong authentication and encryption for remote access across a nonsecure network. SSH provides remote login, remote program execution, file copy, and other functions. It is intended as a secure replacement for **rlogin**, **rsh**, and

rcp in a UNIX environment. To secure the information sent over administrative connections, use SSHv2 for CLI configuration. In Junos OS, SSHv2 is enabled by default, and SSHv1, which is not considered secure, is disabled.

Zeroization—Erasure of all CSPs and other user-created data on a switch before its operation as a FIPS cryptographic module—or in preparation for repurposing the switch for non-FIPS operation. The Crypto Officer can zeroize the system with a CLI operational command. For details, see "Understanding Zeroization to Clear System Data for FIPS Mode" on page 14.

Supported Cryptographic Algorithms

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

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

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

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

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

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

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

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

For Junos OS in FIPS mode, HMAC uses the iterated cryptographic hash function SHA-1 (designated as HMAC-SHA1) along with a secret key.

RSA—Algorithm for public key cryptography that is based on the presumed difficulty of factoring large integers of up to 2048 bits. The RSA algorithm involves three steps: key generation, encryption, and decryption. SSHv2 requires the asymmetric algorithm RSA-2048 with 2,048 bits (617 decimal digits), the largest of the RSA integers. The RSA algorithm is used in the validation of Juniper Networks signed binaries and is also available and used with the **ssh** command.

SHA-1—A Secure Hash Algorithm (SHA) standard defined in FIPS PUB 180-1 (SHA-1). Developed by NIST, SHA-1 produces a 160-bit hash for message authentication.

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

Related Documentation

- Understanding FIPS Self-Tests on page 15
- Understanding Zeroization to Clear System Data for FIPS Mode on page 14
- Understanding Requirements for Secure Communication Between Routing Engines in FIPS Mode on page 23

Understanding Zeroization to Clear System Data for FIPS Mode

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

The Crypto Officer initiates the zeroization process by entering the **request system zeroize (FIPS)** operational command from the CLI after enabling FIPS mode. Use of this command is restricted to the Crypto Officer. (To zeroize the system *before* enabling FIPS mode, use the **request system zeroize media** command.)

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

Zeroization can be time-consuming. Although all configurations are removed in a few seconds, the zeroization process goes on to overwrite all media, which can take considerable time depending on the size of the media.

- Why Zeroize? on page 15
- When to Zeroize? on page 15

Why Zeroize?

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

BEST PRACTICE: **For FIPS 140-2 compliance, you must zeroize the system to remove sensitive information before disabling FIPS mode on the switch..**

When to Zeroize?

As Crypto Officer, perform zeroization in the following situations:

- **Before FIPS operation.** To prepare your switch for operation as a FIPS cryptographic module, perform zeroization after enabling FIPS mode and before FIPS operation.
- **Before non-FIPS operation.** To begin repurposing your switch for non-FIPS operation, perform zeroization before disabling FIPS mode on the switch or loading Junos OS packages that do not include FIPS mode.

  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.**

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

Related Documentation

- Zeroizing the System (FIPS Mode) on page 40
- Setting a Switch to FIPS Mode on page 41
- Disabling FIPS Mode on page 57
- Applying Tamper-Evident Seals to Switch Management Ports for FIPS Mode on page 7

Understanding FIPS Self-Tests

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

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

- **quicksec_kats**—KAT for QuickSec Toolkit cryptographic implementation
- **ssh_ipsec_kats**—KAT for SSH IPsec Toolkit cryptographic implementation

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

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

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

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

Related Documentation

- Understanding FIPS Error States and System Panic on page 16

Understanding FIPS Error States and System Panic

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

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

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

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

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

For details, see:

- FIPS System Panic on page 16
- Memory Allocation Error on page 17
- Error Recovery from Alternate Boot Media on page 17

FIPS System Panic

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

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

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

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

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

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

The following error states create a system panic:

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

- The switch failed a known answer test (KAT).
- The random number is not random.
- Signature generation failed.
- Signature verification failed.
- Certificate verification failed.
- Encryption or decryption failed.
- An environment error occurred.
- An error occurred in a pair-wise conditional test.

Memory Allocation Error

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

FIPS memory failures are logged as follows:

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

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

Error Recovery from Alternate Boot Media

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

If the alternate media are not functional, the switch might not be able to start up at all. In that case, the Crypto Officer must remove the tamper-evident seal from the USB port

and insert the removable boot media so that the system can boot normally and install Junos OS.

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

For this reason, be sure to keep the alternate media on the switch in a functional state by running the **request system snapshot** command after a successful upgrade.

Related Documentation

- Understanding System Snapshot on EX Series Switches
- Applying Tamper-Evident Seals to Switch Management Ports for FIPS Mode on page 7
- request system snapshot

Understanding Roles and Services for Junos OS in FIPS Mode

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

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

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

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

For details, see:

- Crypto Officer Role and Responsibilities on page 18
- FIPS User Role and Responsibilities on page 19
- What Is Expected of All FIPS Users on page 19

Crypto Officer Role and Responsibilities

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

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

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

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

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

- Set the initial root password.
- Reset user passwords for FIPS-approved algorithms during upgrades from Junos OS.
- Set up manual IPsec security associations (SAs) for these switch types:
  - EX9204, EX9208, and EX9214 switches with dual Routing Engines
- Examine log and audit files for events of interest.
- Erase user-generated files and data on (zeroize) the switch.

FIPS User Role and Responsibilities

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

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

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

What Is Expected of All FIPS Users

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

All FIPS users must:

- Keep all passwords confidential.
- Store switches and documentation in a secure area.
- Deploy switches in secure areas.
- Check audit files periodically.

- Conform to all other FIPS 140-2 security rules.
- Follow these guidelines:
  - Users are trusted.
  - Users abide by all security guidelines.
  - Users do not deliberately compromise security.
  - Users behave responsibly at all times.

Related Documentation

- Zeroizing the System (FIPS Mode) on page 40
- Configuring Crypto Officer and FIPS User Identification and Access on page 45

Understanding the Operational Environment for Junos OS in FIPS Mode

A Juniper Networks EX Series Ethernet Switch 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 switch in non-FIPS mode:

- Hardware Environment for Junos OS in FIPS Mode on page 20
- Software Environment for Junos OS in FIPS Mode on page 21
- Critical Security Parameters on page 21

Hardware Environment for Junos OS in FIPS Mode

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

For more information about the cryptographic boundary on your switch, see "Understanding Junos OS in FIPS Mode" on page 3.

An EX Series switch with redundant Routing Engines contains two separate cryptographic modules. Communications involving CSPs between these secure environments must take place using encryption.

BEST PRACTICE: We recommend that you, as Crypto Officer, apply tamper-evident seals to the USB port on all switches to adequately secure the cryptographic module. For details, see "Applying Tamper-Evident Seals to Switch Management Ports for FIPS Mode" on page 7.

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

Modular switches with two Routing Engines use IP Security (IPsec) and a private routing instance for communication between the Routing Engines. (See "Understanding Requirements for Secure Communication Between Routing Engines in FIPS Mode" on page 23.)

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

Software Environment for Junos OS in FIPS Mode

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

FIPS mode on EX9200 switches is available starting with Junos OS Release 14.1R4. The Junos OS in FIPS mode software environment is established after the Crypto Officer successfully enables FIPS mode on an EX Series switch. The Junos OS Release 14.1R4 image that includes FIPS mode is available on the Juniper Networks website and can be installed on an EX Series switch.

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

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

Critical Security Parameters

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

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

Table 5 on page 22 lists CSPs on switches running Junos OS.

Table 5: Critical Security Parameters

CSP	Description	Zeroize	Use
SSH-2 private host key	ECDSA key used to identify the host, generated the first time SSH is configured.	Zeroize command.	Used to identify the host.
SSH-2 session key	Session key used with SSH-2. and as a Diffie-Hellman private key. Encryption: 3DES, AES-128, AES-192, AES-256. MACs: HMAC-SHA-1, HMAC SHA1-96, HMAC SHA-2-256, HMAC SHA2-512. Key exchange: DH Group exchange (2048 ≤ key ≤ 8192), ECDH Prime curve NID_secp521r1 (NIST Curve P-521).	Power cycle and terminate session.	Symmetric key used to encrypt data between host and client.
User authentication key	Hash of the user's password: SHA-1, SHA-256, SHA-512.	Zeroize command.	Used to authenticate a user to the cryptographic module.
Crypto Officer authentication key	Hash of the Crypto Officer's password: SHA-1, SHA-256, SHA-512.	Zeroize command.	Used to authenticate the Crypto Officer to the cryptographic module.
RE-to-RE authentication key	HMAC key (manual IPsec SA): HMAC-SHA1-96 (20 bit), HMAC-SHA2-256 (32-bit).	Zeroize/explicitly delete command.	Used to authenticate the RE-to-RE IPSec connection.
RE-to-RE encryption key	TDES key (manual IPsec SA).	Zeroize/explicitly delete command.	Used in IPSec connection between REs.
HMAC DRBG seed	Seed for deterministic randon bit generator (DRBG).	Seed is not stored by the cryptographic module.	Used for seeding DRBG.
HMAC DRBG V value	The value (V) of output block length (outlen) in bits, which is updated each time another outlen bits of output are produced.	Power cycle.	A critical value of the internal state of DRBG.
HMAC DRBG key value	The current value of the outlen-bit key, which is updated at least once each time that the DRBG mechanism generates pseudorandom bits.	Power cycle.	A critical value of the internal state of DRBG.
NDRNG entropy	Used as entropy input string to the HMAC DRBG.	Power cycle.	A critical value of the internal state of DRBG.

In Junos OS in FIPS mode, all CSPs must enter and leave the cryptographic module in encrypted form. Any CSP encrypted with a non-approved algorithm is considered plain text by FIPS. However, as the Crypto Officer, you can enter user authentication data in plain text. During initial configuration, you can also enter the IP Security (IPsec) keys for communication between internal Routing Engines or for logical communications between

the Routing Engine and system processes in plain text on the console port (under manual key entry rules).

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

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

Related Documentation

- Understanding Requirements for Secure Communication Between Routing Engines in FIPS Mode on page 23
- Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms on page 11
- Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode on page 25
- Understanding Zeroization to Clear System Data for FIPS Mode on page 14
- Understanding Configuration Limitations and Restrictions on Junos OS in FIPS Mode on page 27
- Applying Tamper-Evident Seals to Switch Management Ports for FIPS Mode on page 7

Understanding Requirements for Secure Communication Between Routing Engines in FIPS Mode

The internal IPsec SA provides a secure way to mutually authenticate and encrypt communications between Routing Engines.

The cryptographic boundary on a modular switch is the Routing Engine. For this reason, EX9204, EX9208, and EX9214 switches with dual (redundant) Routing Engines require an internal, manual IP Security (IPsec) security association (SA) configured on each Routing Engine for the Routing Engines to communicate with each other. The Crypto Officer must use the console of each Routing Engine to configure the IPsec SA. Only four parameters are required: SA direction, security parameter index (SPI), a key value for authentication, and a key value for encryption. The SAs must be identical. All values, including the keys, must be statically specified in the configuration and must match on both ends of the connection. For communication to take place, each Routing Engine must have the same configured options.

For details, see:

- SA Direction on page 24
- SPI on page 24
- IPsec Keys on page 24
- IPsec Limitations on page 24

SA Direction

The internal, manual IPsec security association (SA) established by you, the Crypto Officer, on a Routing Engine can have the same SPI, authentication key, and encryption key for inbound and outbound communication, or one set of values for the inbound tunnel and another set for the outbound tunnel:

- Bidirectional—Apply the same SA values in both directions between Routing Engines.
- Inbound—Apply the SA values only to the inbound IPsec tunnel.
- Outbound—Apply the SA values only to the outbound IPsec tunnel.

If you do not configure the SA to be bidirectional, you must configure two unidirectional IPsec tunnels, one in each direction.

NOTE: We do not recommend the use of unidirectional IPsec tunnels.

SPI

The security parameter index (SPI) is an arbitrary value between 256 and 16639 that uniquely identifies the SA to use at the receiving Routing Engine. The sending Routing Engine uses the SPI to identify and select the SA it uses to secure every packet. The receiving Routing Engine uses the SPI to identify and select the encryption algorithm and key it uses to decrypt packets.

IPsec Keys

The internal, manual IPsec SA established by you, the Crypto Officer, on a Routing Engine requires an authentication key with a minimum message digest length of 20 bytes, as well as an encryption key. For this type of SA, we recommend you create preshared keys in hexadecimal format, for maximum key strength. Each key requires a specific cryptographic algorithm:

- Authentication algorithm
  - HMAC-SHA1-96 (40 hexadecimal characters)
  - HMAC-SHA2-256 (64 hexadecimal characters)
- Encryption algorithm
  - 3DES-CBC (48 hexadecimal characters)

You use the configuration mode command **prompt** to enter the value for each key twice. If the two entries do not match, the key is not set.

IPsec Limitations

On a switch with Junos OS in FIPS mode enabled, you cannot configure IPsec SAs to use the IPsec Authentication Header (AH) protocol or the Data Encryption Standard (DES) encryption algorithm. Instead, you must use the Encapsulating Security Payload (ESP)

protocol for both encryption and authentication and the 3DES-CBC algorithm for encryption.

Related Documentation

- Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms on page 11
- Enabling Internal Communications Between Routing Engines (FIPS Mode) on page 47
- For more information about IPsec, see the *Junos OS System Basics Configuration Guide*.

Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode

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

- **Length.** Passwords must contain between 10 and 20 characters.
- **Character set requirements.** Passwords must contain at least three of the following five defined character sets:
  - Uppercase letters
  - Lowercase letters
  - Digits
  - Punctuation marks
  - Keyboard characters not included in the other four sets—such as the percent sign (%) and the ampersand (&)
- **Authentication requirements.** All passwords and keys used to authenticate peers must contain at least 10 characters, and in some cases the number of characters must match the digest size—for example, 20 characters for SHA-1 authentication. For a list of supported cryptographic algorithms (ciphers), see "Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms" on page 11.

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

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

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

- Words that might be found in or exist as a permuted form in a system files such as **/etc/passwd**.
- The hostname of the system (always a first guess).
- Any word or phrase that appears in a dictionary or other well-known source, including dictionaries and thesauruses in languages other than English; works by classical or popular writers; or common words and phrases from sports, sayings, movies or television shows.
- Permutations on any of the above—for example, a dictionary word with letters replaced with digits (**r00t**) or with digits added to the end.
- Any machine-generated password. Algorithms reduce the search space of password-guessing programs and so must not be used.

Related Documentation

- Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms on page 11
- Understanding the Operational Environment for Junos OS in FIPS Mode on page 20

Understanding Remote Access for Junos OS in FIPS Mode

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

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

The Ethernet management (MGMT) port on the switch is disabled by default. To use the MGMT port, you must enable the **me0** interface and assign it an IP address if you have not already done so. For more information, see the *Junos OS System Basics Configuration Guide*.

In Junos OS in FIPS mode, all critical security parameters (CSPs) must enter and leave the cryptographic module in encrypted form. Any CSP encrypted with a non-approved algorithm is considered plain text by FIPS. However, as the Crypto Officer, you can enter user authentication data in plain text. During initial configuration, you can also enter the IP Security (IPsec) keys for communication between internal Routing Engines in plain text on the console port (under manual key entry rules).

Related Documentation

- Understanding Configuration Limitations and Restrictions on Junos OS in FIPS Mode on page 27
- *Junos OS System Basics and Services Command Reference*

Understanding Event Logging for Junos OS in FIPS Mode

A secure Juniper Networks Junos operating system (Junos OS) environment requires the auditing of configuration changes through the system log (syslog).

In addition, if configuration changes are audited, Junos OS can:

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

Event logging for Junos OS in FIPS mode must capture the following events:

- Changes to secret data in the configuration
- Committed changes
- Login and logout of users
- System startup and shutdown

BEST PRACTICE: **We recommend that FIPS logging also include:**

- **Capturing all changes to the configuration**
- **Storing logging information remotely**

Related Documentation

- *Configuring Event Logging for Junos OS in FIPS Mode*

Understanding Configuration Limitations and Restrictions on Junos OS in FIPS Mode

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

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

- Conforms to FIPS 140-2.
- Establishes a cryptographic boundary depending on the switch chassis type. On fixed-configuration chassis, the boundary is the switch case. On modular chassis, the boundary is the Routing Engine.
- Requires special installation procedures.
- Mandates the use of internal, manual IPsec tunnels with specific requirements.
- Limits services used for remote access.
- Allows only the use of approved ciphers.

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

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

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

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

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

Related Documentation

- Understanding Junos OS in FIPS Mode on page 3
- Understanding Requirements for Secure Communication Between Routing Engines in FIPS Mode on page 23
- Understanding Remote Access for Junos OS in FIPS Mode on page 26
- Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms on page 11
- Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode on page 25
- Understanding Event Logging for Junos OS in FIPS Mode on page 27
- Understanding FIPS Error States and System Panic on page 16
- Configuring the Console Port for FIPS Mode on page 53

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

You, as Crypto Officer, can enable and configure Junos OS in FIPS mode on your EX Series switch.

Before you begin enabling and configuring FIPS mode on the switch:

- Verify the secure delivery of your switch. See "Verifying Secure Delivery of the Product" on page 6.
- Apply tamper-evident seals. See "Applying Tamper-Evident Seals to Switch Management Ports for FIPS Mode" on page 7.

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

1. Install the Junos OS Release 14.1R4 image, if you have not already done so. See "Downloading and Installing Junos Software Packages (FIPS Mode)" on page 31.
2. Disable non-CLI user interfaces. See *Disabling Non-CLI User Interfaces (FIPS Mode)*.
3. Erase old passwords and rollback configurations and otherwise zeroize the system. See "Zeroizing the System (FIPS Mode)" on page 40.
4. Establish root password access according to FIPS guidelines. See "Establishing Root Password Access (FIPS Mode)" on page 44.
5. Enable FIPS mode, and commit. See "Setting a Switch to FIPS Mode" on page 41.

   NOTE: **On switches with multiple Routing Engines, ensure that you always use the commit synchronize command to commit configuration changes.**

6. Set IPsec security association (SA) algorithms and keys. See "Enabling Internal Communications Between Routing Engines (FIPS Mode)" on page 47.
7. Configure local login authentication for Crypto Officer access and other FIPS users. See "Configuring Crypto Officer and FIPS User Identification and Access" on page 45.
8. Configure the console port to log out automatically when you unplug the cable and require the root password for single-user mode. See "Configuring the Console Port for FIPS Mode" on page 53.
9. Configure FIPS logging to record events. See "Configuring Event Logging for Junos OS in FIPS Mode" on page 54.

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

Related Documentation

- Understanding Junos OS in FIPS Mode on page 3

CHAPTER 2

Enabling and Configuring Junos OS in FIPS Mode

- Downloading and Installing Junos Software Packages (FIPS Mode) on page 31
- Downloading Software Packages from Juniper Networks (FIPS Mode) on page 32
- Installing Software on an EX Series Switch with a Single Routing Engine (FIPS Mode) on page 33
- Installing Software on an EX Series Switch with Redundant Routing Engines (FIPS Mode) on page 35
- Zeroizing the System (FIPS Mode) on page 40
- Setting a Switch to FIPS Mode on page 41
- Establishing Root Password Access (FIPS Mode) on page 44
- Configuring Crypto Officer and FIPS User Identification and Access on page 45
- Enabling Internal Communications Between Routing Engines (FIPS Mode) on page 47
- Configuring the Console Port for FIPS Mode on page 53
- Configuring Event Logging for Junos OS in FIPS Mode on page 54
- Disabling FIPS Mode on page 57

Downloading and Installing Junos Software Packages (FIPS Mode)

EX Series EX9200 Ethernet switches can provide the security defined by Federal Information Processing Standards (FIPS) 140-2 Level 1 if these switches are operated in the Junos OS in FIPS mode. To operate in Junos OS in FIPS mode, the switch must have the following software packages installed:

- Junos OS for EX Series switches, Release 14.1R4
- Junos FIPS mode, Release 14.1R4

To install these software packages, perform the following tasks:

1. Download the Junos OS package and the Junos FIPS mode package from http://www.juniper.net/. See "Downloading Software Packages from Juniper Networks (FIPS Mode)" on page 32.
2. Connect locally to the console port of the active Routing Engine on the switch.

3. Copy the Junos OS and Junos FIPS mode software packages to the Routing Engine or Routing Engines. See the instructions that are appropriate for your switch:
   - Installing Software on an EX Series Switch with a Single Routing Engine (FIPS Mode) on page 33
   - Installing Software on an EX Series Switch with Redundant Routing Engines (FIPS Mode) on page 35

Related Documentation

- Installing Software on an EX Series Switch with a Single Routing Engine (FIPS Mode) on page 33
- Installing Software on an EX Series Switch with Redundant Routing Engines (FIPS Mode) on page 35

Downloading Software Packages from Juniper Networks (FIPS Mode)

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

- Junos OS for EX Series switches, Release 14.1R4
- Junos FIPS mode, Release 14.1R4

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

To download software packages from Juniper Networks:

1. Using a Web browser, follow the links to the download URL on the Juniper Networks webpage. For EX Series, because separate software packages are not provided for different locations, select **Canada and U.S. Version** regardless of your location:

   https://www.juniper.net/support/downloads/junos.html
2. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. Select the appropriate software package:
   - For Junos OS package, ensure that the name contains the correct switch name and number of the Junos OS release that is FIPS-certified on the switches.

     For example, **jinstall-ex-9200-14.1R4.n-domestic-signed.tgz**

NOTE: **domestic-signed** is appended to all EX Series package names. Although other Juniper Networks platforms use a **domestic** package for the United States and Canada and an **export** package for worldwide distribution, EX Series switches use **domestic** for both domestic and worldwide distribution.

- For the Junos FIPS mode package, select **fips-mode-i386-14.1R4.2-signed.tgz**

4. Download the software to a local host or to an internal software distribution site.
5. To install the Junos OS and Junos FIPS mode packages, perform one of the following tasks:
   - For switches with one Routing Engine, see "Installing Software on an EX Series Switch with a Single Routing Engine (FIPS Mode)" on page 33.
   - For switches with dual (redundant)l Routing Engines, see "Installing Software on an EX Series Switch with Redundant Routing Engines (FIPS Mode)" on page 35.

Related Documentation

- Installing Software on an EX Series Switch with a Single Routing Engine (FIPS Mode) on page 33
- Installing Software on an EX Series Switch with Redundant Routing Engines (FIPS Mode) on page 35

Installing Software on an EX Series Switch with a Single Routing Engine (FIPS Mode)

You can use this procedure to upgrade Junos OS on an EX9200 switch with a single Routing Engine. To upgrade software on an EX9200 switch running two Routing Engines, see "Installing Software on an EX Series Switch with Redundant Routing Engines (FIPS Mode)" on page 35.

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

1. Download the software package as described in "Downloading Software Packages from Juniper Networks (FIPS Mode)" on page 32.
2. If you have not already done so, connect to the console port on the switch from your management device, and log in to the Junos OS CLI. (For instructions, see Connecting and Configuring an EX Series Switch (CLI Procedure).)
3. (Optional) Back up the current software configuration to a second storage option. See the *Junos OS Installation and Upgrade Guide* for instructions on performing this task.
4. (Optional) Copy the software package to the switch. We recommend that you use FTP to copy the file to the **/var/tmp/** directory.

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

   user@switch> **request system software add *package***

   Replace ***package*** with one of the following paths:
   - For a software package in a local directory on the switch, use **/var/tmp/*package*.tgz**.
   - For a software package on a remote server, use one of the following paths, replacing *package* with the software package name—for example,

jinstall-ex-9200-14.1R4.n-domestic-signed.tgz (see "Downloading Software Packages from Juniper Networks (FIPS Mode)" on page 32):

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

NOTE: If you need to terminate the installation, do not reboot your switch; instead, finish the installation and then issue the **request system software delete *package*.tgz** command, where *package*.tgz is, for example, **jinstall-ex-9200-14.1R4.n-domestic-signed.tgz**. This is your last chance to stop the installation.

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

   user@switch> **request system reboot**

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

```
user@switch> show version
fpc0:
--------------------------------------------------------------------------
Hostname: switch
Model: ex9204
Junos: 14.1R4
JUNOS Base OS boot [14.1R4]
JUNOS Base OS Software Suite [14.1R4]
JUNOS 64-bit Kernel Software Suite [14.1R4]
JUNOS Crypto Software Suite [14.1R4]
JUNOS Packet Forwarding Engine Support (M/T/EX Common) [14.1R4]
JUNOS Packet Forwarding Engine Support (EX92XX) [14.1R4]
JUNOS Online Documentation [14.1R4]
JUNOS Services AACL Container package [14.1R4]
JUNOS Services Application Level Gateways [14.1R4]
JUNOS AppId Services [14.1R4]
JUNOS Border Gateway Function package [14.1R4]
JUNOS Services Captive Portal and Content Delivery Container package [14.1R4]
JUNOS Services HTTP Content Management package [14.1R4]
JUNOS IDP Services [14.1R4]
JUNOS Services Jflow Container package [14.1R4]
JUNOS Services LL-PDF Container package [14.1R4]
JUNOS Services MobileNext Software package [14.1R4]
JUNOS Services Mobile Subscriber Service Container package [14.1R4]
JUNOS Services NAT [14.1R4]
JUNOS Services PTSP Container package [14.1R4]
JUNOS Services RPM [14.1R4]
JUNOS Services Stateful Firewall [14.1R4]
JUNOS Voice Services Container package [14.1R4]
JUNOS Services Crypto [14.1R4]
JUNOS Services SSL [14.1R4]
JUNOS Services IPSec [14.1R4]
```

JUNOS platform Software Suite [14.1R4]
JUNOS Routing Software Suite [14.1R4]
JUNOS Runtime Software Suite [14.1R4]
JUNOS 64-bit Runtime Software Suite [14.1R4]
JUNOS py-base-i386 [14.1R4]
JUNOS FIPS mode utilities [14.1R4]

Related Documentation

- Troubleshooting Software Installation
- Understanding Software Installation on EX Series Switches

Installing Software on an EX Series Switch with Redundant Routing Engines (FIPS Mode)

For an EX9200 switch with redundant Routing Engines, you can minimize disruption to network operation during a Junos OS upgrade by upgrading the Routing Engines separately, starting with the backup Routing Engine.

CAUTION: If graceful Routing Engine switchover (GRES) or nonstop active routing (NSR) is enabled when you initiate a software installation, the software does not install properly. Make sure GRES and NSR are disabled before you begin the software installation.

You disable GRES by entering **deactivate chassis redundancy graceful-switchover** in configuration mode, as shown in "Preparing the Switch for the Software Installation" on page 36. If GRES is enabled, it is removed with this command.

By default, NSR is disabled. If NSR is enabled, you enter **delete routing-options nonstop-routing** in configuration mode, as shown in "Preparing the Switch for the Software Installation" on page 36, to disable it.

To upgrade the software package on an EX9200 switch with one installed Routing Engine, see "Installing Software on an EX Series Switch with a Single Routing Engine (FIPS Mode)" on page 33.

To upgrade redundant Routing Engines, you first install the new Junos OS release on the backup Routing Engine while keeping the currently running software version on the master Routing Engine. After making sure that the new software version is running correctly on the backup Routing Engine, you switch device control to the backup Routing Engine. Finally, you install the new software on the new backup Routing Engine.

To upgrade Junos OS on the switch, perform the following tasks:

- Preparing the Switch for the Software Installation on page 36
- Installing Software on the Backup Routing Engine on page 37
- Installing Software on the Default Master Routing Engine on page 38
- Returning Routing Control to the Default Master Routing Engine (Optional) on page 40

Preparing the Switch for the Software Installation

Perform the following steps before installing the software:

1. Log in to the master Routing Engine's console.

   For information on logging in to the Routing Engine through the console port, see Connecting and Configuring an EX Series Switch (CLI Procedure).

2. Enter the Junos OS CLI configuration mode:

   a. Start the CLI from the shell prompt:

      ```
      user@switch:RE% cli
      {master}
      user@switch>
      ```

   b. Enter configuration mode:

      ```
      user@switch> configure
      {master}[edit]
      user@switch#
      ```

3. Disable nonstop active routing (NSR):

   ```
   {master}[edit]
   user@switch# delete routing-options nonstop-routing
   ```

4. Disable graceful Routing Engine switchover (GRES):

   ```
   {master}[edit]
   user@switch# deactivate chassis redundancy graceful-switchover
   ```

5. Save the configuration change on both Routing Engines:

   ```
   {master}[edit]
   user@switch# commit synchronize
   ```

   NOTE: To ensure that the most recent configuration changes are committed before the software upgrade, perform this step even if nonstop active routing (NSR) and graceful Routing Engine switchover (GRES) were previously disabled.

6. Exit the CLI configuration mode:

   ```
   [edit]
   user@switch# exit
   ```

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

Installing Software on the Backup Routing Engine

After you have prepared the switch for software installation, install the software on the backup Routing Engine. During the installation, the master Routing Engine continues operations, minimizing the disruption to network traffic.

1. Download the software by following the procedures in "Downloading Software Packages from Juniper Networks (FIPS Mode)" on page 32.
2. Copy the software package to the switch. We recommend that you use FTP to copy the file to the **/var/tmp** directory.
3. Log in to the console of the backup Routing Engine.
4. Install the new software package:

   ```
   user@switch> request system software add  /var/tmp/package.tgz
   ```

   where ***package*.tgz** is, for example, **jinstall-ex-9200-14.1R4.n-domestic-signed.tgz**.

   NOTE: If you need to terminate the installation, do not reboot your switch; instead, finish the installation and then issue the **request system software delete *package*.tgz** command, where ***package*.tgz** is, for example, **jinstall-ex-9200-14.1R4.n-domestic-signed.tgz**. This is your last chance to stop the installation.

5. Reboot to start the new software:

   ```
   user@switch> request system reboot
   Reboot the system? [yes, no] (no) yes
   ```

   NOTE: You must reboot the switch to load the new installation of the Junos OS.

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

   ```
   {master}
   user@switch> show version
   Model: ex9204
   Junos: 14.1R4
   JUNOS Base OS boot [14.1R4]
   JUNOS Base OS Software Suite [14.1R4]
   JUNOS 64-bit Kernel Software Suite [14.1R4]
   JUNOS Crypto Software Suite [14.1R4]
   JUNOS Packet Forwarding Engine Support (M/T/EX Common) [14.1R4]
   JUNOS Packet Forwarding Engine Support (EX92XX) [14.1R4]
   JUNOS Online Documentation [14.1R4]
   JUNOS Services AACL Container package [14.1R4]
   JUNOS Services Application Level Gateways [14.1R4]
   ```

```
JUNOS AppId Services [14.1R4]
JUNOS Border Gateway Function package [14.1R4]
JUNOS Services Captive Portal and Content Delivery Container package [14.1R4]
JUNOS Services HTTP Content Management package [14.1R4]
JUNOS IDP Services [14.1R4]
JUNOS Services Jflow Container package [14.1R4]
JUNOS Services LL-PDF Container package [14.1R4]
JUNOS Services MobileNext Software package [14.1R4]
JUNOS Services Mobile Subscriber Service Container package [14.1R4]
JUNOS Services NAT [14.1R4]
JUNOS Services PTSP Container package [14.1R4]
JUNOS Services RPM [14.1R4]
JUNOS Services Stateful Firewall [14.1R4]
JUNOS Voice Services Container package [14.1R4]
JUNOS Services Crypto [14.1R4]
JUNOS Services SSL [14.1R4]
JUNOS Services IPSec [14.1R4]
JUNOS platform Software Suite [14.1R4]
JUNOS Routing Software Suite [14.1R4]
JUNOS Runtime Software Suite [14.1R4]
JUNOS 64-bit Runtime Software Suite [14.1R4]
JUNOS py-base-i386 [14.1R4]
JUNOS FIPS mode utilities [14.1R4]
```

Installing Software on the Default Master Routing Engine

To transfer control to the backup Routing Engine and then upgrade or downgrade the master Routing Engine software:

1. Log in to the master Routing Engine console port.
2. Transfer control to the backup Routing Engine:

   CAUTION: Because graceful Routing Engine switchover (GRES) is disabled, this switchover causes all line cards in the switch to reload. All network traffic passing through these line cards is lost during the line card reloads.

   ```
   user@switch> request chassis routing-engine master switch
   ```

3. Verify that the default backup Routing Engine (shown as **Slot 1** in the command output) is now the master Routing Engine:

   ```
   user@switch> show chassis routing-engine
   ```

   On switches with multiple Routing Engines, you will see:

   ```
   Routing Engine status:
    Slot 0:
      Current state          Master
      Election priority      Master (default)
   Routing Engine status:
    Slot 1:
      Current state          Backup
      Election priority      Backup (default)
   ```

On switches with a single Routing Engine, you will see:

```
Routing Engine status:
 Slot 0:
  Current state          Master
```

4. Install the new software package:

   ```
   user@switch> request system software add package.tgz
   ```

5. Reboot the Routing Engine:

   ```
   user@switch> request system reboot
   Reboot the system? [yes, no] (no) yes
   ```

   When the reboot completes, the prompt will reappear. Wait for this prompt to reappear before proceeding to the next step.

6. Log in to the default backup Routing Engine (slot 1) through the console port.

7. Reenable graceful Routing Engine switchover (GRES):

   ```
   [edit]
   user@switch# activate chassis redundancy graceful-switchover
   ```

   Re-enabling GRES allows any future Routing Engine switchovers to occur without loss of any network traffic.

8. Reenable nonstop active routing:

   ```
   [edit]
   user@switch# set routing-options nonstop-routing
   ```

   NOTE: Automatic commit synchronization is a requirement for nonstop active routing. If you have not yet enabled it, do so with the **set system commit synchronize** command.

9. Save the configuration change:

   ```
   [edit]
   user@switch# commit synchronize
   ```

10. Log in and verify the version of the software installed.

11. If you want to return routing control to the Routing Engine that was the master Routing Engine at the beginning of the procedure (the default master Routing Engine), go on to "Returning Routing Control to the Default Master Routing Engine (Optional)" on page 40.

Returning Routing Control to the Default Master Routing Engine (Optional)

The switch can maintain normal operations with the Routing Engine in slot 1 acting as the master Routing Engine after the software upgrade; therefore, perform this task only if you want to return routing control to the default master Routing Engine in slot 0.

1. Transfer routing control back to the default master Routing Engine:

   user@switch> **request chassis routing-engine master switch**

2. Verify that the default master Routing Engine (slot 0) is indeed the master Routing Engine:

   user@switch> **show chassis routing-engine**

   You will see:

```
Routing Engine status:
  Slot 0:
    Current state          Master
    Election priority      Master (default)
Routing Engine status:
  Slot 1:
    Current state          Backup
    Election priority      Backup (default)
```

Related Documentation

- Troubleshooting Software Installation
- Understanding Software Installation on EX Series Switches

Zeroizing the System (FIPS Mode)

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

For FIPS 140-2 compliance, you must zeroize the system to remove sensitive information before disabling FIPS mode on the switch.

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

To zeroize your switch:

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

1. From the CLI, enter

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

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

```
  Erase all data, including configuration and log files?  [yes, no] (no)
yes
  re1:
  --------------------------------------------------------------------------
  warning: zeroizing re1
  warning: zeroizing re0
  ...
  Rebooting after scrubbing memory...
  ...
```

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

3. When the system finishes rebooting and performing FIPS self-tests, proceed with FIPS configuration.

   - Go on to "Setting a Switch to FIPS Mode" on page 41.

Related Documentation

- Establishing Root Password Access (FIPS Mode) on page 44
- Enabling Internal Communications Between Routing Engines (FIPS Mode) on page 47
- Understanding Zeroization to Clear System Data for FIPS Mode on page 14

Setting a Switch to FIPS Mode

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

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

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

To enable FIPS mode in Junos OS on the switch:

1. Enter configuration mode:

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

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

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

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

3. Commit the configuration:

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

For switches with multiple Routing Engines:

```
{master:0[edit security]
root@switch# delete ipsec
{master:0}[edit security]
root@switch# commit synchronize
configuration check succeeds
[edit]
 'system'
   reboot is required to transition to FIPS level 1
commit complete
```

For switches with a single Routing Engine:

```
{master:0}[edit security]
root@switch# delete ipsec
{master:0}[edit security]
root@switch# commit
configuration check succeeds
[edit]
 'system'
   reboot is required to transition to FIPS level 1
commit complete
```

4. Reboot the switch:

For switches with multiple Routing Engines:

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

For switches with a single Routing Engine:

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

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

```
Verified jkernel-ex-14.1-20141229.0 signed by PackageProduction_12_1_0
Mounted jpfe-ex42x package on /dev/md9...
...
Creating initial configuration...mgd: Running FIPS Self-tests
mgd: Testing file integrity:
mgd:   File integrity Known Answer Test:            Passed
mgd: Testing crypto integrity:
mgd:   Crypto integrity Known Answer Test:          Passed
mgd: Testing kernel KATS:
mgd:   DES3-CBC Known Answer Test:                  Passed
...
mgd: FIPS Self-tests Passed
mgd: commit complete
[edit system services]
 'ftp'
   warning: not allowed in FIPS mode; ignored
[edit system services]
 'telnet'
   warning: not allowed in FIPS mode; ignored
[edit system services]
 'tftp'
   warning: not allowed in FIPS mode; ignored
mgd: commit complete
...
clean, 28550 free (22 frags, 3566 blocks, 0.0% fragmentation)


switch (ttyu0)

login:
```

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

```
--- JUNOS 14.1-20141229.0 built 2014-12-29 04:12:22 UTC
root@switch:fips>
```

Related Documentation

- Disabling FIPS Mode on page 57
- Understanding Junos OS in FIPS Mode on page 3

Establishing Root Password Access (FIPS Mode)

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

As Crypto Officer, you must establish a root password conforming to the FIPS password requirements in "Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode" on page 25. When you enable FIPS mode in Junos OS on the switch, you cannot configure passwords unless they meet this standard.

Local passwords are encrypted with the HMAC-SHA-1 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.

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

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

   ```
   % cli
     — JUNOS 14.1-20141229.0 built 2014-12-29 04:12:22 UTC
   root@switch:fips> configure
     Entering configuration mode
     [edit]
     root@switch:fips#
   ```

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

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

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

     Ensure that you follow the password guidelines in "Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode" on page 25.

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

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

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

Related Documentation

- Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode on page 25
- For more information about the root password and root logins, see the *Junos OS System Basics Configuration Guide*.
- Understanding Remote Access for Junos OS in FIPS Mode on page 26

Configuring Crypto Officer and FIPS User Identification and Access

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

- Configuring Crypto Officer Login Access on page 45
- Configuring FIPS User Login Access on page 46

Configuring Crypto Officer Login Access

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

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

To configure login access for a Crypto Officer:

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

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

2. Name the user "crypto-officer" and assign the Crypto Officer a user ID (for example, **6400**) and a class (for example, **super-user**). When you assign the class, you assign the permissions—for example, **secret**, **security**, **maintenance**, and **control**.

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

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

3. Following the guidelines in "Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode" on page 25, assign the Crypto Officer a plain-text password for login authentication. Set the password by typing a password after the prompts **New password** and **Retype new password**.

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

4. Optionally, display the configuration:

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

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

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

Otherwise, go on to "Configuring FIPS User Login Access" on page 46.

Configuring FIPS User Login Access

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

As the Crypto Officer you set up FIPS users. FIPS users can be granted permissions normally reserved for the Crypto Officer—for example, permission to zeroize the system.

To configure login access for a FIPS user:

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

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

2. Give the user a username, assign the FIPS user a user ID (for example, **6401**) and a class (for example, **operator**). When you assign the class, you assign the permissions—for example, **clear**, **configure**, **network**, **resetview**, and **view-configuration**.

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

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

3. Following the guidelines in "Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode" on page 25, assign the FIPS a plain-text password for login authentication. Set the password by typing a password after the prompts **New password** and **Retype new password**.

```
[edit]
```



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

4. Optionally, display the configuration:

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

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

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

Otherwise, go on to "Configuring the Console Port for FIPS Mode" on page 53.

Related Documentation

- Understanding Roles and Services for Junos OS in FIPS Mode on page 18

Enabling Internal Communications Between Routing Engines (FIPS Mode)

A switch in FIPS mode must have an internal IPsec security association (SA) manually configured to enable communications between Routing Engines. As Crypto Officer, you configure an identical IPsec SA through the console *of each Routing Engine*. Only four parameters are required: SA direction, Security Parameter Index (SPI) value, a key value for authentication, and a key value for encryption.

NOTE: You cannot configure DES-based IPsec SAs in Junos OS in FIPS mode. The internal IPsec SAs use HMAC-SHA1-96 authentication and 3DES-CBC encryption.

Manual SAs require no negotiation. All values, including the keys, are static and specified in the configuration. Manual SAs statically define the SPI values, algorithms, and keys to be used, and require matching configurations on both ends of the tunnel. Each peer must have the same configured options for communication to take place.

NOTE: When the switch is in FIPS mode, you cannot use the commit synchronize command until you have established an IPsec SA on each Routing Engine.

As Crypto Officer, you configure an internal IPsec SA for communication between Routing Engines by creating an SA on each Routing Engine with the following statements at the **[edit security]** hierarchy level:

```
[edit security]
ipsec {
  internal {
    security-association {
      manual
        direction (bidirectional | inbound | outbound) {
          protocol esp;
          spi spi-value;
          authentication {
            algorithm (hmac-sha1-96 | hmac-sha2-256);
            key (ascii-text ascii-text-string | hexadecimal hexadecimal-number);
          }
          encryption {
            algorithm 3des-cbc;
            key (ascii-text ascii-text-string |hexadecimal hexadecimal-number);
          }
        }
      }
    }
  }
}
```

You (as Crypto Officer) can also issue **load merge terminal** to perform this task:

```
[edit]
crypto-officer@switch:fips# load merge terminal
[Type ^D at a new line to end input]
security {
  ipsec {
    internal {
      security-association {
        manual {
          direction bidirectional {
            protocol esp;
            spi 512;
            encryption {
              algorithm 3des-cbc;
              key hexadecimal
                "$%ABC123";
            }
          }
        }
      }
    }
  }
}
load complete
```

```
{master:0}[edit]
crypto-officer@switch:fips# commit
configuration check succeeds
commit complete
```

The SA you configure can have two unidirectional tunnels—an inbound and outbound tunnel—or a single tunnel for bidirectional communication.

NOTE: We do not recommend the use of unidirectional IPsec tunnels.

If you do not configure the SA to be bidirectional, you must configure SA parameters for IPsec tunnels in both directions. The following instructions show how to configure a bidirectional IPsec SA on a Routing Engine:

- Configuring the IPsec SA on the Master Routing Engine on page 49
- Configuring the IPsec SA on the Backup Routing Engine on page 51

Configuring the IPsec SA on the Master Routing Engine

To configure an IPsec SA for communication between the dual Routing Engines of a modular switch in FIPS mode, you create an identical SA on each Routing Engine. If you are configuring the IPsec SA on a switch with a single Routing Engine, you have to configure the SA only once, on this single, master Routing Engine. You do not have to create the SA on any other Routing Engine.

To configure an internal, manual IPsec SA on the master Routing Engine:

1. Log in to the console of the master Routing Engine if you have not already done so, and enter configuration mode:

```
% cli
  — JUNOS 14.1-20141229.0 built 2014-12-29 04:12:22 UTC
  {master}
root@switch:fips> configure
  Entering configuration mode
  {master} [edit]
  root@switch:fips#
```

2. Specify the direction of the IPsec SA as bidirectional:

```
  {master} [edit]
root@switch:fips# set security ipsec internal security-association manual direction
  bidirectional
```

3. For the SA, specify the protocol (ESP is required) and an SPI between 256 and 16639—for example, 512:

```
  {master} [edit security ipsec internal security-association manual direction
  bidirectional]
root@switch:fips# set protocol esp spi 512
```

4. Specify the *authentication* algorithm (HMAC-SHA1-96 or HMAC-SHA2-256):

```
  {master} [edit security ipsec internal security-association manual direction
  bidirectional]
root@switch:fips# set authentication algorithm hmac-sha1-96
```

5. Specify the *encryption* algorithm (3DES-CBC is required):

```
  {master} [edit security ipsec internal security-association manual direction
  bidirectional]
```

```
root@switch:fips# set encryption algorithm 3des-cbc
```

6. In configuration mode, use the **prompt** command to enter a secret key value of 40 hexadecimal characters for *authentication*—for example, 309fc4be20f04e53e011b00744642d3fe66c2c7c:

```
{master} [edit]
root@switch:fips# prompt security ipsec internal security-association manual direction
  bidirectional authentication key hexadecimal
New hexadecimal (secret):
Retype new hexadecimal (secret):
```

7. Use **prompt** again to enter a secret key value of 48 hexadecimal characters for *encryption*—for example, b0344c61d8db38535ca8afceaf0bf12b881dc200c9833da7:

```
{master} [edit]
root@switch:fips# prompt security ipsec internal security-association manual direction
  bidirectional encryption key hexadecimal
New hexadecimal (secret):
Retype new hexadecimal (secret):
```

8. Use **show security** to verify that the key values for both authentication and encryption—and other required IPsec SA values—have been configured on the master Routing Engine. The key hexadecimal values are never displayed.

```
{master} [edit]
root@switch:fips# show security
ipsec {
  internal {
    security-association {
      manual {
        direction bidirectional {
          protocol esp;
          spi 512;
          authentication {
            algorithm hmac-sha1-96;
            key hexadecimal "<cipher-text>"; ## SECRET- DATA
          }
          encryption {
            algorithm 3des-cbc;
            key hexadecimal "<cipher-text>"; ## SECRET- DATA
          }
        }
      }
    }
  }
}
```

9. Commit the changes on the master Routing Engine:

```
{master} [edit]
root@switch:fips# commit
```

10. If you have configured the IPsec SA on the master Routing Engine of a switch with redundant Routing Engines, go on to "Configuring the IPsec SA on the Backup Routing Engine" on page 51.

Configuring the IPsec SA on the Backup Routing Engine

To configure an IPsec SA for communication between dual Routing Engines of a switch in FIPS mode, you create an *identical* SA on each Routing Engine. (To configure an IPsec SA on the other Routing Engine, see "Configuring the IPsec SA on the Master Routing Engine" on page 49.)

To configure an internal, manual IPsec SA on the backup Routing Engine that matches the SA on the master:

1. Log in to the console of the backup Routing Engine, and enter configuration mode:

```
% cli
  — JUNOS 14.1-20141229.0 built 2014-12-29 04:12:22 UTC
root@switch:fips> configure
  Entering configuration mode
  [edit]
  root@switch:fips#
```

2. Specify the direction of the IPsec SA—for example, **bidirectional**. The direction must be the same as that entered on the master Routing Engine.

```
  [edit]
root@switch:fips# set security ipsec internal security-association manual direction
  bidirectional
```

3. For the SA, specify the protocol (ESP is required) and an SPI between 256 and 16639—for example, 512. The SPI must be the same as that entered on the master Routing Engine.

```
  [edit security ipsec internal security-association manual direction bidirectional]
root@switch:fips# set protocol esp spi 512
```

4. Specify the *authentication* algorithm (HMAC-SHA1-96 or HMAC-SHA2-256):

```
  [edit security ipsec internal security-association manual direction  bidirectional]
root@switch:fips# set authentication algorithm hmac-sha1-96
```

5. Specify the *encryption* algorithm (3DES-CBC is required):

```
  [edit security ipsec internal security-association manual direction  bidirectional]
root@switch:fips# set encryption algorithm 3des-cbc
```

6. In configuration mode, use the **prompt** command to enter a secret key value of 40 characters for *authentication*—for example, 309fc4be20f04e53e011b00744642d3fe66c2c7c. The key value must be the same as that entered on the master Routing Engine.

```
[edit]
{master} [edit]
root@switch:fips# prompt security ipsec internal security-association manual direction
  bidirectional authentication key hexadecimal
New hexadecimal (secret):
Retype new hexadecimal (secret):
```

7. Use **prompt** again to enter a secret key value of 48 hexadecimal characters for *encryption*—for example, b0344c61d8db38535ca8afceaf0bf12b881dc200c9833da7. The key value must be the same as that entered on the master Routing Engine.

```
[edit]
root@switch:fips# prompt security ipsec internal security-association manual direction
  bidirectional encryption key hexadecimal
New hexadecimal (secret):
Retype new hexadecimal (secret):
```

8. Use **show security** to verify that the key values for both authentication and encryption—and other required IPsec SA values—have been configured on the backup Routing Engine and are identical to the IPsec SA values configured on the master Routing Engine. The key hexadecimal values are never displayed.

```
[edit]
root@switch:fips# show security
ipsec {
  internal {
    security-association {
      manual {
        direction bidirectional {
          protocol esp;
          spi 512;
          authentication {
            algorithm hmac-sha1-96;
            key hexadecimal "<cipher-text>"; ## SECRET-DATA
          }
          encryption {
            algorithm 3des-cbc;
            key hexadecimal "<cipher-text>"; ## SECRET-DATA
          }
        }
      }
    }
  }
}
```

9. Commit the changes on the backup Routing Engine:

```
[edit]
root@switch:fips# commit
```

Related Documentation

- For information about IP Security (IPsec) monitoring and troubleshooting, see the *Junos OS System Basics and Services Command Reference*.
- Understanding Requirements for Secure Communication Between Routing Engines in FIPS Mode on page 23

Configuring the Console Port for FIPS Mode

You initially connect to your switch through an RJ-45 serial cable plugged into the console port. From the console port, you can use the CLI to configure the switch. By default, the console port is enabled.

For FIPS compliance, your user account must be automatically logged out when you unplug the serial console cable from a switch running Junos OS in FIPS mode. Junos OS in FIPS mode automatically logs out of your user account when you disconnect because the **log-out-on-disconnect** configuration statement is enabled by default. Also, Junos OS in FIPS mode does not automatically disable root password recovery, so you must explicitly configure that by specifying the **insecure** configuration statement.

CAUTION: If you disable root password recovery by setting the insecure statement, the root password can be recovered only if the Crypto Officer logs in to the system and modifies the configuration by removing that setting.

To configure automatic logout on disconnection:

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

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

2. Configure the switch to automatically log out of a user session when the console port cable is unplugged:

   ```
     [edit]
   crypto-officer@switch:fips# set system ports console log-out-on-disconnect
   ```

3. Configure the switch to disable root password recovery:

   ```
     [edit]
   crypto-officer@switch:fips# set system ports console insecure
   ```

4. Optionally, display the configuration:

   ```
   [edit]
   crypto-officer@switch:fips# edit system
   [edit system]
   ports {
     console {
       log-out-on-disconnect;
       insecure;
     }
   }
   ```

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

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

```
commit complete
crypto-officer@switch:fips# exit
crypto-officer@switch:fips> exit
```

Otherwise, go on to "Configuring Event Logging for Junos OS in FIPS Mode" on page 54.

Related Documentation

- For information about local console configuration and more information about console port options, see the *Junos OS System Basics Configuration Guide*.

Configuring Event Logging for Junos OS in FIPS Mode

The system log (syslog) files record system events in Junos OS.

BEST PRACTICE: **Because of the sensitive nature of information used to configure and operate a system running Junos OS in FIPS mode, we recommend that you as Crypto Officer log certain events and examine the logs frequently.**

For Junos OS in FIPS mode, we recommend that you as Crypto Officer configure the system log to record the following events. You can log more types of information, but these events are particularly important to the Junos OS in FIPS mode environment.

- All authorization events—stored in **/var/log/authlog** and **/var/log/auditlog**
- All interactive commands and configuration change events, including secrets—stored in **/var/log/auditlog**
- All events of moderate severity—stored in **/var/log/messages**

In Junos OS in FIPS mode, the actual secrets themselves are not logged. When Junos OS encounters secret information that it would ordinarily log, it replaces the secrets with the token **/* SECRET-DATA */**. For example, a secret string entered as part of the command line is not logged, but is replaced with the following token:

```
Feb 10 23:57:01 shmoo mgd[15558]: UI_CFG_AUDIT_SET_SECRET: User 'root' set: [system
 tacplus-server 172.17.12.120 secret]
Feb 10 23:57:01 shmoo mgd[15558]: UI_CMDLINE_READ_LINE: User 'root', command 'set
 system tacplus-server frodo secret /* SECRET-DATA */ '
```

The following system log configuration is recommended for Junos OS in FIPS mode:

```
[edit]
system {
   syslog {
      file authlog {
         authorization info;
      }
      file messages {
         any any;
      }
      file auditlog {
         authorization info;
```

```
        change-log any;
        interactive-commands any;
    }
  }
}
```

You can configure the system to log events to a local file or to a remote server:

- Configuring Event Logging to a Local File on page 55
- Configuring Event Logging to a Remote Server on page 56

Configuring Event Logging to a Local File

To configure the system to store the recommended information for Junos OS in FIPS mode, you create log files on the switch called **authlog**, **auditlog**, and **messages**.

(You can also store event logs on a secure, remote server. For details, see "Configuring Event Logging to a Remote Server" on page 56.)

To configure the system to log the recommended events to local files on the switch in the **/var/log/** directory:

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

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

2. Configure a file named **authlog** to store informational messages from the authorization system in **/var/log/authlog** on the switch:

   ```
   [edit]
   crypto-officer@switch:fips# set system syslog file authlog authorization info
   ```

3. Configure a file named **auditlog** to store informational messages from the authorization system, all configuration changes, and all commands entered through the CLI—including secrets—in **/var/log/auditlog** on the switch:

   ```
   [edit]
   crypto-officer@switch:fips# set system syslog file auditlog authorization info
   [edit]
   crypto-officer@switch:fips# set system syslog file auditlog change-log any
   [edit]
   crypto-officer@switch:fips# set system syslog file auditlog interactive-commands
   any
   ```

4. Configure a file named **messages** to store notices of all events of moderate severity in **/var/log/messages** on the switch:

   ```
   [edit]
   crypto-officer@switch:fips# set system syslog file messages any any
   ```

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

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

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

To view the contents of the log files, enter the following operational mode commands:

```
crypto-officer@switch:fips> file show /var/log/authlog
crypto-officer@switch:fips> file show /var/log/auditlog
crypto-officer@switch:fips> file show /var/log/messages
```

Configuring Event Logging to a Remote Server

In addition to storing log files in the local **/var/log/** directory on the switch (see "Configuring Event Logging to a Local File" on page 55), you can export the information in system log files to a secure, remote server.

BEST PRACTICE: We recommend that you store system log files remotely.

To configure the system to log the recommended events to a remote host:

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

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

2. Configure the system to import informational messages from the authorization system and store them on a remote host—for example, a host named **Secure-Audit-Server**:

   ```
   [edit]
   crypto-officer@switch:fips# set system syslog host Secure-Audit-Server authorization
    info
   ```

3. Configure the system to import all configuration changes and all commands entered through the CLI—including secrets—and store them on the remote host **Secure-Audit-Server**:

   ```
   [edit]
   crypto-officer@switch:fips# set system syslog host Secure-Audit-Server change-log
    any
   [edit]
   crypto-officer@switch:fips# set system syslog host Secure-Audit-Server
   interactive-commands any
   ```

4. Configure the system to import all notices of events of moderate severity and store them on the remote host **Secure-Audit-Server**:

   ```
   [edit]
   crypto-officer@switch:fips# set system syslog host Secure-Audit-Server any notice
   ```

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

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

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

Related Documentation

- Understanding Event Logging for Junos OS in FIPS Mode on page 27
- For more information about system logging, see the *Junos OS System Basics Configuration Guide*.
- To configure features on the switch that are not specific to FIPS mode, see the EX Series hardware and software documentation at http://www.juniper.net/techpubs/en_US/release-independent/information-products/pathway-pages/ex-series/product/index.html.

Disabling FIPS Mode

As Crypto Officer, you might need to disable FIPS mode on your switch to return it to non-FIPS operation.

BEST PRACTICE: **For FIPS 140-2 compliance, you must zeroize the system to remove sensitive information before disabling FIPS mode on the switch.**

To disable FIPS mode in Junos OS:

1. Log in to the switch with your Crypto Officer password if you have not already done so:

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

2. Follow the instructions in "Zeroizing the System (FIPS Mode)" on page 40 to zeroize the switch.

3. When the system finishes rebooting, log in to the switch again with your Crypto Officer password and enter configuration mode:

   ```
   — JUNOS 14.1-20141229.0 built 2014-12-29 04:12:22 UTC
   crypto-officer@switch> configure
   Entering configuration mode
   [edit]
   crypto-officer@switch#
   ```

4. Commit the configuration change:

   ```
   [edit]
   crypto-officer@switch:fips# commit
   configuration check succeeds commit complete
   ```

Related Documentation

- Setting a Switch to FIPS Mode on page 41

CHAPTER 3

Administering Junos OS in FIPS Mode on an EX Series Switch

- Verifying That FIPS Self-Tests Are Taking Place on page 59

Verifying That FIPS Self-Tests Are Taking Place

Purpose Verify that FIPS self-tests are taking place on the switch.

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

After a self-test is run on the switch, the system log (syslog) file is updated to display the known answer tests (KATs) that are executed. To view the system log file, issue the command **file show /var/log/messages**:

```
user@switch:fips> file show /var/log/messages
Oct 25 22:28:50  host kernel_kats[5358]: DES3-CBC Known Answer Test: Passed

Oct 25 22:28:50  host kernel_kats[5358]: HMAC-SHA1 Known Answer Test: Passed

Oct 25 22:28:50  host kernel_kats[5358]: HMAC-SHA2-256 Known Answer Test: Passed

Oct 25 22:28:50  host kernel_kats[5358]: SHA-2 Known Answer Test: Passed

Oct 25 22:28:50  host kernel_kats[5358]: AES128-CMAC Known Answer Test: Passed

Oct 25 22:28:50  host kernel_kats[5358]: AES-CBC Known Answer Test: Passed

Oct 25 22:28:50  host kernel_kats[5358]: FIPS Known Answer Tests passed

Oct 25 22:28:50  host md_kats[5360]: HMAC-SHA1 Known Answer Test: Passed

Oct 25 22:28:50  host md_kats[5360]: HMAC-SHA2-256 Known Answer Test: Passed

Oct 25 22:28:50  host md_kats[5360]: FIPS Known Answer Tests passed

Oct 25 22:28:50  host openssl_kats[5362]: FIPS RNG Known Answer Test: Passed

Oct 25 22:28:57  host openssl_kats[5362]: FIPS DSA Known Answer Test: Passed

Oct 25 22:28:57  host openssl_kats[5362]: FIPS ECDSA Known Answer Test: Passed

Oct 25 22:28:58  host openssl_kats[5362]: FIPS ECDH Known Answer Test: Passed

Oct 25 22:29:00  host openssl_kats[5362]: FIPS RSA Known Answer Test: Passed
```

```
Oct 25 22:29:00  host openssl_kats[5362]: DES3-CBC Known Answer Test: Passed

Oct 25 22:29:00  host openssl_kats[5362]: HMAC-SHA1 Known Answer Test: Passed

Oct 25 22:29:00  host openssl_kats[5362]: SHA-2 Known Answer Test: Passed

Oct 25 22:29:00  host openssl_kats[5362]: AES-CBC Known Answer Test: Passed

Oct 25 22:29:00  host openssl_kats[5362]: ECDSA-SIGN Known Answer Test: Passed

Oct 25 22:29:00  host openssl_kats[5362]: KDF-IKE-V1 Known Answer Test: Passed

Oct 25 22:29:00  host openssl_kats[5362]: FIPS Known Answer Tests passed

Oct 25 22:29:00  host ssh_ipsec_kats[5364]: DES3-CBC Known Answer Test: Passed

Oct 25 22:29:00  host ssh_ipsec_kats[5364]: HMAC-SHA1 Known Answer Test: Passed

Oct 25 22:29:00  host ssh_ipsec_kats[5364]: HMAC-SHA2-256 Known Answer Test:
Passed

Oct 25 22:29:00  host ssh_ipsec_kats[5364]: SHA-2 Known Answer Test: Passed

Oct 25 22:29:00  host ssh_ipsec_kats[5364]: AES-CBC Known Answer Test: Passed

Oct 25 22:29:01  host ssh_ipsec_kats[5364]: SSH-RSA-ENC Known Answer Test: Passed

Oct 25 22:29:03  host ssh_ipsec_kats[5364]: SSH-RSA-SIGN Known Answer Test: Passed

Oct 25 22:29:03  host ssh_ipsec_kats[5364]: KDF-IKE-V1 Known Answer Test: Passed

Oct 25 22:29:03  host ssh_ipsec_kats[5364]: FIPS Known Answer Tests passed
```

Meaning The system log file displays the date and time at which each KAT was executed, the name of the test, and its status.

Related Documentation

- Understanding FIPS Self-Tests on page 15

CHAPTER 4

Configuration Statements for Junos OS in FIPS Mode

- algorithm (FIPS) on page 62
- authentication (FIPS) on page 62
- direction (FIPS) on page 63
- encryption (FIPS) on page 64
- fips (FIPS) on page 64
- internal (FIPS) on page 65
- ipsec (FIPS) on page 66
- key (FIPS) on page 67
- level (FIPS) on page 68
- manual (FIPS) on page 69
- protocol esp (FIPS) on page 69
- security (FIPS) on page 70
- security-association (FIPS) on page 71
- spi (FIPS) on page 72

algorithm (FIPS)

Syntax algorithm <*name*>;

Hierarchy Level [edit security ipsec internal security-association manual direction authentication],
[edit security ipsec internal security-association manual direction encryption]

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

Description Select the authentication and encryption algorithm for an IPsec security association (SA) between internal Routing Engines.

Options **3des-cbc**—Use a triple-Data Encryption Standard (3DES) cyclical block check (CBC) as the encryption algorithm.

Required Privilege Level maintenance—To add and view this statement in the configuration.

Related Documentation
- Enabling Internal Communications Between Routing Engines (FIPS Mode) on page 47

authentication (FIPS)

Syntax
```
authentication {
  algorithm (hmac-sha1-96 | hmac-sha2-256);
  key (ascii-text ascii-text-string | hexadecimal key-value);
}
```

Hierarchy Level [edit security ipsec internal security-association manual direction]

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

Description Define the authentication parameters for communication between internal Routing Engines.

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

The remaining statements are explained separately.

Required Privilege Level maintenance—To view and add this statement in the configuration.

Related Documentation
- Enabling Internal Communications Between Routing Engines (FIPS Mode) on page 47

direction (FIPS)

Syntax

```
direction (bidirectional | inbound | outbound) {
  protocol esp ;
  spi spi-value;
  authentication {
    algorithm (hmac-sha1-96 | hmac-sha2-256);
    key (ascii-text ascii-text-string| hexadecimal key-value);
  }
  encryption {
    algorithm 3des-cbc;
    key (ascii-text ascii-text-string| hexadecimal key-value);
  }
}
```

Hierarchy Level [edit security ipsec internal security-association manual]

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

Description Establish a manual security association (SA) for communication between internal Routing Engines.

Options

bidirectional—Apply the same SA values in both directions between Routing Engines.

inbound—Apply these SA properties only to the inbound IPsec tunnel.

outbound—Apply these SA properties only to the outbound IPsec tunnel.

The remaining statements are explained separately.

Required Privilege Level maintenance—To view and add this statement in the configuration.

Related Documentation

- Enabling Internal Communications Between Routing Engines (FIPS Mode) on page 47

encryption (FIPS)

Syntax

```
encryption {
  algorithm 3des-cbc;
  key (ascii-text ascii-text-string| hexadecimal key-value);
}
```

Hierarchy Level [edit security ipsec internal security-association manual direction]

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

Description Define the encryption parameters for communication between internal Routing Engines.

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

The remaining statements are explained separately.

Required Privilege Level maintenance—To view and add this statement in the configuration.

Related Documentation

- Enabling Internal Communications Between Routing Engines (FIPS Mode) on page 47

fips (FIPS)

Syntax

```
fips {
  level level;
```

Hierarchy Level [edit system]

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

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

The remaining statements are explained separately.

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

Related Documentation

- Setting a Switch to FIPS Mode on page 41
- Disabling FIPS Mode on page 57

internal (FIPS)

Syntax

```
internal {
  security-association {
    manual
      direction (bidirectional | inbound | outbound) {
        protocol esp;
        spi spi-value;
        authentication {
          algorithm (hmac-sha1-96 | hmac-sha2-256);
          key (ascii-text ascii-text-string| hexadecimal key-value);
        }
        encryption {
          algorithm 3des-cbc;
          key (ascii-text ascii-text-string| hexadecimal key-value);
        }
      }
    }
  }
}
```

Hierarchy Level [edit security ipsec]

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

Description Define an internal security association (SA) for communication between internal Routing Engines.

The remaining statements are explained separately.

Required Privilege Level maintenance—To view and add this statement in the configuration.

Related Documentation

- Enabling Internal Communications Between Routing Engines (FIPS Mode) on page 47

ipsec (FIPS)

Syntax

```
ipsec {
  internal {
    security-association {
      manual
        direction (bidirectional | inbound | outbound) {
          protocol esp;
          spi spi-value;
          authentication {
            algorithm (hmac-sha1-96 | hmac-sha2-256);
            key (ascii-text ascii-text-string| hexadecimal key-value);
          }
          encryption {
            algorithm 3des-cbc;
            key (ascii-text ascii-text-string| hexadecimal key-value);
          }
        }
      }
    }
  }
}
```

Hierarchy Level [edit security]

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

Description Set up an Internet Protocol Security (IPsec) hierarchy in which you can define a manual internal security association (SA) for communication between internal Routing Engines.

The remaining statements are explained separately.

Required Privilege Level maintenance—To view and add this statement in the configuration.

Related Documentation

- Enabling Internal Communications Between Routing Engines (FIPS Mode) on page 47

key (FIPS)

Syntax key (ascii-text *ascii-text-string* | hexadecimal *key-value*);

Hierarchy Level [edit security ipsec internal security-association manual direction authentication], [edit security ipsec internal security-association manual direction encryption]

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

Description Following FIPS password guidelines, use the **prompt** command, in configuration mode, to specify one key (password) value each for the authentication algorithm and the encryption algorithm in an internal IPsec security association (SA) between internal Routing Engines. You must specify a value for each algorithm.

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

You must enter the hexadecimal value for each key twice, and the strings entered must match; otherwise, the key is not set. The hexadecimal key value is never displayed in plain text.

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

- For the authentication algorithm (HMAC-SHA1-96), enter a key consisting of 40 hexadecimal characters.
- For the authentication algorithm (HMAC-SHA2-256), enter a key consisting of 64 hexadecimal characters.
- For the encryption algorithm (3DES-CBC), enter a key consisting of 48 hexadecimal characters.

Required Privilege Level maintenance—To add and view this statement in the configuration.

Related Documentation

- Enabling Internal Communications Between Routing Engines (FIPS Mode) on page 47
- Understanding Password Specifications and Guidelines for Junos OS in FIPS Mode on page 25

level (FIPS)

Syntax level *level*;

Hierarchy Level [edit system fips]

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

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

Compared to non-FIPS mode, Junos OS in FIPS mode is a nonmodifiable operational environment with limitations. (See "Understanding Configuration Limitations and Restrictions on Junos OS in FIPS Mode" on page 27.)

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

Range: 0 through 4

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

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

Related Documentation

- Setting a Switch to FIPS Mode on page 41
- Disabling FIPS Mode on page 57

manual (FIPS)

Syntax

```
manual {
  direction (bidirectional | inbound | outbound) {
    protocol esp;
    spi spi-value;
    authentication {
      algorithm (hmac-sha1-96 | hmac-sha2-256);
      key (ascii-text ascii-text-string| hexadecimal key-value);
    }
    encryption {
      algorithm 3des-cbc;
      key (ascii-text ascii-text-string| hexadecimal key-value);
    }
  }
}
```

Hierarchy Level [edit security ipsec internal security-association]

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

Description Define a manual security association (SA) for communication between internal Routing Engines.

The remaining statements are explained separately.

Required Privilege Level maintenance—To view and add this statement in the configuration.

Related Documentation
- Enabling Internal Communications Between Routing Engines (FIPS Mode) on page 47

protocol esp (FIPS)

Syntax protocol esp;

Hierarchy Level [edit security ipsec internal security-association manual direction]

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

Description Specify the protocol (esp) used for an internal IPsec security association (SA) between internal Routing Engines.

Options **esp**—Use the TCP/IP Encapsulating Security Protocol (ESP).

Required Privilege Level maintenance—To add and view this statement in the configuration.

Related Documentation
- Enabling Internal Communications Between Routing Engines (FIPS Mode) on page 47

security (FIPS)

Syntax

```
security {
  ipsec {
    internal {
      security-association {
        manual {
          direction (bidirectional | inbound | outbound) {
            protocol esp;
            spi spi-value;
            authentication {
              algorithm (hmac-sha1-96 | hmac-sha2-256);
              key (ascii-text ascii-text-string| hexadecimal key-value);
            }
            encryption {
              algorithm 3des-cbc;
              key (ascii-text ascii-text-string| hexadecimal key-value);
            }
          }
        }
      }
    }
  }
}
```

Hierarchy Level [edit]

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

Description Define security parameters for communication between internal Routing Engines.

The remaining statements are explained separately.

Required Privilege Level security—To view and add this statement in the configuration.

Related Documentation

- Enabling Internal Communications Between Routing Engines (FIPS Mode) on page 47

security-association (FIPS)

Syntax

```
security-association {
  manual {
    direction (bidirectional | inbound | outbound) {
      protocol esp;
      spi spi-value;
      authentication {
        algorithm (hmac-sha1-96 | hmac-sha2-256);
        key (ascii-text ascii-text-string| hexadecimal key-value);
      }
      encryption {
        algorithm 3des-cbc;
        key (ascii-text ascii-text-string| hexadecimal key-value);
      }
    }
  }
}
```

Hierarchy Level [edit security ipsec internal]

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

Description Define an IPsec security association (SA) for communication between internal Routing Engines.

The remaining statements are explained separately.

Required Privilege Level maintenance—To view and add this statement in the configuration.

Related Documentation

- Enabling Internal Communications Between Routing Engines (FIPS Mode) on page 47

spi (FIPS)

Syntax spi *spi-value*;

Hierarchy Level [edit security ipsec internal security-association manual direction]

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

Description Specify the security parameter index (SPI) value for the internal IPsec security association (SA) between internal Routing Engines. The SPI is an arbitrary value that uniquely identifies the SA to use at the receiving Routing Engine. The sending Routing Engine uses the SPI to identify and select the SA it uses to secure every packet. The receiving Routing Engine uses the SPI to identify and select the encryption algorithm and key it uses to decrypt packets.

Options ***spi-value***—Integer to use for this SPI.

Range: 256 through 16639

Required Privilege Level maintenance—To add and view this statement in the configuration.

Related Documentation

- Enabling Internal Communications Between Routing Engines (FIPS Mode) on page 47

CHAPTER 5

Operational Commands for Junos OS in FIPS Mode

- request system zeroize (FIPS)

request system zeroize (FIPS)

Syntax **request system zeroize**

Release Information Command introduced in Junos OS Release 12.1 for EX Series switches.

Description Erase and replace with zeros all user-created data from Routing Engines.

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

Required Privilege Level maintenance

Related Documentation
- Understanding Zeroization to Clear System Data for FIPS Mode on page 14
- Zeroizing the System (FIPS Mode) on page 40

List of Sample Output request system zeroize (FIPS) on page 74

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

Sample Output

request system zeroize (FIPS)

```
crypto-officer@switch:fips> request system zeroize
warning:System will be rebooted and may not boot without configuration
Erase all data, including configuration and log files? [yes, no] (no)  yes
re1:
--------------------------------------------------------------------------
warning: zeroizing re1
warning: zeroizing re0
...
Rebooting after scrubbing memory...
...
```