

Chapter 2

Upgrading and Configuring JUNOS-FIPS

This chapter describes the major characteristics of JUNOS-FIPS, including the upgrade procedure. In this chapter, the term “cryptographic module” applies to JUNOS-FIPS running on the Routing Engine.

This chapter discusses the following topics:

- Critical Security Parameters on page 9
- Upgrading a JUNOS Software Router to JUNOS-FIPS on page 10
- Entering Multi-User Mode on page 11
- Configuring the JUNOS-FIPS Router on page 12
- Errors and Error Status Messages on page 13
- Recommended JUNOS-FIPS System Log Configuration on page 14
- Command Summary on page 15

Critical Security Parameters

Critical security parameters (CSPs) are defined as security-related information (including cryptographic keys and authentication data, such as passwords), the disclosure or modification of which can compromise the security of a cryptographic module or the security of the information protected by the module.

In JUNOS-FIPS, user authentication data can be entered in plain text. During initial configuration, the Routing-Engine-to-Routing-Engine IP Security (IPSec) key can also be entered in plain text on the console (under manual key entry rules). Otherwise all CSPs must enter and leave the cryptographic module in encrypted form. In general, configuration should be done with secure shell (SSH) or Transport Layer Security (TLS) connections.

Services such as RADIUS and TACACS+ can still use clear text because FIPS 140 Level 2 or below allows for authentication data to be sent in clear text. For strict compliance, the RADIUS or TACACS+ server secret must be 10 characters or longer.

Local passwords are encrypted using HMAC-SHA1. Password recovery is not possible in JUNOS-FIPS. JUNOS-FIPS cannot boot into single-user mode without the correct root password.

If JUNOS-FIPS encounters a FIPS error, this condition halts all cryptographic processing, stops data flows, creates a system panic, and displays only status messages on the console.

For example, a FIPS error is logged as:

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

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

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

Memory failures are logged as well:

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

Upgrading a JUNOS Software Router to JUNOS-FIPS

To upgrade a Juniper Networks router running JUNOS software to JUNOS-FIPS, perform the following tasks in the order listed:

- Install the router under normal operating procedures. For more information, see the *JUNOS System Basics Configuration Guide*.
- Download the correct JUNOS-FIPS software package from www.juniper.net.
- Connect locally to the active Routing Engine console port.
- Copy the JUNOS-FIPS software to both Routing Engines.
- Upgrade to JUNOS-FIPS using the `request system software add reboot junos-juniper-7.2*-fips.tgz` command. There is no “-signed” version of the JUNOS-FIPS software. All JUNOS-FIPS software is signed. The router reboots in JUNOS-FIPS and becomes a cryptographic module. For more details about adding system software, see the *JUNOS System Basics Configuration Guide*.
 - When upgrading from JUNOS Release 6.4, you should use the `no-validate` option on the JUNOS-FIPS software module. You can validate upgrades to JUNOS-FIPS from JUNOS Release 7.x. Upgrade to JUNOS-FIPS from JUNOS Release 6.4 using the `request system software add reboot no-validate junos-juniper-7.2*-fips.tgz` command.
- For hardware configurations with dual Routing Engines, configure a manual IPsec security association (SA) for Routing-Engine-to-Routing-Engine communication. You cannot use the `commit sync` command until you have established an IPsec SA on each Routing Engine.



NOTE: Downgrading a JUNOS-FIPS cryptographic module to non-JUNOS-FIPS JUNOS software is not supported.

Attempts to install non-JUNOS-FIPS JUNOS software on a router running JUNOS-FIPS will generate the following error message:

```

junos-fips-user@host> request system software add
jinstall-7.2B1.2-domestic-signed.tgz
WARNING: Package jinstall-7.2B1.2-domestic-signed is not compatible with this
system.
WARNING: Please install a supported package (junos-juniper-*.tgz).

```

Juniper Networks does not support downgrades to non-JUNOS-FIPS software packages, but this might be necessary in certain test environments. You can install non-JUNOS-FIPS JUNOS software from PCMCIA media.

Entering Multi-User Mode

When JUNOS-FIPS is booted into single-user mode, a reboot is necessary to enter multi-user mode for normal operation with all services fully functional. You cannot exit the single-user shell and allow the system to come up in multi-user mode. A reboot loads the IPSec kernel module necessary for Routing-Engine-to-Routing-Engine communications in a multiple Routing Engine configuration.

```

Hit [Enter] to boot immediately, or space bar for command prompt. Booting [kernel]
in 1 second...

```

```

Type '?' for a list of commands, 'help' for more detailed help. ok boot -s Copyright
(c) 1996-2001, Juniper Networks, Inc. All rights reserved. Copyright (c) 1992-2001
The FreeBSD Project. Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991,
1992, 1993, 1994

```

```

The Regents of the University of California. All rights reserved. JUNOS
7.2I20050420_0432_sjg #3: 2005-04-20 04:32:35 UTC
sjg@swift.juniper.net:/c/sjg/work/7.2R1/obj-i386/sys/compile/JUNIPER
Timecounter "i8254" frequency 1193182 Hz
...(many lines deleted)
FIPS self tests completed.
kern.securelevel: -1 -> 1
System watchdog timer disabled
Enter root password, or ^D to go multi-user

```



NOTE: Do *not* exit the shell for multi-user mode in JUNOS-FIPS. You must reboot.

Password:

Enter full pathname of shell or 'recovery' for root password recovery or RETURN for /bin/sh:

NOTE: to go to multi-user operation, exit the single-user shell (with ^D)

NOTE: If you exit from this shell, the system will attempt to come up normally. However the securelevel has already been raised so kernel modules cannot be loaded and this may prevent the system being fully functional.

The best way to bring the system up from here is to 'reboot'.

To run a shell with a normal view of the system:

```
chroot /junos /bin/sh
```

```
# reboot
```

```
Apr 21 05:10:46 init: Multiuser: old requested_transition==0x0 sighupped=0
```

```
Waiting (max 60 seconds) for system process `bufdaemon' to stop...stopped
```

```
Waiting (max 60 seconds) for system process `syncer' to stop...stopped
```

```
syncing disks...
```

```
done
```

```
Uptime: 1m26s
```

```
ata0: Spinning down devices. Please wait...
```

```
Rebooting...
```



NOTE: You must reboot JUNOS-FIPS from single-user mode to enter multi-user mode with all services intact.

Configuring the JUNOS-FIPS Router

To configure a Juniper Networks router running JUNOS-FIPS, the Crypto Officer performs the following tasks in the order listed:

- Establish a root password conforming to the JUNOS-FIPS password guidelines discussed in “Passwords and Supported Cipher Sets” on page 30.
- For strict FIPS compliance, delete all rollback configurations.
- For strict FIPS compliance, reset any existing user passwords to ensure encryption with FIPS algorithms.
- For strict FIPS compliance, reset all keys.
- Apply a tamper-evident seal to the PCMCIA slot on applicable router models.
- For FIPS Level 2 operation, apply a tamper-evident label to seal each Rotuing Engine into the chassis. On some models, tamper-evident labels must be applied to other components as well. See the *FIPS Level 2 Label Installation Instructions* for details. Tamper-evident labels are ordered separately and applied according to the instructions included in the label kit.
- Establish Crypto Officer and other JUNOS-FIPS User logins. For more information about Crypto Officer and JUNOS-FIPS User logins, see “Crypto Officer and JUNOS-FIPS User Configurations” on page 31.



NOTE: The set of JUNOS-FIPS permissions that distinguish Crypto Officers from other JUNOS-FIPS Users are **secret**, **security**, **maintenance**, and **control**. All users should be assigned to a login class that contains all or none of these permissions.

- Every AS II FIPS PIC used for external IPsec must be authorized. AS II FIPS PICs can be used for services such as firewalls or Network Address Translation (NAT) without authorization, but all external IPsec tunnels require authorization. For more information about authorizing AS II FIPS PICs, see “Authorizing the AS II FIPS PIC” on page 20.
- Connect the router to the network and proceed with normal router configuration.

Errors and Error Status Messages

JUNOS-FIPS errors stop all data output from the entire cryptographic module and cause a module panic, except very early in the boot cycle. Errors that occur early in the boot cycle can prevent the system from successfully booting. Keep alternate boot media up-to-date using the `request system snapshot` command. For more information about this command, see the *JUNOS System Basics and Services Command Reference*.

JUNOS-FIPS uses only FIPS-approved cryptographic algorithms, and only after a series of self-tests, including Known Answer Tests. A self-test failure results in a JUNOS-FIPS error state.

All but one of the following JUNOS-FIPS error conditions will create a system panic condition:

- Known Answer Test failed
- Random Number is not random
- Signature generation failed
- Signature verification failed
- Certificate verification failed
- Encryption/decryption failed
- Environment error
- Error in pair-wise conditional test
- Memory allocation error

The memory allocation error aborts the process making the call. All other errors result in a system panic condition and stop all data output. All errors except for memory allocation errors have only an extremely small chance of occurring.

For information about AS II FIPS PIC errors, see “AS II FIPS PIC Errors” on page 21.

For more information about JUNOS software errors in general, see the *JUNOS System Basics Configuration Guide*.

Recommended JUNOS-FIPS System Log Configuration

The system log files are used to log system events in JUNOS and JUNOS-FIPS. Due to the sensitive nature of information used to configure and operate a system running JUNOS-FIPS, you should log certain events and examine the logs frequently.

The following is a recommended system log configuration for JUNOS-FIPS. More types of information can be logged, but these events are particularly important to the JUNOS-FIPS environment.

```
[edit]
system {
  syslog {
    file authlog {
      authorization info;
    }
    file messages {
      any notice;
    }
    file auditlog {
      authorization info;
      change-log any;
      interactive-commands any;
    }
  }
}
```

This system log configuration logs all authorization events to the `/var/log/authlog` and `/var/log/auditlog` files. The audit log file also receives all interactive commands and configuration change events. All events of moderate severity are logged to the `/var/log/messages` file.

JUNOS-FIPS secrets are not logged. When secret information that would ordinarily be logged in the JUNOS software is encountered, the secrets are replaced 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 */ '
```

For more information about system logging, see the *JUNOS System Basics Configuration Guide*.

Command Summary

request system software add reboot junos-juniper-7.4*-fips.tgz

Syntax	<code>request system software add reboot junos-juniper-7.4*-fips.tgz</code>
Release Information	Statement introduced before JUNOS Release 7.4.
Description	Upgrade the Routing Engine to JUNOS-FIPS.
Options	<p>none—Upgrades the Routing Engine from JUNOS Release 7.x or higher and boots into JUNOS-FIPS.</p> <p>no-validate—Do <i>not</i> validate the module when upgrading from JUNOS Release 6.4.</p>
Required Privilege Level	maintenance

Sample Output

```

crypto-officer@host> request system software add reboot
/var/tmp/junos-juniper-7.4releasedetails-fips.tgz
Installing package '/var/tmp/junos-juniper-7.4releasedetails-fips.tgz'
...
Verified jpfe-7.4releasedetails.tgz signed by PackageProduction_7_2_0
Verified junos-boot-juniper-7.4releasedetails.tgz signed by
PackageProduction_7_4_0
Verified junos-juniper-7.4releasedetails-fips-optest signed by
PackageProduction_7_4_0
Available space: 69723 require: 36970
JUNOS 7.4releasedetails will become active at next reboot
jpfe-7.4releasedetails.tgz will be installed after next reboot
Saving package file in /var/sw/pkg/junos-7.4releasedetails.tgz
...
Saving state for rollback
...
Rebooting
...

```

