



**JUNOS® Software**

## **Common Criteria and Junos-FIPS for J Series and SRX Series**

*Release 9.3*

Revision History  
March 2011—Revision 1

# Table of Contents

Introduction .....	1
Common Criteria for J-series and SRX-series Devices .....	3
Evaluation of JUNOS 9.3 .....	3
FIPS for J-series and SRX-series Devices .....	3



## Introduction

---

This document describes the Common Criteria and Federal Information Processing Standard version of Junos 9.3 as it applies to J Series and SRX Series devices.

For information for MX Series, M Series, T Series, and EX Series devices, refer to *Secure Configuration Guide for Common Criteria and JUNOS-FIPS*.



## **Common Criteria for J-series and SRX-series Devices**

---

Common Criteria is a framework in which computer system users can specify their security functional and assurance requirements. Based on the common criteria, vendors can then implement and make claims about the security attributes of their products. Testing laboratories can evaluate the products to determine if they actually meet the claims. Common Criteria provides assurance that the process of specification, implementation, and evaluation of a computer security product has been conducted following rigorous and standard process.

The Security Target document that describes the features tested and the certification report are available at

[http://www.dsd.gov.au/infosec/evaluation\\_services/epl/network\\_security/juniper\\_junos9-3.html](http://www.dsd.gov.au/infosec/evaluation_services/epl/network_security/juniper_junos9-3.html).

### ***Evaluation of JUNOS 9.3***

JUNOS 9.3 has been evaluated at Evaluation Level (EAL) 3 on the following devices:

- J2320, J2350, J4350, J6350
- SRX5600, SRX5800

The following features have been evaluated for JUNOS 9.3:

- Security audit
- Communication
- Cryptographic support
- User data protection
- Identification and authentication
- Security management

The following features were not evaluated for JUNOS 9.3:

- External NTP server
- External management platform
- External authentication server

### ***FIPS for J-series and SRX-series Devices***

FIPS is issued to coordinate the requirements and standards for cryptography modules that include both hardware and software components.

The JUNOS-FIPS is a special version of JUNOS that has been tested and certified for compliance with the FIPS 140-2 standard.

The JUNOS-FIPS version of JUNOS 9.3 is in the process of FIPS 140-2 validation at level 2 on the following devices:

- J2320
- J2350
- J4350
- J6350

Changes to JUNOS-FIPS for FIPS compliance:

- Weak cryptographic algorithms are not available to be configured for VPN or management connections:
  - DES, MD5, Diffie-Hellman Group 1
  - SSL (permitted for remote access but not for management)
  - Minimum strength requirements are imposed on an administrator password.
  - SSH requires that version 2 is used. Version 1 is not available.
  - Management related services that operate unencrypted are disabled, for example, telnet.
- High availability features are disabled.

A full description of the behavior of JUNOS-FIPS and the steps necessary to place a J-series device into a compliant configuration are described in *Juniper J-series Services Routers: J2320, J2350, J4350, J6350 Security Policy*.