

JUNOScope 8.2 Software Release Notes (Common Criteria EAL3 Certified)

Release 8.2R2
7 August 2007
Part No. 530-017350-01
Revision 3

These release notes accompany Release 8.2R2 of the JUNOScope software. They describe the key features, documentation, and known problems with the software. The JUNOScope software is a network management application that provides router configuration management, inventory management, software management, operation status, and troubleshooting tools for Juniper Networks J-series, M-series, MX-series, T-series, and TX-series routing platforms.



Note

The JUNOScope software Release 8.2R2.4 is the official Common Criteria Evaluation Assurance Level 3 (EAL3) certified version. The JUNOScope software is certified to run on a UNIX server running Sun Solaris version 9/04 or 10. For certification details, see <http://www.cesg.gov.uk/site/iacs/index.cfm?menuSelected=1&displayPage=152&id=409>.

To set up the JUNOScope software common criteria certified version, follow the instructions in “JUNOScope Software Usage Guidelines” on page 5 and “Installing the JUNOScope Software” on page 9.

You can also find these release notes on the Juniper Networks Technical Publications Web page, which is located at <http://www.juniper.net/>.

Contents	Release 8.2 Features	2
	Current Software Release	3
	Outstanding Issues	3
	Resolved Issues	3
	Product Support Notification	4
	JUNOScope Software Usage Guidelines	5
	Installing the JUNOScope Software	9
	System Requirements	9
	Red Hat Enterprise Linux ES File Package Requirements	10
	JUNOScope Client Workstation Requirements	11
	RADIUS Server Requirements	11
	Syslog Server Requirements	11
	Installing the JUNOScope Software	11
	Reconfiguring the JUNOScope Software	13
	Reinstalling or Upgrading the JUNOScope Software	13
	Uninstalling the JUNOScope Software	14
	Related Juniper Networks Documentation	14
	How To Request Support	18
	Revision History	18

Release 8.2 Features

The following features have been added to JUNOScope Release 8.2. For more detailed information, see the appropriate sections of the *JUNOScope 8.2 Software User Guide*.

- **User Group Authorization**—The JUNOScope administrator can create user groups of one or more JUNOScope users with specified permissions and access to devices and device groups configured in the JUNOScope software. The administrator can associate devices and device groups to a user group. User group authentication provides four predefined user groups: administrator, read-write user, read-only user, and nobody. Each user group must be associated with one of the following permission levels: superuser, read-write, read-only, and none. Users in the same user group have access permission to a set of devices and device groups that are associated with the user group, but users in the administrator user group have read-write access to all devices and device groups configured in JUNOScope. A user can belong to multiple user groups. Therefore, the least restrictive permission of the user groups to which the user belongs applies. The JUNOScope administrator can configure user groups by clicking Settings > User > Authorization from the JUNOScope main window. For more information about setting up user group authorization, see the *JUNOScope 8.2 Software User Guide*.



Note

NOTE: If you do not use this user group authorization feature, you do not have to create any new user-defined user groups. You can simply treat the three predefined user groups (administrator, read-write user, and read-only user), as the three distinct permission levels: superuser, read-write, and read-only.

- **Element Management Support for the MX960 Ethernet Services Router**—The JUNOScope software now provides element management for the Juniper Networks MX960 Ethernet Services Router. For more information about the MX960 Ethernet Services Router, see the corresponding hardware guide. The JUNOScope software allows you to configure the MX960 Ethernet Services Router and manage it using element management tools, such as Looking Glass, Configuration Manager, Software Manager, and Inventory Management.
- **Device Configuration Comparison and Difference Auditing**—For any JUNOScope managed device, the user can tag a configuration revision in the repository as a master and compare it with another archived configuration revision. The comparison can be made with a running configuration or a version from the archive repository. Devices with configurations different from the master are highlighted and are also reported as system log events. To create and associate archive tags, click Configuration > Repository > Archive Tags. To compare configurations, click Configuration > Repository > Audit Configuration. For more information about configuration tagging and comparison, see the *JUNOScope 8.2 Software User Guide*.
- **Purging of Status and Audit Log Tables**—The JUNOScope administrator can now purge unwanted entries in the Status and Audit Log tables through the user interface. Most JUNOScope operations generate multiple rows of audit and status records in the Status and Audit Log tables. These tables grow in size and consume valuable disk space on the JUNOScope software server. The data in these tables is useful only to the JUNOScope administrator. To purge the Status table, from the JUNOScope main window, click Monitor > Purge > Status. To purge the Audit Log table, click Monitor > Purge > Audit Log. The scripts to clear the Status and Audit log tables (`clear_status_table.sh` and `clear_audit_table.sh`) are no longer available. For more information about purging the Status and Audit Log tables, see the *JUNOScope 8.2 Software User Guide*.

- **Global Authentication Policies**—The JUNOScope administrator can now configure global authentication policies in addition to user authentication policies. The global authentication policy is used when an authentication policy has not been configured for a user. The administrator can create an access list, which specifies which client machines to deny or allow access to the JUNOScope software. To configure the global authentication policy and the access control list, from the JUNOScope main window, click Home > Settings > Users > Authentication Policy > Global Authentication Policy. For more information about setting up global authentication policies, see the *JUNOScope 8.2 Software User Guide*.

Current Software Release

The current JUNOScope software release is Release 8.2R2. For information about installing the software release, see “Installing the JUNOScope Software” on page 9.

Outstanding Issues

The following issues are outstanding in the JUNOScope software release.

- User Group Authorization** When a user is assigned to multiple user groups configured with different permission levels, the most restrictive (least privileges) user group takes priority. This issue affects all user groups (predefined and user-defined) and all permission levels (superuser, read-write, read-only, and none). The intended behavior, as documented in the *JUNOScope Software User Guide*, “Setting Up User Group Authorization and Viewing User Permissions” chapter is that the least restrictive (most privileges) should be granted. (PR 101487)
- User Local Authentication** The *JUNOScope Software User Guide* states that a password that you create for a JUNOScope user should be between 6 and 40 characters in length. Although it is possible to create a user password in the range 41 to 128 characters, this is not supported in the Common Criteria certification evaluation version of JUNOScope software. If the password is longer than 47 characters JUNOScope will prevent a user from successfully logging in. If you create a password that is longer than 128 characters, an error message appears. (PR 105151)

Resolved Issues

The following issues were resolved in the previous JUNOScope software release:

- Devices** When multiple users simultaneously use JUNOScope to perform interactions on the same device, more than one management (mgd) session might be created on that device. Of the mgd sessions created, one is used by JUNOScope for pooling purposes. The remaining mgd sessions are not automatically closed even after interaction with the device is completed. (PR 72451)
- Audit Log** The Archive and Restore operations produce an incorrect client IP address in the audit log entry. (PR 70020)
- Looking Glass** When the refresh command is enabled and activated, the Looking Glass page displayed will always be reset to the top level. (PR 73530)

- Archive Tags**
- When you use Archive Tags, the following functions do not operate as specified: (PR 78055)
 - Associate groups to a tag—This command does not operate properly.
 - Import or export a tag—These commands do not operate properly.
 - You cannot associate a tag to a device when the tag name is as follows: (PR 78058)
 - Only numeric
 - Contains more than one word
 - Contains alphanumerics, such as 23-test, \$\$, _@@, and etc.
 - In date format
 - Like < test >

- Audit Configurations**
- You cannot perform an audit configuration in the following instances: (PR 78883)
 - When source tag is **tag1** and target tag is running.
 - When source tag is **head** and target tag is running.

Also, the Schedule table that appears in the Configuration > Repository > Audit Configuration dialog box is incorrect.

- When using Audit Configurations, no syslog event is logged when there is a difference between the compared configuration revisions. (PR 80416)

- Devices** You cannot delete four or more devices at the same time. As a workaround, delete one device at a time using Settings > Devices. (PR 81523)

Product Support Notification

- JUNOScope and Daylight Saving Time** You must perform the procedure document in Public Support Notification PSN-2007-02-031, *Daylight Saving Time (DST) and JUNOScope*. To view the procedure, go to <http://www.juniper.net/customers/support>, and under the Research A Problem section, click Technical Bulletins. On the JTAC Technical Bulletins Web page, enter PSN-2007-02-031 in the Search field, select the CS Technical Bulletin ID radio button, and click Search.

JUNOScope Software Usage Guidelines

The following are recommended guidelines for using the JUNOScope software.

- Install Latest Appropriate Operating System Patches on page 5
- Perform MD5 or SHA1 Calculation on the JUNOScope Image Before Installing and Verify Against Values Published on the Juniper Networks Web Site on page 6
- Upgrading JUNOScope and Password Policies on page 6
- Protecting JUNOScope Data Files on page 6
- Always Use Strong Passwords on page 6
- Change the Default Install Time User from 'admin' to Another Name on page 7
- Disable Access to the Inventory Management System SQL Interface on page 7
- Do Not Enable Debugging on JUNOScope at Installation on page 7
- Use Only HTTPS to Connect from a Browser Client to the JUNOScope Server on page 8
- Use Only SSL to Connect from the JUNOScope Software to Network Devices on page 8
- Do Not Export JUNOScope Data in Clear Text or with the Encryption Key in the Exported Data on page 8
- Disable User Accounts After Login Failure Attempts Within The Time Window Are Exceeded on page 8
- Regularly Back Up the JUNOScope Software Server on page 8

Install Latest Appropriate Operating System Patches

Apply all appropriate operating system (such as Solaris or Linux) patches to keep the JUNOScope server less vulnerable to discovered exploits. Regularly check for and install updates. For more information, see the *JUNOScope Software User Guide*, “Installing, Reconfiguring, Reinstalling, Upgrading, or Uninstalling the JUNOScope Software” chapter.

Perform MD5 or SHA1 Calculation on the JUNOScope Image Before Installing and Verify Against Values Published on the Juniper Networks Web Site

To ensure the authenticity of the JUNOScope software, please visit <https://www.juniper.net/support/csc/swdist-encr/swdist-jtk/>. You can validate the JUNOScope image distributed by way of HTTPS download or contained on the CD, for example, `jtk-install-8.2R2-sunos5.sh` for Solaris, by comparing it with the MD5 or SHA-1 hash values posted on the Juniper Web site.

- The MD5 hash value should be `6d96f50621c9c795703a11c5b3e1d632`
- The SHA1 hash value should be `b5da794099f1103425a6dc22dffe37366553f1b1`

To generate the hash value, use the following command:

```
hostname% openssl dgst -sha1 jtk-install-8.2R2.4-sunos5.sh
```

Upgrading JUNOScope and Password Policies

When upgrading from JUNOScope 8.1 or earlier, the password policy is not enforced on any existing user accounts. It is recommended that the administrator change the password for existing user accounts in order to comply with the password policy.

Protecting JUNOScope Data Files

During the JUNOScope software installation, you are asked to specify how you want to protect JUNOScope data files. The available options are `user`, `group`, and `all`. Select the `User` option to specify that only the user who installed the JUNOScope software can read JUNOScope data files.

Always Use Strong Passwords

The initial admin account, created at install time, should have an extra-strong password as it cannot be disabled through repeated login failures. The password for the administrator should not match the username, and should not be a word that can be easily guessed.

In general, JUNOScope software passwords must be:

- Easy to remember so that users are not tempted to write them down.
- Contain between 6 and 40 characters, using at least two of the four defined character sets (uppercase, lowercase, numeric, other). The characters in the set "other" are those that can be entered using a single keystroke, or a keyboard character accessed using the Shift key, that does not fall into any of the other three groups.
- Changed periodically.
- Not divulged to anyone.

Weak passwords are:

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

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

Strong reusable passwords can be:

- Based on letters from a favorite phrase or word, and
- Concatenated with other, unrelated words, along with added digits and punctuation.

Passwords should be changed from time to time. For more information, see the *JUNOScope Software User Guide*, “Installing, Reconfiguring, Reinstalling, Upgrading, or Uninstalling the JUNOScope Software” chapter.

Change the Default Install Time User from ‘admin’ to Another Name

The JUNOScope administrative default user account name is admin. The JUNOScope installation creates this initial JUNOScope administrative user account so the administrator can use it to add other users. Change the default user account name to another name during the installation process. For more information, see the *JUNOScope Software User Guide*, “Installing, Reconfiguring, Reinstalling, Upgrading, or Uninstalling the JUNOScope Software” chapter.

Disable Access to the Inventory Management System SQL Interface

During the JUNOScope software installation, you are asked to confirm whether you want to enable access to the Inventory Management System SQL interface. The default is no. If you select no, the SQL interface cannot be accessed by any other application or host except JUNOScope clients. If you select yes, the MySQL database can be accessed by any application with Inventory Management System user credentials.

Do Not Enable Debugging on JUNOScope at Installation

The JUNOScope software installation confirms whether you want to enable debug logging for technical support purposes. The default and recommended setting is no. For more information, see the *JUNOScope Software User Guide*, “Installing, Reconfiguring, Reinstalling, Upgrading, or Uninstalling the JUNOScope Software” chapter.

Use Only HTTPS to Connect from a Browser Client to the JUNOScope Server

The JUNOScope software accepts Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS).

The JUNOScope software provides security between the client and the server. MD5 RSA certification is available between the JUNOScope server and the client Web browser. All communication is encrypted between the client Web browser and the JUNOScope server. The JUNOScope software installation creates an X.509 digital certificate to authenticate the HTTPS server. The JUNOScope software administrator can use self-assigned certificates, or have one assigned by a trusted certificate authority.

The JUNOScope software installation prompts for the HTTPS port that the JUNOScope software Web server uses for its transactions. It is recommended that you use the HTTPS port for communication between the JUNOScope Web browsers and the JUNOScope server. For more information, see the *JUNOScope Software User Guide*, “Installing, Reconfiguring, Reinstalling, Upgrading, or Uninstalling the JUNOScope Software” chapter.

Use Only SSL to Connect from the JUNOScope Software to Network Devices

The JUNOScope software uses the SSL JUNOScript access protocol to connect to configured devices on the network. The SSL protocol is preferred because it encrypts security information (such as a password) before transmitting it across the network. For more information about how to use the SSL access protocol to connect to devices, see the *JUNOScope Software User Guide*, “Setting Up Access Methods” chapter.

Do Not Export JUNOScope Data in Clear Text or with the Encryption Key in the Exported Data

When exporting sensitive data in authentication information from the JUNOScope software server, use the Encrypt sensitive data and provide key at import time export option. Sensitive data is exported encrypted and the key to decrypt it is not included in the exported data, but is supplied during import. For more information about exporting all data from the JUNOScope server, see the *JUNOScope Software User Guide*, “Importing and Exporting All Settings Data” chapter, or the specific JUNOScope operation chapter export section.

Disable User Accounts After Login Failure Attempts Within The Time Window Are Exceeded

Configure a Global User Authentication Policy to disable user accounts after the login failure attempts within the time window, as defined by the administrator, has been exceeded. Enable the global user authentication policy; it is disabled by default. For more information about creating global authentication policies, see the *JUNOScope Software User Guide*, “Setting Up a Global Authentication Policy” chapter.

Regularly Back Up the JUNOScope Software Server

Perform regular backups of application data stored by JUNOScope to prevent data loss in the event of a disaster. For more information about backing up JUNOScope application data, see the *JUNOScope Software User Guide*, “Backing Up and Restoring the JUNOScope Application Data” chapter.

Installing the JUNOScope Software

This section describes how to install, reconfigure, reinstall, upgrade, and uninstall the JUNOScope software.

Before installing the JUNOScope software, ensure that your network meets the requirements described in the following sections:

- System Requirements on page 9
- Red Hat Enterprise Linux ES File Package Requirements on page 10
- JUNOScope Client Workstation Requirements on page 11
- RADIUS Server Requirements on page 11

To install, reconfigure, reinstall or upgrade, or deinstall the JUNOScope software, see the following sections:

- Installing the JUNOScope Software on page 11
- Reconfiguring the JUNOScope Software on page 13
- Reinstalling or Upgrading the JUNOScope Software on page 13
- Uninstalling the JUNOScope Software on page 14

System Requirements

The JUNOScope software runs on both Sun Solaris servers (see Table 1) and Red Hat Linux servers (see Table 2). Before you install the JUNOScope software, ensure that the supported UNIX server workstation on which you install the software meets the following system requirements.



Note

The JUNOScope software Release 8.2R2.4 is the official Common Criteria EAL3 certified version. The JUNOScope software is certified to run on a UNIX server running Sun Solaris version 9/04 or 10. For certification details, see <http://www.cesg.gov.uk/site/iacs/index.cfm?menuSelected=1&displayPage=152&id=409>.

Make sure the JUNOScope UNIX server is located in a secure location with access only by authorized personnel. The JUNOScope administrator is responsible for maintaining security for the JUNOScope server.

Table 1 shows the minimum system requirements for a Sun Solaris server.

Table 1: Sun Solaris Server System Minimum Requirements

System	Minimum Requirement
Operating system	Solaris 9/04 or 10 or later
Processor	UltraSPARC III or equivalent
Speed	1.3 GHz or faster
RAM	1 GB
Free disk space	1 GB

Table 2 shows the minimum system requirements for a Red Hat Linux server. (See also “Red Hat Enterprise Linux ES File Package Requirements” on page 10.)

Table 2: Red Hat Linux Server System Minimum Requirements

System	Minimum Requirement
Hardware	Red Hat certified hardware platforms
Operating system	Red Hat Enterprise Linux ES version 3 and 4
Processor	Pentium 4 processor
Speed	2.8 GHz or faster
RAM	1 GB
Free disk space	1 GB

Red Hat Enterprise Linux ES File Package Requirements

If a minimal install of Red Hat Enterprise Linux ES is performed on the server, the JUNOScope software administrator should ensure that the following file packages are installed for the JUNOScope software to run properly. All packages should be available in a full install of Red Hat Enterprise Linux ES.

Table 3: Red Hat Enterprise Linux ES File Package Requirements

Version	Required File Packages
Red Hat Enterprise Linux ES version 3 (Update 6)	krb5-libs-1.2.7-47.i386.rpm XFree86-libs-4.3.0-97.EL.i386.rpm
Red Hat Enterprise Linux ES version 4 (Update 2)	compat-libcom_err-1.0-5.i386.rpm krb5-libs-1.3.4-17.i386.rpm xorg-x11-deprecated-libs-6.8.2-1.EL.13.20.i386.rpm xorg-x11-libs-6.8.2-1.EL.13.20.i386.rpm

To verify that the file package `krb5-libs-1.3.4-17.i386.rpm` is installed, use the following command:

```
hostname% rpm -queryformat "%{NAME}-%{VERSION}-%{RELEASE}-%{ARCH}\n" --query krb5-libs
```

You can install each package individually via `rpm`, from the original Red Hat Enterprise Linux ES distribution.

To install the file package `xorg-x11-libs-6.8.2-1.EL.13.20.i386.rpm`, use the following command:

```
hostname% rpm -install xorg-x11-libs-6.8.2-1.EL.13.20.i386.rpm
```

JUNOScope Client Workstation Requirements

Ensure that the client workstation from which you connect to the JUNOScope software is running either Microsoft Internet Explorer 6 or Netscape Navigator 6 or later with JavaScript enabled.

RADIUS Server Requirements

Ensure that the RADIUS server complies with RFC 2865, *Remote Authentication Dial-In User Service*.

Syslog Server Requirements

Ensure that the syslog server (`syslogd`) is running and configured to receive JUNOScope system log messages.

Installing the JUNOScope Software

You can install the JUNOScope software in one of the following ways:

- Installing the JUNOScope Software from the CD on page 12
- Downloading the JUNOScope Software from the Software Download Page on page 12

To upgrade the JUNOScope software, see “Reinstalling or Upgrading the JUNOScope Software” on page 13.

For more information about installing the JUNOScope software, see the *JUNOScope Software User Guide*.

Installing the JUNOScope Software from the CD

To install the JUNOScope software from the product CD, follow these steps:

1. Insert the JUNOScope software CD into the CD drive of the server workstation.
2. Mount the CD.

If the volume management (volmgt) daemon, vold, is running on your server, the CD automatically mounts itself. To mount the CD manually, follow the procedure for your operating system.

3. Start the JUNOScope installation:

```
hostname% cdrom-mount-directory/jtk-installer install-directory
```

Replace *cdrom-mount-directory* with the directory on which the CD is mounted: /mnt, /cdrom, or /cdrom/JUNOScope, depending on your host setup.

Replace *install-directory* with the directory in which to install the JUNOScope software. If you do not specify an installation directory, the software is installed in the current directory.

For more information about installing the JUNOScope software, see the *JUNOScope Software User Guide*.

Downloading the JUNOScope Software from the Software Download Page

The JUNOScope software Release 2.4R2.4 package for Common Criteria is `jtk-install-8.2R2.4-sunos5-sparc.sh`. The MD5 hash value is `6d96f50621c9c795703a11c5b3e1d632`. You can install either the JUNOScope Sun Solaris or Red Hat Linux version; but the JUNOScope Sun Solaris version is certified for Common Criteria.

To download the JUNOScope software from the Juniper Networks Web site and start the JUNOScope installation, follow these steps:

1. Using a Web browser, go to the following location:

```
https://www.juniper.net/junos/swdist/encryption/index.htm
```

2. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by a Juniper Networks representative.
3. Download the appropriate JUNOScope software to the server workstation.
4. Start the JUNOScope installation program:

```
hostname% download-directory/jtk-install-8.2R2.4-sunos5-sparc.sh install-directory
```

or

```
hostname% download-directory/jtk-install-8.2R2.4-linux2-i386.sh install-directory
```

Replace *download-directory* with the directory into which you downloaded the JUNOScope software from the software download page.

jtk-install-8.2R2.4-sunos5-sparc.sh or **jtk-install-8.2R2.4-linux2-i386.sh** is the JUNOScope software file. Replace *X* with the software version to download.

Replace *install-directory* with the directory in which to install the JUNOScope software. If you do not specify an installation directory, the software is installed in the current directory.

Reconfiguring the JUNOScope Software

You can change the following JUNOScope software installation settings without rerunning the installation program. For more information about these settings, see the *JUNOScope Software User Guide*.

- HTTPS and HTTP ports on which the JUNOScope Web server should listen
- Port on which the JUNOScope server listens for control messages
- HTTP port on which the JUNOScope report server should listen
- Java Database Connectivity (JDBC) URL for accessing the JUNOScope database and demo database
- Enable or disable access for SQL interface to Inventory Management System
- Debug logging
- Syslog facility
- Idle session timeout
- Licensed software modules

You cannot change some settings, such as passwords.

To change JUNOScope software settings, use the following command:

```
hostname% <install-directory>/jtk/bin/jtk-setup.sh
```

Reinstalling or Upgrading the JUNOScope Software

The process for reinstalling or upgrading the JUNOScope software is the same as for installing the software. To install the JUNOScope software, see “Installing the JUNOScope Software from the CD” on page 12 or “Downloading the JUNOScope Software from the Software Download Page” on page 12.

To reinstall or upgrade JUNOScope software, you must use the same user ID as the one used for the currently installed software.

Uninstalling the JUNOScope Software

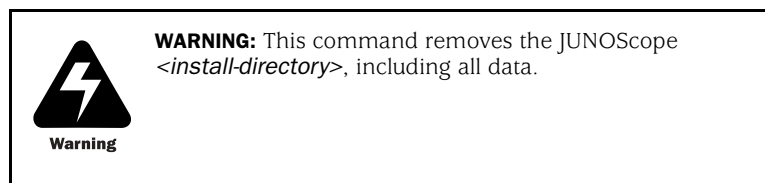
To uninstall the JUNOScope software, follow these steps:

1. Stop the JUNOScope software and database by changing to the directory where you installed the JUNOScope software and typing the following command:

```
hostname% <install-directory>/jtk/rc.d/jtk stop
```

2. Remove the JUNOScope software by typing the following command:

```
hostname% rm -rf <install-directory>
```



Related Juniper Networks Documentation

Table 4 lists the software and hardware guides and release notes for the supported Juniper Networks routing platforms and describes the contents of each document. Table 5 lists the books included in the *Network Operations Guide* series.

Table 4: Technical Documentation for Supported Routing Platforms (Sheet 1 of 3)

Document	Description
JUNOS Internet Software Configuration Guides	
<i>Class of Service</i>	Provides an overview of the class-of-service (CoS) functions of the JUNOS software and describes how to configure CoS features, including configuring multiple forwarding classes for transmitting packets, defining which packets are placed into each output queue, scheduling the transmission service level for each queue, and managing congestion through the random early detection (RED) algorithm.
<i>CLI User Guide</i>	Describes how to use the JUNOS command-line interface (CLI) to configure, monitor, and manage Juniper Networks routing platforms. This material was formerly covered in the <i>JUNOS System Basics Configuration Guide</i> .
<i>Feature Guide</i>	Provides a detailed explanation and configuration examples for several of the most complex features in the JUNOS software.
<i>MPLS Applications</i>	Provides an overview of traffic engineering concepts and describes how to configure traffic engineering protocols.
<i>Multicast Protocols</i>	Provides an overview of multicast concepts and describes how to configure multicast routing protocols.
<i>Network Interfaces</i>	Provides an overview of the network interface functions of the JUNOS software and describes how to configure the network interfaces on the routing platform.
<i>Network Management</i>	Provides an overview of network management concepts and describes how to configure various network management features, such as SNMP and accounting options.
<i>Policy Framework</i>	Provides an overview of policy concepts and describes how to configure routing policy, firewall filters, forwarding options, and cflowd.

Table 4: Technical Documentation for Supported Routing Platforms (Sheet 2 of 3)

Document	Description
<i>Routing Protocols</i>	Provides an overview of routing concepts and describes how to configure routing, routing instances, and unicast routing protocols.
<i>Secure Configuration Guide for Common Criteria and JUNOS-FIPS</i>	Provides an overview of secure Common Criteria and JUNOS-FIPS protocols for the JUNOS Internet software and describes how to install and configure secure Common Criteria and JUNOS-FIPS on a routing platform.
<i>Services Interfaces</i>	Provides an overview of the services interfaces functions of the JUNOS software and describes how to configure the services interfaces on the routing platform.
<i>Software Installation and Upgrade Guide</i>	Provides a description of JUNOS software components and packaging, and includes detailed information about how to initially configure, reinstall, and upgrade the JUNOS system software. This material was formerly covered in the <i>JUNOS System Basics Configuration Guide</i> .
<i>System Basics</i>	Describes Juniper Networks routing platforms, and provides information about how to configure basic system parameters, supported protocols and software processes, authentication, and a variety of utilities for managing your router on the network.
<i>VPNs</i>	Provides an overview and describes how to configure Layer 2 and Layer 3 virtual private networks (VPNs), virtual private LAN service (VPLS), and Layer 2 circuits. Provides configuration examples.
JUNOS References	
<i>Hierarchy and RFC Reference</i>	Describes the JUNOS configuration mode commands. Provides a hierarchy reference that displays each level of a configuration hierarchy, and includes all possible configuration statements that can be used at that level. This material was formerly covered in the <i>JUNOS System Basics Configuration Guide</i> .
<i>Interfaces Command Reference</i>	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot interfaces.
<i>Routing Protocols and Policies Command Reference</i>	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot routing protocols and policies, including firewall filters.
<i>System Basics and Services Command Reference</i>	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot system basics, including commands for real-time monitoring and route (or path) tracing, system software management, and chassis management. Also describes commands for monitoring and troubleshooting services such as CoS, IP Security (IPSec), stateful firewalls, flow collection, and flow monitoring.
<i>System Log Messages Reference</i>	Describes how to access and interpret system log messages generated by JUNOS software modules and provides a reference page for each message.
J-Web User Guide	
<i>J-Web Interface User Guide</i>	Describes how to use the J-Web GUI to configure, monitor, and manage Juniper Networks routing platforms.
JUNOS API and Scripting Documentation	
<i>JUNOScript API Guide</i>	Describes how to use the JUNOScript application programming interface (API) to monitor and configure Juniper Networks routing platforms.
<i>JUNOS XML API Configuration Reference</i>	Provides reference pages for the configuration tag elements in the JUNOS XML API.
<i>JUNOS XML API Operational Reference</i>	Provides reference pages for the operational tag elements in the JUNOS XML API.
<i>JUNOS Configuration and Diagnostic Automation Guide</i>	Describes how to use the commit script and self-diagnosis features of the JUNOS software. This guide explains how to enforce custom configuration rules defined in scripts, how to use commit script macros to provide simplified aliases for frequently used configuration statements, and how to configure diagnostic event policies.
<i>NETCONF API Guide</i>	Describes how to use the NETCONF API to monitor and configure Juniper Networks routing platforms.

Table 4: Technical Documentation for Supported Routing Platforms (Sheet 2 of 3)

Document	Description
<i>Routing Protocols</i>	Provides an overview of routing concepts and describes how to configure routing, routing instances, and unicast routing protocols.
<i>Secure Configuration Guide for Common Criteria and JUNOS-FIPS</i>	Provides an overview of secure Common Criteria and JUNOS-FIPS protocols for the JUNOS Internet software and describes how to install and configure secure Common Criteria and JUNOS-FIPS on a routing platform.
<i>Services Interfaces</i>	Provides an overview of the services interfaces functions of the JUNOS software and describes how to configure the services interfaces on the routing platform.
<i>Software Installation and Upgrade Guide</i>	Provides a description of JUNOS software components and packaging, and includes detailed information about how to initially configure, reinstall, and upgrade the JUNOS system software. This material was formerly covered in the <i>JUNOS System Basics Configuration Guide</i> .
<i>System Basics</i>	Describes Juniper Networks routing platforms, and provides information about how to configure basic system parameters, supported protocols and software processes, authentication, and a variety of utilities for managing your router on the network.
<i>VPNs</i>	Provides an overview and describes how to configure Layer 2 and Layer 3 virtual private networks (VPNs), virtual private LAN service (VPLS), and Layer 2 circuits. Provides configuration examples.
JUNOS References	
<i>Hierarchy and RFC Reference</i>	Describes the JUNOS configuration mode commands. Provides a hierarchy reference that displays each level of a configuration hierarchy, and includes all possible configuration statements that can be used at that level. This material was formerly covered in the <i>JUNOS System Basics Configuration Guide</i> .
<i>Interfaces Command Reference</i>	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot interfaces.
<i>Routing Protocols and Policies Command Reference</i>	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot routing protocols and policies, including firewall filters.
<i>System Basics and Services Command Reference</i>	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot system basics, including commands for real-time monitoring and route (or path) tracing, system software management, and chassis management. Also describes commands for monitoring and troubleshooting services such as CoS, IP Security (IPSec), stateful firewalls, flow collection, and flow monitoring.
<i>System Log Messages Reference</i>	Describes how to access and interpret system log messages generated by JUNOS software modules and provides a reference page for each message.
J-Web User Guide	
<i>J-Web Interface User Guide</i>	Describes how to use the J-Web GUI to configure, monitor, and manage Juniper Networks routing platforms.
JUNOS API and Scripting Documentation	
<i>JUNOScript API Guide</i>	Describes how to use the JUNOScript application programming interface (API) to monitor and configure Juniper Networks routing platforms.
<i>JUNOS XML API Configuration Reference</i>	Provides reference pages for the configuration tag elements in the JUNOS XML API.
<i>JUNOS XML API Operational Reference</i>	Provides reference pages for the operational tag elements in the JUNOS XML API.
<i>JUNOS Configuration and Diagnostic Automation Guide</i>	Describes how to use the commit script and self-diagnosis features of the JUNOS software. This guide explains how to enforce custom configuration rules defined in scripts, how to use commit script macros to provide simplified aliases for frequently used configuration statements, and how to configure diagnostic event policies.
<i>NETCONF API Guide</i>	Describes how to use the NETCONF API to monitor and configure Juniper Networks routing platforms.

Table 4: Technical Documentation for Supported Routing Platforms (Sheet 3 of 3)

Document	Description
JUNOS Comprehensive Index and Glossary	
<i>Comprehensive Index and Glossary</i>	Provides a complete index of all JUNOS software books, the <i>JUNOScript API Guide</i> , and the <i>NETCONF API Guide</i> . Also provides a comprehensive glossary.
JUNOScope Documentation	
<i>JUNOScope Software User Guide</i>	Describes the JUNOScope software GUI, how to install and administer the software, and how to use the software to manage routing platform configuration files and monitor routing platform operations.
J-series Services Router Documentation	
<i>Getting Started Guide</i>	Provides an overview, basic instructions, and specifications for J-series Services Routers. The guide explains how to prepare your site for installation, unpack and install the router and its components, install licenses, and establish basic connectivity. Use the <i>Getting Started Guide</i> for your router model.
<i>Basic LAN and WAN Access Configuration Guide</i>	Explains how to configure the interfaces on J-series Services Routers for basic IP routing with standard routing protocols, ISDN backup, and digital subscriber line (DSL) connections.
<i>Advanced WAN Access Configuration Guide</i>	Explains how to configure J-series Services Routers in virtual private networks (VPNs) and multicast networks, configure data link switching (DLSw) services, and apply routing techniques such as policies, stateless and stateful firewall filters, IP Security (IPSec) tunnels, and class-of-service (CoS) classification for safer, more efficient routing.
<i>Administration Guide</i>	Shows how to manage users and operations, monitor network performance, upgrade software, and diagnose common problems on J-series Services Routers.
Hardware Documentation	
<i>Hardware Guide</i>	Describes how to install, maintain, and troubleshoot routing platforms and components. Each platform has its own hardware guide.
<i>PIC Guide</i>	Describes the routing platform PICs. Each platform has its own PIC guide.
Release Notes	
<i>JUNOS Release Notes</i>	Summarize new features and known problems for a particular software release, provide corrections and updates to published JUNOS, JUNOScript, and NETCONF manuals, provide information that might have been omitted from the manuals, and describe upgrade and downgrade procedures.
<i>Hardware Release Notes</i>	Describe the available documentation for the routing platform and the supported PICs, and summarize known problems with the hardware and accompanying software. Each platform has its own release notes.
<i>JUNOScope Software Release Notes</i>	Contain corrections and updates to the published JUNOScope manual, provide information that might have been omitted from the manual, and describe upgrade and downgrade procedures.
<i>J-series Services Router Release Notes</i>	Briefly describe the J-series Services Router features, identify known hardware problems, and provide upgrade and downgrade instructions.

Table 5: JUNOS Internet Software Network Operations Guides (Sheet 1 of 2)

Book	Description
<i>Baseline</i>	Describes the most basic tasks for running a network using Juniper Networks products. Tasks include upgrading and reinstalling JUNOS software, gathering basic system management information, verifying your network topology, and searching log messages.

Table 5: JUNOS Internet Software Network Operations Guides (Sheet 2 of 2)

Book	Description
<i>Interfaces</i>	Describes tasks for monitoring interfaces. Tasks include using loopback testing and locating alarms.
<i>MPLS</i>	Describes tasks for configuring, monitoring, and troubleshooting an example MPLS network. Tasks include verifying the correct configuration of the MPLS and RSVP protocols, displaying the status and statistics of MPLS running on all routers in the network, and using the layered MPLS troubleshooting model to investigate problems with an MPLS network.
<i>MPLS Log Reference</i>	Describes MPLS status and error messages that appear in the output of the <code>show mpls lsp extensive</code> command. The guide also describes how and when to configure Constrained Shortest Path First (CSPF) and RSVP trace options, and how to examine a CSPF or RSVP failure in a sample network.
<i>Hardware</i>	Describes tasks for monitoring M-series and T-series routing platforms.

How To Request Support

For technical support, open a support case using the Case Manager link at <http://www.juniper.net/> or call 1-888-314-JTAC (from the United States, Canada, or Mexico) or 1-408-745-9500 (from elsewhere).

For documentation issues, fill out the bug report form located at <https://www.juniper.net/techpubs/docbug/docbugreport.html>.

Revision History

7 August 2007—Revision 3, JUNOScope Release 8.2R2

20 March 2007—Revision 2, JUNOScope Release 8.2R2

17 January 2007—Revision 1, JUNOScope Release 8.2R1

Copyright © 2007, Juniper Networks, Inc. All rights reserved.

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

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

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.