

JUNOS Software with Enhanced Services 9.1 for J-series Services Router Release Notes

Release 9.1R4
February 2009
Part Number: 530-023626-01
Revision 4

These release notes accompany Release 9.1R4 of JUNOS software with enhanced services for J-series Services Routers. They briefly describe new software and hardware features and provide a summary of the current software limitations and known defects that exist in this release.



NOTE: J-series Services Routers are currently shipped with the JUNOS software. To install JUNOS software with enhanced services on your Services Router, see the *JUNOS Software Migration Guide*. The *J-series Services Router Quick Start* is shipped with the router. You can download the *J-series Services Routers Quick Start* from the Juniper Web site at <http://www.juniper.net/techpubs/>.

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

Contents

JUNOS Software with Enhanced Services Features	3
Interfaces and Chassis	3
Security Features	4
JUNOS Features Not Supported for Chassis Clusters	4
Outstanding Issues	5
Resolved Issues	8
Errata	8
Power and Heat Dissipation Requirements for J-series PIMs	9
Supported Third-Party Hardware	9

J-series Compact Flash and Memory Requirements	10
JUNOS Software with Enhanced Services Upgrade and Downgrade	
Instructions	10
Upgrade and Downgrade Overview	11
Upgrade Software Packages	11
Recovery Software Packages	12
Before You Begin	12
Downloading Software Upgrades from Juniper Networks	13
Installing Software Upgrades with the J-Web Interface	13
Installing Software Upgrades from a Remote Server	13
Installing Software Upgrades by Uploading Files	14
Installing Software Upgrades with the CLI	15
Installing Software Upgrades by Downloading Files	15
Installing Software Upgrades from a Remote Server	16
Downgrade Instructions	16
Downgrading the Software with the J-Web Interface	17
Downgrading the Software with the CLI	17
List of Technical Publications	18
Documentation Feedback	25
Requesting Technical Support	25
Revision History	26

JUNOS Software with Enhanced Services Features

Release 9.1R4 of JUNOS software with enhanced services includes the following features. For more information, see the following manuals:

- *JUNOS Software Migration Guide*
- *JUNOS Software with Enhanced Services Getting Started Guide*
- *J-series Services Routers Quick Start*
- *JUNOS Software Design and Implementation Guide*
- *JUNOS Software Interfaces and Routing Configuration Guide*
- *JUNOS Software Administration Guide*
- *JUNOS Software CLI Reference*
- *WXC Integrated Services Module Installation and Configuration Guide*

Interfaces and Chassis

- **HA Status LED for Chassis Clusters**—The Services Router provides a high availability (HA) LED that is used to indicate the status of the router when it is deployed in single-chassis mode and when it is used in a chassis cluster. The HA LED indicates one of four states:
 - The router is not configured for clustering, or it is disabled.
 - All routers belonging to the cluster and all high availability links are available.
 - All routers belonging to the cluster are present, but some links are down.
 - A cluster member is missing or unreachable.
- **High Availability Support for Route-Based IPSec VPNs**—The Services Router enhances high availability with graceful failover by providing route-based IP Security (IPSec) VPN support in a chassis cluster, including the following features:
 - Site-to-site manual and Internet Key Exchange (IKE)-negotiated route-based IPSec VPNs
 - Next-hop tunnel binding (NHTB)
 - Dead peer detection (DPD)
 - VPN monitoring
 - Invalid Security Parameter Index (SPI)
 - Network Address Translation (NAT) traversal
 - Remote access IPSec VPNs for dynamic endpoints
 - Public key infrastructure (PKI)



NOTE: When configuring chassis clusters you are automatically in `configure private` mode. As a result, you must commit changes from the top of the hierarchy. For information about the `configure private` mode, see the *JUNOS CLI User Guide*.

Security Features

- **Generation of Self-Signed Certificates**—The Services Router supports generation of self-signed certificates.

Self-signed certificates:

- Attest to the identity of the person who creates and signs them.
- Allow for use of Secure Sockets Layer (SSL)-based services without requiring that you obtain an identity certificate signed by a certificate authority (CA).

The Services Router provides two methods for generating a self-signed certificate:

- **Automatic generation**—The self-signed certificate is configured on the router as a factory default. This certificate enables the router to provide immediate access to SSL services, such as Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS), after it is initialized.
- **Manual generation**—You can use the command-line interface (CLI) to generate a self-signed certificate, which can also be used to gain access to SSL services.

Self-signed certificates are valid for 5 years from the time they are generated.

- **SecurID for User Authentication**—The Services Router supports several methods for performing user authentication. Release 9.1 adds support for use of SecurID as an external authentication method. SecurID user authentication is an RSA proprietary authentication method that supports use of static or dynamic passwords. Dynamic passwords consist of a user's pin number and a randomly generated token. JUNOS software with enhanced services does not support use of authentication challenges.

JUNOS Features Not Supported for Chassis Clusters

For this release of JUNOS software with enhanced services, the following features are not supported when chassis clustering is enabled on the router:

- **Packet-based protocols.** All packet-based protocols, such as Multiprotocol Label Switching (MPLS), Connectionless Network Service (CLNS), and IP version 6 (IPv6)
- **Services interfaces functions.** Any function that depends on the configurable J-series services interfaces:
 - `ls-0/0/0`—Link services Multilink Point-to-Point Protocol (MLPPP), Multilink Frame Relay (MLFR), and Compressed Real-Time Transport Protocol (CRTP)
 - `gr-0/0/0`—Generic routing encapsulation (GRE) and tunneling

- ip-0/0/0—IP-over-IP (IP-IP) encapsulation
- pd-0/0/0, pe-0/0/0, and mt-0/0/0—All multicast protocols
- lt-0/0/0—Real-time performance monitoring (RPM)
- **WXC Integrated Services Module (ISM 200)**
- **Ethernet switching on some PIMs:**
 - 4-port Fast Ethernet ePIMs running in switching mode
 - 8-port and 16-port Gigabit Ethernet uPIMs running in switching mode
- **ISDN BRI**

Outstanding Issues

- ALG**
 - On J6350 Services Routers handling more than 1000 simultaneous MGCP calls, the success rate for all MGCP ALG calls is approximately 95 percent. [PR/254297]
 - JUNOS software with enhanced services does not have an option for setting default values for Sun RPC and Microsoft RPC applications. As a workaround, you can define a security policy that specifies a Sun RPC or Microsoft RPC application with the value **any** for the source address, destination address, and application name. [PR/256971]
- Authentication**
 - During user authentication, the firewall authentication table in the output of the `security firewall-authentication users` command displays multiple failures even though the network table in the output of `show network-access requests statistics` shows successful authentications. [PR/250780]
 - Your attempt to log in to the router from a management device through FTP or Telnet might fail if you type your username and password in quick succession before the prompt is displayed, in some operating systems. As a workaround, type your username and password after getting the prompts. [PR/255024]
- Chassis Cluster**
 - In a chassis cluster, the `show interface terse` command on the secondary routing engine does not display the same details as that of the primary routing engine. [PR/237982]
 - Because the `clear security alg sip call` command triggers a SIP RTO to synchronize sessions in a chassis cluster, use of the command on one node with the `node-id`, `local`, or `primary` option might result in a SIP call being removed from both nodes. [PR/263976]
 - When a new redundancy group is added to a chassis cluster, the node with lower priority might be elected as primary when the `preempt` option is not enabled for the nodes in the redundancy group. [PR/265340]
 - In a chassis cluster, if you manually fail over redundant groups to move the system from active-passive mode to active-active mode during an active call, a subsequent call transfer involving the endpoints of the existing call might fail. [PR/265598]
 - When you commit a configuration for a node belonging to a chassis cluster, all the redundancy groups might fail over to node 0. If graceful protocol restart is

not configured, the failover can destabilize routing protocol adjacencies and disrupt traffic forwarding. To allow the commit operation to take place without causing a failover, we recommend that you use the `set chassis cluster heartbeat-threshold 5` command on the cluster. [PR/265801]

- In a chassis cluster, Layer 2 switching does not work for 4-Port Fast Ethernet ePIMs, 8-Port Gigabit Ethernet uPIMs, and 16-Port Gigabit Ethernet uPIMs. [PR/266857]
 - In a chassis cluster, if a forwarding process restart or system reboot triggers a cold synchronization during an active SIP call, the call might stay in both routing nodes even after the endpoints hang up. As a work around, use the `clear security alg sip call` command to clear the call. [PR/267696]
 - In a chassis cluster, a high load of SIP ALG traffic might result in some call leaks in active resource manager groups and gates on the backup router. [PR/268613]
 - A chassis cluster using Web authentication might display an “invalid username-password” message even though the user is successfully authenticated locally or through authentication servers. To verify user authentication success, use the `show security firewall-authentication users` command. [PR/274077]
 - In a chassis cluster, CA certificate enrollment from the secondary Routing Engine does not work. As a workaround, enroll the CA certificate from the primary Routing Engine. [PR/278420]
 - In a chassis cluster, J-Web does not enable you to configure the address book. We recommend that you use the command-line interface (CLI) to configure the address book. [PR/281986]
- Class of Service**
- J4350 and J6350 Services Routers might not have the requisite data buffers needed to meet expected delay-bandwidth requirements. Lack of data buffers might degrade CoS performance with smaller-sized (500 bytes or less) packets. [PR/73054]
 - With a CoS configuration, when you try to delete all the flow sessions using the `clear security flow session` command, the WX application acceleration platform may fail over with heavy traffic. [PR/273843]
 - In J2350 Services Routers, the CoS does not work when the data sent to the egress GE interface is more than 100 MB. [PR/281367]
- Flow**
- Firewall filter counters for ingress (inbound) and egress (outbound) forwarding table filters (FTFs) do not work for IPv4. [PR/97230]
 - OSPF over GRE over IPSec does not work. [PR/105279]
 - In JUNOS software with enhanced services, the TTL value on the Internet control message protocol (ICMP) responses is set to 65. [PR/233844]
 - Even when forwarding options are set to drop packets for the ISO protocol family, the router forms End System-to-Intermediate System (ES-IS) adjacencies and transmits packets because ES-IS packets are Layer 2 terminating packets. [PR/252957]

- OSPF over a multipoint interface connected as a hub-and-spoke network does not restart when a new path is found to the same destination. [PR/280771]
 - On J-series Services Routers, outbound filters will be applied twice for host-generated IPv4 traffic. [PR/301199]
- Infrastructure**
- On J-series Services Routers, you cannot use a USB device that provides U3 features (such as the U3 Titanium device from SanDisk Corporation) as the media device during system boot. You must remove the U3 support before using the device as a boot medium. For the U3 Titanium device, you can use the U3 Launchpad Removal Tool on a Windows-based system to remove the U3 features. The tool is available for download at <http://www.sandisk.com/Retail/Default.aspx?CatID=1415>. (To restore the U3 features, use the U3 Launchpad Installer Tool accessible at <http://www.sandisk.com/Retail/Default.aspx?CatID=1411>). [PR/102645]
 - If the router does not have an ARP entry for an IP address, it drops the first packet from itself to that IP address. [PR/233867]
 - On J2320, J2350, J4350, and J6350 Services Routers, when you press the F10 key to save and exit from BIOS configuration mode, the operation might not work as expected. As a workaround, use the **Save and Exit** option from the **Exit** menu. This issue can be seen on the J4350 and J6350 routers with BIOS Version 080011 and on the J2320 and J2350 routers with BIOS Version 080012. [PR/237721]
 - On J2320, J2350, J4350, and J6350 Services Routers, the **Clear NVRAM** option in the BIOS configuration mode does not work as expected. This issue can be seen on the J4350 and J6350 routers with BIOS Version 080011 and on the J2320 and J2350 routers with BIOS Version 080012. To help mitigate this issue, note any changes you make to the BIOS configuration so that you can revert to the default BIOS configuration as needed. [PR/237722]
 - If you enable security trace options, the log file might not be created in the default location at `/var/log/security-trace`. As a workaround, manually set the log file to the directory `/var/log/security-trace`. [PR/254563]
- Interfaces and Chassis**
- The link status of the onboard Gigabit Ethernet interfaces (`ge-0/0/0` through `ge-0/0/3`) or the 1-port Gigabit Ethernet ePIM interface on J4350 and J6350 Services Routers fails when you configure these interfaces in loopback mode. [PR/72381]
 - If the MTU is set to more than 6 KB for a built-in Gigabit Ethernet port or a 1-port Gigabit Ethernet ePIM, packets might be discarded with an FCS error. [PR/82245]
 - For policy-based IPsec VPNs, you cannot configure `proxy-id`. The `proxy-id` field is supported for only route-based IPsec VPNs. [PR/296468]

- Routing** ■ Asymmetric routing, such as tracing a route to a destination behind J-series routers running JUNOS software with enhanced services with Virtual Router Redundancy Protocol (VRRP), does not work. [PR/237589]
- System** ■ The ping status of the generic routing interfaces (gr-x/y/x) connection established through ISDN simulator fails. As a workaround, deactivate and reactivate the generic routing interfaces. [PR/282588]
- WXC Integrated Services Module** ■ When two J-series routers with WXC Integrated Services Modules (ISM 200s) installed are configured as peers, traceroute fails if `redirect-wx` is configured on both peers. [PR/227958]
- JUNOS software with enhanced services does not support policy-based VPN with WXC Integrated Services Modules (ISM200s). [PR/281822]

Resolved Issues

The following issues have been resolved since Release 9.1R2 of JUNOS software with enhanced services. The identifier following the description is the tracking number in our bug database.

- Chassis Cluster** ■ In a chassis cluster configuration, after redundancy group 1 failed over to the secondary node, the statistics for the TCP SYN-ACK-ACK proxy screen were displayed for the primary node rather than the secondary. [PR/264790: This issue has been resolved.]
- Flow** ■ When heartbeat signals were sent to an interface at the server side, the counter on that interface was not incremented even after considerable wait time. [PR/273901: This issue has been resolved.]

Errata

- Screens** ■ The following guides contain incorrect screen configuration instructions:
 - *JUNOS Software Security Configuration Guide*, “Attack Detection and Prevention” chapter
 - *JUNOS Software Design and Implementation Guide*, “Implementing Firewall Deployments for Branch Offices” chapter

Examples throughout both of these guides describe how to configure screen options using the `[set security screen screen-name]` CLI statements. Instead, you should use the `[set security screen ids-option screen-name]` CLI statements. All

screen configuration options are located at the [set security screen ids-option *screen-name*] level of the configuration hierarchy.

Power and Heat Dissipation Requirements for J-series PIMs

On J-series Services Routers, the system monitors the PIMs and verifies that the PIMs fall within the power and heat dissipation capacity of the chassis. If power management is enabled and the capacity is exceeded, the system prevents one or more of the PIMs from becoming active.



CAUTION: Disabling power management can result in hardware damage if you overload the chassis capacities.

You can also use CLI commands to choose which PIMs are disabled. For details about calculating the power and heat dissipation capacity of each PIM and troubleshooting procedures, see the *J-series Services Routers Hardware Guide*.

Supported Third-Party Hardware

The following third-party hardware is supported for use with J-series Services Routers running JUNOS software with enhanced services.

USB Modem We recommend using a Multi-Tech MultiModem MT5634ZBA-USB-V92 USB modem with J-series Services Routers.

Storage Devices The USB slots on J-series Services Routers accept a USB storage device or USB storage device adapter with a compact flash disk installed, as defined in the CompactFlash Specification published by the CompactFlash Association. When the USB device is installed and configured, it automatically acts as a secondary boot device if the primary compact flash disk fails on startup. Depending on the size of the USB storage device, you can also configure it to receive any core files generated during a router failure. The USB device must have a storage capacity of at least 256 MB.

Table 1 on page 9 lists the USB and compact flash storage devices supported for use with the J-series Services Routers.

Table 1: Supported Storage Devices on the J-series Services Routers

Manufacturer	Storage Capacity	Third-Party Part Number
SanDisk—Cruzer Mini 2.0	256 MB	SDCZ2-256-A10
SanDisk	512 MB	SDCZ3-512-A10
SanDisk	1024 MB	SDCZ7-1024-A10
Kingston	512 MB	DTI/512KR
Kingston	1024 MB	DTI/1GBKR

Table 1: Supported Storage Devices on the J-series Services Routers (continued)

Manufacturer	Storage Capacity	Third-Party Part Number
SanDisk—ImageMate USB 2.0 Reader/Writer for CompactFlash Type I and II	N/A	SDDR-91-A15
SanDisk CompactFlash	512 MB	SDCFB-512-455
SanDisk CompactFlash	1 GB	SDCFB-1000.A10

J-series Compact Flash and Memory Requirements

Table 2 on page 10 lists the compact flash and DRAM requirements for J-series Services Routers.

Table 2: J-series Compact Flash and DRAM Requirements

Model	Minimum Compact Flash Required	Minimum DRAM Required	Maximum DRAM Supported
J2320	512 MB	512 MB	1 GB
J2350	512 MB	512 MB	1 GB
J4350	512 MB	512 MB	2 GB
J6350	512 MB	1 GB	2 GB

JUNOS Software with Enhanced Services Upgrade and Downgrade Instructions



NOTE: This information applies only to upgrading one release of JUNOS software with enhanced services to another. To upgrade from the JUNOS software to JUNOS software with enhanced services, see the *JUNOS Software Migration Guide*.

In JUNOS Release 8.5, the JUNOS software was extended to use FreeBSD version 6.1. As a result, the following requirements apply when you upgrade your router to JUNOS Release 8.5 and later:

- To upgrade with the JUNOS CLI, the minimum requirement for installation media (such as a compact flash disk, internal flash disk, or PC card) is 512 MB. To use the J-Web interface for an upgrade, you must have 512 MB or more.

- Before upgrading to JUNOS software with enhanced services, perform the following:
 - Upgrade to a 512-MB compact flash. For upgrading the DRAM module or compact flash, see the “Upgrading the DRAM Module or Compact Flash” section of the *JUNOS Software Migration Guide*. For information on formatting a new, blank compact flash card, see the “Configuring Internal Compact Flash Recovery” section of the *JUNOS Software Administration Guide*.

This section contains the following topics:

- Upgrade and Downgrade Overview on page 11
- Before You Begin on page 12
- Downloading Software Upgrades from Juniper Networks on page 13
- Installing Software Upgrades with the J-Web Interface on page 13
- Installing Software Upgrades with the CLI on page 15
- Downgrade Instructions on page 16

Upgrade and Downgrade Overview

Typically, you upgrade JUNOS software with enhanced services on a Services Router by downloading a set of images onto your router or onto another system on your local network, such as a PC. You then uncompress the package and install the uncompressed software using the CLI. Finally, you boot your system with this upgraded device.

A JUNOS software package is a collection of files that make up a software component. You can download software packages either for upgrading JUNOS software or for recovering a primary compact flash.

All JUNOS software and JUNOS software with enhanced services is delivered in signed packages that contain digital signatures, Secure Hash Algorithm (SHA-1) checksums, and Message Digest 5 (MD5) checksums. For more information about signed software packages, see the *JUNOS Software Installation and Upgrade Guide*.

Upgrade Software Packages

Download an upgrade software package, also known as an install package, to install new features and software fixes as they become available.

An upgrade software package name is in the following format:
package-name-m.nZx.y-distribution.tgz.

- *package-name* is the name of the package—for example, `junos-jsr`.
- *m.n* is the software release, with *m* representing the major release number—for example, `9.0`.
- *Z* indicates the type of software release. For example, **R** indicates released software, and **B** indicates beta-level software.

- *x.y* represents the version of the major software release—for example, **1.1**.
- *distribution* indicates the area for which the software package is provided—**domestic** for the United States and Canada and **export** for worldwide distribution.

A sample JUNOS software with enhanced services package name is `junos-jsr-9.1R4.1-domestic.tgz`.

Recovery Software Packages

Download a recovery software package, also known as an install media package, to recover a primary compact flash device.

A recovery software package name is in the following format:
package-name-m.nZx-export-cfnnn.gz.

- *package-name* is the name of the package—for example, `junos-jsr`.
- *m.n* is the software release, with *m* representing the major release number—for example, **8.5**.
- *Z* indicates the type of software release. For example, **R** indicates released software, and **B** indicates beta-level software.
- *x* represents the version of the major software release—for example, **1**.
- **export** indicates that the recovery software package is the exported worldwide software package version.
- *cfnnn* indicates the size of the target compact flash device in megabytes—for example, `cf256`.

A sample JUNOS software with enhanced services recovery package name is `junos-jsr-8.5R1-export-cf256.gz`.

Before You Begin

Before upgrading, be sure to back up the currently running and active file system and configuration so that you can recover to a known, stable environment in case the upgrade is unsuccessful. To back up the file system, you must have a removable compact flash disk installed on a J2320 or J2350 Services Router, or a USB drive installed on any J-series Services Router. The backup device must have a storage capacity of at least 256 MB.

To back up the file system to the removable compact flash disk, issue the following command:

```
user@host> request system snapshot media removable-compact-flash
```

To back up the file system to the removable USB drive, issue the following command:

```
user@host> request system snapshot media usb
```

Downloading Software Upgrades from Juniper Networks

Follow these steps to download software upgrades from Juniper Networks:

1. Using a Web browser, follow the links to the download URL on the Juniper Networks Web page. Depending on your location, select either **Canada and U.S. Version** or **Worldwide Version**:
 - <https://www.juniper.net/support/csc/swdist-domestic/> (customers in the United States and Canada)
 - <https://www.juniper.net/support/csc/swdist-ww/> (all other customers)
2. Log in to the Juniper Networks Web site using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. Using the J-Web interface or the CLI, select the appropriate JUNOS software with enhanced services image for your application. For information about JUNOS software with enhanced services packages, see “Upgrade and Downgrade Overview” on page 11.
4. Download JUNOS software with enhanced services to a local host or to an internal software distribution site.

Installing Software Upgrades with the J-Web Interface

If your router has at least a 512-MB compact flash, you can use the J-Web interface to install software upgrades from a remote server using FTP or HTTP, or by uploading the software image to the router. This section contains the following topics:

- Installing Software Upgrades from a Remote Server on page 13
- Installing Software Upgrades by Uploading Files on page 14

Installing Software Upgrades from a Remote Server

If your router has at least a 512-MB compact flash, you can use the J-Web interface to install software packages on the router that are retrieved with FTP or HTTP from the location specified. Installing software upgrades using this method copies the software image to the router.



NOTE: This procedure applies only to upgrading one release of JUNOS software with enhanced services to another. To upgrade from the JUNOS software to JUNOS software with enhanced services, see the *JUNOS Software Migration Guide*.

To install software upgrades from a remote server:

1. Download the software package as described in “Downloading Software Upgrades from Juniper Networks” on page 13.
2. In the J-Web interface, select **Manage > Software > Install Package**.

3. On the Install Package Quick Configuration page, enter information into the fields described in Table 3 on page 14.
4. Click **Fetch and Install Package**. The software is activated after the router reboots.

Table 3: Install Package Summary

Field	Function	Your Action
Package Location (required)	Specifies the FTP or HTTP server, file path, and software package name.	Type the full address of the software package location server—one of the following: <code>ftp://hostname/pathname/package-name</code> <code>http://hostname/pathname/package-name</code>
User	Specifies the username, if the server requires one.	Type the username.
Password	Specifies the password, if the server requires one.	Type the password.
Reboot If Required	If this box is checked, the router is automatically rebooted when the upgrade is complete.	Check the box if you want the router to reboot automatically when the upgrade is complete.

Installing Software Upgrades by Uploading Files

If your router has at least a 512-MB compact flash, you can use the J-Web interface to install software packages uploaded from your computer to the router.



NOTE: This procedure applies only to upgrading one release of JUNOS software with enhanced services to another. To upgrade from the JUNOS software to JUNOS software with enhanced services, see the *JUNOS Software Migration Guide*.

To install software upgrades by uploading files:

1. Download the software package as described in “Downloading Software Upgrades from Juniper Networks” on page 13.
2. In the J-Web interface, select **Manage > Software > Upload Package**.
3. On the Upload Package page, enter information into the fields described in Table 4 on page 14.
4. Click **Upload Package**. The software is activated after the router has rebooted.

Table 4: Upload Package Summary

Field	Function	Your Action
File to Upload (required)	Specifies the location of the software package on the local system.	Type the location of the software package, or click Browse to navigate to the location.

Table 4: Upload Package Summary (continued)

Field	Function	Your Action
Reboot If Required	If this box is checked the router is automatically rebooted when the upgrade is complete.	Select the check box if you want the router to reboot automatically when the upgrade is complete.

Installing Software Upgrades with the CLI

This section contains the following topics:

- Installing Software Upgrades by Downloading Files on page 15
- Installing Software Upgrades from a Remote Server on page 16

Installing Software Upgrades by Downloading Files

To install software upgrades by downloading files to the router:

1. Download the JUNOS software with enhanced services package to the router using the following command:

```
user@host> file copy source destination
```

Replace *source* with one of the following paths:

- ftp://hostname/pathname/package-name
- or
- http://hostname/pathname/package-name

Replace *destination* with the path to the destination directory on the router. We recommend the `/var/tmp` directory.

2. Install the new package on the Services Router, entering the following command in operational mode in the CLI:

```
user@host> request system software add validate unlink no-copy source
```

Replace *source* with `/pathname/package-name` (for example, `/var/tmp/junos-jsr-8.5R2.1.tar.gz`).

By default, the `request system software add` command uses the `validate` option to validate the software package against the current configuration as a prerequisite to adding the software package. This validation ensures that the router can reboot successfully after the software package is installed. This is the default behavior when you are adding a software package.

The `unlink` option removes the package at the earliest opportunity so that the router has enough room to complete the installation.

(Optional) The `no-copy` option specifies that a software package is installed, but a copy of the package is not saved. Include this option if you do not have enough

space on the compact flash to perform an upgrade that keeps a copy of the package on the router.

3. After the software package is installed, reboot the router:

```
user@host> request system reboot
```

When the reboot is complete, the router displays the login prompt.

Installing Software Upgrades from a Remote Server

To install the software upgrades from a remote server:

1. Install the JUNOS software with enhanced services package on the Services Router, entering the following command in operational mode in the CLI:

```
user@host> request system software add validate unlink no-copy source
```

Replace *source* with one of the following paths:

- `ftp://hostname/pathname/package-name`
- or
- `http://hostname/pathname/package-name`

By default, the `request system software add` command uses the `validate` option to validate the software package against the current configuration as a prerequisite to adding the software package. This validation ensures that the router can reboot successfully after the software package is installed. This is the default behavior when you are adding a software package.

The `unlink` option removes the package at the earliest opportunity so that the router has enough room to complete the installation.

(Optional) The `no-copy` option specifies that a software package is installed, but a copy of the package is not saved. Include this option if you do not have enough space on the compact flash to perform an upgrade that keeps a copy of the package on the router.

2. After the software package is installed, reboot the router:

```
user@host> request system reboot
```

When the reboot is complete, the router displays the login prompt.

Downgrade Instructions

This section contains the following topics:

- Downgrading the Software with the J-Web Interface on page 17
- Downgrading the Software with the CLI on page 17



NOTE: Juniper Networks supports direct software downgrades for a maximum of three releases.

Downgrading the Software with the J-Web Interface

You can downgrade the software from the J-Web interface. For the changes to take effect, you must reboot the router.



NOTE: This procedure applies only to downgrading one release of JUNOS software with enhanced services to another. To downgrade JUNOS software with enhanced services to the JUNOS software, see the *JUNOS Software Migration Guide*.

To downgrade software with the J-Web interface:

1. In the J-Web interface, select **Manage > Software > Downgrade**. The image of the previous software version (if any) is displayed on this page.



NOTE: After you perform this operation, you cannot undo it.

2. Select **Downgrade** to downgrade to the previous version of the software or **Cancel** to cancel the downgrade process.
3. When the downgrade process is complete, for the new software to take effect, click **Manage > Reboot** from the J-Web interface to reboot the router.

After you downgrade the software, the previous release is loaded, and you cannot reload the running version of software again. To downgrade to an earlier version of software, follow the procedure for upgrading, using the software image of JUNOS software with enhanced services labeled with the appropriate release.

Downgrading the Software with the CLI

You can revert to the previous version of software using the `request system software rollback` command in the CLI. For the changes to take effect, you must reboot the router. To downgrade to an earlier version of software, follow the procedure for upgrading, using the software image of JUNOS software with enhanced services labeled with the appropriate release.



NOTE: This procedure applies only to downgrading one release of JUNOS software with enhanced services to another. To downgrade JUNOS software with enhanced services to the JUNOS software, see the *JUNOS Software Migration Guide*.

To downgrade software with the CLI:

1. Enter the `request system software rollback` command to return to the previous JUNOS software version:

```
user@host> request system software rollback
```

The previous software version is now ready to become active when you next reboot the router.

2. Reboot the router:

```
user@host> request system reboot
```

The router is now running the previous version of the software. To downgrade to an earlier version of software, follow the procedure for upgrading, using the software image of JUNOS software with enhanced services labeled with the appropriate release.

List of Technical Publications

Table 5 on page 18 lists the software and hardware guides and release notes for Juniper Networks J-series, M-series, MX-series, and T-series routing platforms and describes the contents of each document. Table 6 on page 22 lists the books included in the *Network Operations Guide* series. Table 7 on page 23 lists the manuals and release notes supporting JUNOS software with enhanced services. All documents are available at <http://www.juniper.net/techpubs/>.

Table 8 on page 24 lists additional books on Juniper Networks solutions that you can order through your bookstore. A complete list of such books is available at <http://www.juniper.net/books>.

Table 5: Technical Documentation for Supported Routing Platforms

Book	Description
JUNOS Software for Supported Routing Platforms	
<i>Access Privilege</i>	Explains how to configure access privileges in user classes by using permission flags and regular expressions. Lists the permission flags along with their associated command-line interface (CLI) operational mode commands and configuration statements.
<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.

Table 5: Technical Documentation for Supported Routing Platforms (continued)

Book	Description
<i>High Availability</i>	Provides an overview of hardware and software resources that ensure a high level of continuous routing platform operation and describes how to configure high availability (HA) features such as nonstop active routing (NSR) and graceful Routing Engine switchover (GRES).
<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>Multiplay Solutions</i>	Describes how you can deploy IPTV and voice over IP (VoIP) services in your network.
<i>MX-series Solutions Guide</i>	Describes common configuration scenarios for the Layer 2 features supported on the MX-series routers, including basic bridged VLANs with normalized VLAN tags, aggregated Ethernet links, bridge domains, Multiple Spanning Tree Protocol (MSTP), and integrated routing and bridging (IRB).
<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, and forwarding options.
<i>Protected System Domain</i>	Provides an overview of the JCS 1200 platform and the concept of Protected System Domains (PSDs). The JCS 1200 platform, which contains up to six redundant pairs of Routing Engines running JUNOS software, is connected to a T320 router or to a T640 or T1600 routing node. To configure a PSD, you assign any number of Flexible PIC concentrators (FPCs) in the T-series routing platform to a pair of Routing Engines on the JCS 1200 platform. Each PSD has the same capabilities and functionality as a physical router, with its own control plane, forwarding plane, and administration.
<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 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 router.

Table 5: Technical Documentation for Supported Routing Platforms (continued)

Book	Description
<i>Software Installation and Upgrade Guide</i>	Describes the JUNOS software components and packaging and explains 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 explains 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 policies and protocols, 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 class of service (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 graphical user interface (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.

Table 5: Technical Documentation for Supported Routing Platforms (continued)

Book	Description
<i>JUNOS XML API Operational Reference</i>	Provides reference pages for the operational tag elements in the JUNOS XML API.
<i>NETCONF API Guide</i>	Describes how to use the NETCONF API to monitor and configure Juniper Networks routing platforms.
<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.
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's Physical Interface Cards (PICs). Each platform has its own PIC guide.
<i>DPC Guide</i>	Describes the Dense Port Concentrators (DPCs) for all MX-series routers.
JUNOScope Documentation	
<i>JUNOScope Software User Guide</i>	Describes the JUNOScope software graphical user interface (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.
Advanced Insight Solutions (AIS) Documentation	
<i>Advanced Insight Solutions Guide</i>	Describes the Advanced Insight Manager (AIM) application, which provides a gateway between JUNOS devices and Juniper Support Systems (JSS) for case management and intelligence updates. Explains how to run AI scripts on Juniper Networks devices.
J-series Routing Platform Documentation	
<i>Getting Started Guide</i>	Provides an overview, basic instructions, and specifications for J-series routing platforms. 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.

Table 5: Technical Documentation for Supported Routing Platforms (continued)

Book	Description
<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.
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 summarize known problems with the hardware and accompanying software. Each platform has its own release notes.
<i>JUNOScope 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>AIS Release Notes</i>	Summarize AIS new features and guidelines, identify known and resolved problems, provide information that might have been omitted from the manuals, and provide initial setup, upgrade, and downgrade procedures.
<i>AIS AI Script Release Notes</i>	Summarize AI Scripts new features, identify known and resolved problems, provide information that might have been omitted from the manuals, and provide instructions for automatic and manual installation, including deleting and rolling back.
<i>J-series Services Router Release Notes</i>	Briefly describe Services Router features, identify known hardware problems, and provide upgrade and downgrade instructions.

Table 6: JUNOS Software Network Operations Guides

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.
<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 routing platforms in the network, and using the layered MPLS troubleshooting model to investigate problems with an MPLS network.

Table 6: JUNOS Software Network Operations Guides (continued)

Book	Description
<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>MPLS Fast Reroute</i>	Describes operational information helpful in monitoring and troubleshooting an MPLS network configured with fast reroute (FRR) and load balancing.
<i>Hardware</i>	Describes tasks for monitoring M-series and T-series routing platforms.

To configure and operate a J-series Services Router running JUNOS software with enhanced services, you must also use the configuration statements and operational mode commands documented in JUNOS configuration guides and command references. To configure and operate a WX Integrated Services Module, you must also use WX documentation.

Table 7: JUNOS Software with Enhanced Services Documentation

Book	Description
All Platforms	
<i>JUNOS Software Interfaces and Routing Configuration Guide</i>	Explains how to configure J-series interfaces for basic IP routing with standard routing protocols, ISDN service, firewall filters (access control lists), and class-of-service (CoS) traffic classification.
<i>JUNOS Software Security Configuration Guide</i>	Explains how to configure and manage security services such as stateful firewall policies, IP Security (IPsec) virtual private networks (VPNs), firewall screens, Network Address Translation (NAT), Public Key Cryptography, and Application Layer Gateways (ALGs).
<i>JUNOS Software Administration Guide</i>	Shows how to monitor J-series devices and routing operations, firewall and security services, system alarms and events, and network performance. This guide also shows how to administer user authentication and access, upgrade software, and diagnose common problems.
<i>JUNOS Software CLI Reference</i>	Provides the complete JUNOS software with enhanced services configuration hierarchy and describes the configuration statements and operational mode commands not documented in the standard JUNOS manuals.
J-series Only	
<i>JUNOS Software Design and Implementation Guide</i>	Provides guidelines and examples for designing and implementing IP Security (IPsec) virtual private networks (VPNs), firewalls, and routing on J-series Services Routers running JUNOS software with enhanced services.

Table 7: JUNOS Software with Enhanced Services Documentation (continued)

Book	Description
<i>J-series Services Routers Quick Start</i>	Explains how to quickly set up a J-series Services Router. This document contains router declarations of conformity.
<i>JUNOS Software Migration Guide</i>	Provides instructions for migrating an SSG device running ScreenOS software or a J-series Services Router running the JUNOS software to JUNOS software with enhanced services.
<i>WXC Integrated Services Module Installation and Configuration Guide</i>	Explains how to install and initially configure a WXC Integrated Services Module in a J-series Services Router for application acceleration.
<i>JUNOS Software with Enhanced Services for J-series Routers Release Notes</i>	Summarizes new features and known problems for a particular release of JUNOS software with enhanced services on J-series Services Routers, including J-Web interface features and problems. The release notes also contain corrections and updates to the manuals and software upgrade and downgrade instructions for JUNOS software with enhanced services.

Table 8: Additional Books Available Through <http://www.juniper.net/books>

Book	Description
<i>Interdomain Multicast Routing</i>	Provides background and in-depth analysis of multicast routing using Protocol Independent Multicast sparse mode (PIM SM) and Multicast Source Discovery Protocol (MSDP); details any-source and source-specific multicast delivery models; explores multiprotocol BGP (MBGP) and multicast IS-IS; explains Internet Gateway Management Protocol (IGMP) versions 1, 2, and 3; lists packet formats for IGMP, PIM, and MSDP; and provides a complete glossary of multicast terms.
<i>JUNOS Cookbook</i>	Provides detailed examples of common JUNOS software configuration tasks, such as basic router configuration and file management, security and access control, logging, routing policy, firewalls, routing protocols, MPLS, and VPNs.
<i>MPLS-Enabled Applications</i>	Provides an overview of Multiprotocol Label Switching (MPLS) applications (such as Layer 3 virtual private networks [VPNs], Layer 2 VPNs, virtual private LAN service [VPLS], and pseudowires), explains how to apply MPLS, examines the scaling requirements of equipment at different points in the network, and covers the following topics: point-to-multipoint label switched paths (LSPs), DiffServ-aware traffic engineering, class of service, interdomain traffic engineering, path computation, route target filtering, multicast support for Layer 3 VPNs, and management and troubleshooting of MPLS networks.
<i>OSPF and IS-IS: Choosing an IGP for Large-Scale Networks</i>	Explores the full range of characteristics and capabilities for the two major link-state routing protocols: Open Shortest Path First (OSPF) and IS-IS. Explains architecture, packet types, and addressing; demonstrates how to improve scalability; shows how to design large-scale networks for maximum security and reliability; details protocol extensions for MPLS-based traffic engineering, IPv6, and multitopology routing; and covers troubleshooting for OSPF and IS-IS networks.
<i>Routing Policy and Protocols for Multivendor IP Networks</i>	Provides a brief history of the Internet, explains IP addressing and routing (Routing Information Protocol [RIP], OSPF, IS-IS, and Border Gateway Protocol [BGP]), explores ISP peering and routing policies, and displays configurations for both Juniper Networks and other vendors' routers.

Table 8: Additional Books Available Through <http://www.juniper.net/books> (continued)

Book	Description
<i>The Complete IS-IS Protocol</i>	Provides the insight and practical solutions necessary to understand the IS-IS protocol and how it works by using a multivendor, real-world approach.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document name
- Document part number
- Page number
- Software release version (not required for *Network Operations Guides [NOGs]*)

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 postsales 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/customers/support/downloads/710059.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 located at <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, visit us at <http://www.juniper.net/support/requesting-support.html>.

If you are reporting a hardware or software problem, issue the following command from the CLI before contacting support:

```
user@host> request support information | save filename
```

To provide a core file to Juniper Networks for analysis, compress the file with the `gzip` utility, rename the file to include your company name, and copy it to `ftp.juniper.net:pub/incoming`. Then send the filename, along with software version information (the output of the `show version` command) and the configuration, to `support@juniper.net`. For documentation issues, fill out the bug report form located at <https://www.juniper.net/cgi-bin/docbugreport/>.

Revision History

February 2009—Revision 4, Release 9.1R4 of JUNOS software with enhanced services.

October 2008—Revision 3, Release 9.1R3 of JUNOS software with enhanced services.

June 2008—Revision 2, Release 9.1R2 of JUNOS software with enhanced services.

April 2008—Revision 1, Release 9.1R1 of JUNOS software with enhanced services.

Copyright © 2009, Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, ScreenOS, and Steel-Belted Radius are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOSe is a trademark 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.