



Junos[®] OS

Installation and Upgrade Guide for Security Devices

Release
12.1X46-D10



Modified: 2016-04-17

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

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, 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.

Junos[®] OS Installation and Upgrade Guide for Security Devices
12.1X46-D10
Copyright © 2016, Juniper Networks, Inc.
All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

	About the Documentation	xiii
	Documentation and Release Notes	xiii
	Supported Platforms	xiii
	Using the Examples in This Manual	xiii
	Merging a Full Example	xiv
	Merging a Snippet	xiv
	Documentation Conventions	xv
	Documentation Feedback	xvii
	Requesting Technical Support	xvii
	Self-Help Online Tools and Resources	xvii
	Opening a Case with JTAC	xviii
Part 1	Overview	
Chapter 1	Product Overview	3
	Junos OS Overview	3
	One Operating System	3
	One Software Release	3
	One Modular Software Architecture	4
	Junos OS Editions	4
	Installation Categories on the J Series Services Routers	5
	Software Naming Convention	5
	Junos OS Release Numbers	6
	Hardware Overview (J Series Services Routers)	7
	System Memory	7
	Storage Media	8
Chapter 2	Software Installation and Upgrade	9
	Installation Type Overview	9
	Standard Installation	9
	Category Change Installation	9
	Recovery Installation	10
	Software Package Information Security	10
	Understanding Junos OS Upgrades for SRX Series Devices	10
	Understanding Junos OS Upgrades for J Series Devices	11
	Junos OS Upgrade Methods on the SRX Series Devices	12
	Understanding Junos OS Upgrade and Downgrade Procedures for on SRX Series Devices	13

	Understanding Junos OS Upgrade and Downgrade Procedures for J Series	
	Devices	14
	Junos OS Upgrade Packages	14
	Junos OS Recovery Packages	14
	Installation Modules	15
	Understanding Download Manager	16
	Overview	16
	Using Download Manager to Upgrade Junos OS	17
	Handling Errors	17
	Considerations	18
Chapter 3	Dual-Root Partitioning and Autorecovery	19
	Dual-Root Partitioning Scheme Overview	19
	Boot Media and Boot Partition on the SRX Series Devices	20
	Important Features of the Dual-Root Partitioning Scheme	20
	Understanding Integrity Check and Autorecovery of Configuration, Licenses, and	
	Disk Information	21
	Overview	21
	How Autorecovery Works	21
	How to Use Autorecovery	22
	Data That Is Backed Up in an Autorecovery	22
	Troubleshooting Alarms	22
	Considerations	23
Chapter 4	BIOS Upgrade	25
	Understanding Auto BIOS Upgrade Using Junos CLI	25
	Understanding Manual BIOS Upgrade Using Junos CLI	25
Chapter 5	Autoinstallation	27
	Autoinstallation Overview	27
	Automatic Installation of Configuration Files	28
	Supported Autoinstallation Interfaces and Protocols	28
	Typical Autoinstallation Process on a New Device	29
	Automatic Installation of Configuration Files (J Series Services Routers and SRX	
	Series Services Gateways)	30
	J Series Automatic Installation Overview	30
	SRX Series Services Gateways Automatic Installation Overview	31
Chapter 6	Licenses	33
	Junos OS License Overview	33
	License Enforcement	33
	License Key Components	34
	License Management Fields Summary	34
	License Enforcement	35
	Junos OS Feature License Model Number for J Series Services Routers and SRX	
	Series Services Gateways	36

Part 2	Installation	
Chapter 7	Software Installation and Upgrade	41
	Upgrading Individual Software Packages	42
	Preparing Your SRX Series Device for Junos OS Upgrades	44
	Preparing Your J Series Services Router for Junos OS Upgrades	45
	Preparing the USB Flash Drive to Upgrade Junos OS	46
	Determining the Junos OS Version	48
	Connecting to the Console Port	48
	Backing Up the Current Installation (J Series Services Routers and SRX Series Services Gateways)	49
	Downloading Software	50
	Downloading Software with a Browser	50
	Downloading Software Using the Command-Line Interface	51
	Downloading Junos OS Upgrades for SRX Series Devices	52
	Downloading Junos OS Upgrades for J Series Devices	53
	Checking the Current Configuration and Candidate Software Compatibility	53
	Verifying Available Disk Space on SRX Series Devices	54
	Example: Installing Junos OS Upgrades on SRX Series Devices	55
	Example: Installing Junos OS Upgrades on J Series Devices	57
	Installing Junos OS Using TFTP on SRX Series Devices	60
	Installing Junos OS Using a USB Flash Drive on SRX Series Devices	62
	Installing Junos OS Upgrades from a Remote Server on the SRX Series Devices	63
	Installing Junos OS Upgrades from a Remote Server on J Series Devices	64
Chapter 8	Dual-Root Partitioning and Autorecovery	67
	Understanding Automatic Recovery of the Primary Junos OS Image with Dual-Root Partitioning	67
	Understanding How the Primary Junos OS Image with Dual-Root Partitioning Recovers on SRX Series Devices	69
	Junos OS Release 9.6 or Earlier Installation on SRX Series Devices with Dual-Root Partitioning	71
	Junos OS Release 10.0 or Later Upgrades with Dual-Root Partitioning on SRX Series Devices	72
	Example: Installing Junos OS on SRX Series Devices Using the Partition Option	72
	Reinstalling the Single-Root Partition Using request system software add Command	76
Chapter 9	Boot Loaders and Boot Devices	77
	Installing Junos OS from the Boot Loader Using a USB Storage Device on an SRX Series Device	77
	Upgrading the Boot Loader on SRX Series Devices	77
Chapter 10	Software Downgrade	79
	Example: Downgrading Junos OS on SRX Series Devices	79
	Example: Downgrading Junos OS on J Series Devices	81

Part 3	Configuration	
Chapter 11	Autoinstallation	87
	Example: Configuring Autoinstallation	87
Chapter 12	Backup and Snapshot Configuration Files	91
	Configuring a Boot Device to Receive Junos OS Failure Memory Snapshots in J Series Devices	91
	Configuring External CompactFlash on SRX650 Devices	92
Chapter 13	Boot Loaders and Boot Devices	95
	Example: Configuring Boot Devices for SRX Series Devices	95
	Example: Configuring Boot Devices for J Series Devices	98
Chapter 14	Configuration Statements	101
	System Configuration Statement Hierarchy	101
	autoinstallation	132
	configuration-servers	133
	interfaces (Autoinstallation)	134
	license	135
	usb	137
Part 4	Administration	
Chapter 15	Auto BIOS	141
	Disabling Auto BIOS Upgrade on SRX Series Devices	141
Chapter 16	Licenses	143
	Displaying License Keys	143
	Generating a License Key	144
	Downloading License Keys	144
	Saving License Keys	145
	Updating License Keys	146
	Example: Adding a New License Key	146
	Example: Deleting a License Key	150
Chapter 17	Software Stop and Restart	153
	Example: Rebooting SRX Series Devices	153
	Example: Rebooting J Series Devices	155
	Restarting the Chassis on SRX Series Devices	157
	Restarting the Chassis on J Series Devices	157
	Example: Halting SRX Series Devices	158
	Example: Halting J Series Devices	159
	Bringing Chassis Components Online and Offline on SRX Series Devices	161
	Bringing Chassis Components Online and Offline on J Series Devices	162
Chapter 18	Operational Commands	165
	request system autorecovery state	166
	request system download abort	168
	request system download clear	169
	request system download pause	170
	request system download resume	171

request system download start	172
request system firmware upgrade	173
request system license update	174
request system partition compact-flash	175
request system power-off fpc	176
request system snapshot (Maintenance)	177
request system software abort in-service-upgrade (ICU)	180
request system software add (Maintenance)	181
request system reboot	182
request system software rollback (Maintenance)	183
show chassis usb storage	184
show system autorecovery state	185
show system auto-snapshot	187
show system download	189
show system license (View)	191
show system login lockout	194
show system snapshot media	195
show system storage (View SRX Series)	196
show system storage partitions (View SRX Series)	198
show version	199

Part 5

Index

Index	203
-------------	-----

List of Figures

Part 1	Overview	
Chapter 1	Product Overview	3
	Figure 1: J Series Services Routers (J4300 Shown)	7
Part 2	Installation	
Chapter 7	Software Installation and Upgrade	41
	Figure 2: Connecting to the Console Port on a Junos OS Device	49

List of Tables

	About the Documentation	xiii
	Table 1: Notice Icons	xv
	Table 2: Text and Syntax Conventions	xv
Part 1	Overview	
Chapter 1	Product Overview	3
	Table 3: Routing Engines and Storage Media Names (J Series Routers)	8
Chapter 2	Software Installation and Upgrade	9
	Table 4: show system download Output Fields	17
Chapter 3	Dual-Root Partitioning and Autorecovery	19
	Table 5: Storage Media on SRX Series Devices	20
	Table 6: Autorecovery Alarms	22
Chapter 4	BIOS Upgrade	25
	Table 7: CLI Commands for Manual BIOS Upgrade	26
Chapter 5	Autoinstallation	27
	Table 8: Interfaces and Protocols for IP Address Acquisition During Autoinstallation	28
Chapter 6	Licenses	33
	Table 9: Summary of License Management Fields	34
	Table 10: Junos OS Feature Licenses	36
Part 2	Installation	
Chapter 7	Software Installation and Upgrade	41
	Table 11: Secondary Storage Devices for SRX Series Devices	44
	Table 12: Secondary Storage Devices for Backup	45
	Table 13: Environment Variables Settings	61
	Table 14: Install Package Summary	64
	Table 15: Install Remote Summary	65
Part 3	Configuration	
Chapter 12	Backup and Snapshot Configuration Files	91
	Table 16: CLI set system dump-device Command Options	91
Part 4	Administration	
Chapter 18	Operational Commands	165

Table 17: show system autorecovery state Output Fields	185
Table 18: show system auto-snapshot Output Fields	187
Table 19: show system download Output Fields	189
Table 20: show system license Output Fields	191
Table 21: show system login lockout	194
Table 22: show system storage Output Fields	196

About the Documentation

- Documentation and Release Notes on page xiii
- Supported Platforms on page xiii
- Using the Examples in This Manual on page xiii
- Documentation Conventions on page xv
- Documentation Feedback on page xvii
- Requesting Technical Support on page xvii

Documentation and Release Notes

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

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

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

Supported Platforms

For the features described in this document, the following platforms are supported:

- [SRX Series](#)

Using the Examples in This Manual

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

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

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

Merging a Full Example

To merge a full example, follow these steps:

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

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

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

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

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

Merging a Snippet

To merge a snippet, follow these steps:

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

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

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

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

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

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

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

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

Documentation Conventions

Table 1 on page xv defines notice icons used in this guide.

Table 1: Notice Icons






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

Table 2 on page xv defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none">Introduces or emphasizes important new terms.Identifies guide names.Identifies RFC and Internet draft titles.	<ul style="list-style-type: none">A policy <i>term</i> is a named structure that defines match conditions and actions.<i>Junos OS CLI User Guide</i>RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none">To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level.The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric metric>;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (string1 string2 string3)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop address; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	}
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none">In the Logical Interfaces box, select All Interfaces.To cancel the configuration, click Cancel.

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

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

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at <http://www.juniper.net/techpubs/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <http://www.juniper.net/techpubs/feedback/>.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>

- Download the latest versions of software and review release notes:
<http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications:
<http://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum:
<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

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

Opening a Case with JTAC

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

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

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

PART 1

Overview

- [Product Overview on page 3](#)
- [Software Installation and Upgrade on page 9](#)
- [Dual-Root Partitioning and Autorecovery on page 19](#)
- [BIOS Upgrade on page 25](#)
- [Autoinstallation on page 27](#)
- [Licenses on page 33](#)

CHAPTER 1

Product Overview

- [Junos OS Overview on page 3](#)
- [Junos OS Editions on page 4](#)
- [Installation Categories on the J Series Services Routers on page 5](#)
- [Software Naming Convention on page 5](#)
- [Junos OS Release Numbers on page 6](#)
- [Hardware Overview \(J Series Services Routers\) on page 7](#)

Junos OS Overview

Juniper Networks provides high-performance network devices that create a responsive and trusted environment for accelerating the deployment of services and applications over a single network. Junos OS is the foundation of these high-performance networks. Unlike other complex, monolithic software architectures, Junos OS incorporates key design and developmental differences to deliver increased network availability, operational efficiency, and flexibility. The key advantages to this approach are:

- [One Operating System on page 3](#)
- [One Software Release on page 3](#)
- [One Modular Software Architecture on page 4](#)

One Operating System

Unlike other network operating systems that share a common name but splinter into many different programs, Junos OS is a single, cohesive operating system that is shared across all network devices and product lines. This allows Juniper Networks engineers to develop software features once and share these features across all product lines simultaneously. Because features are common to a single source, they generally are implemented the same way for all product lines, thus reducing the training required to learn different tools and methods for each product. Because all Juniper Networks products use the same code base, interoperability between products is not an issue.

One Software Release

Each new version of Junos OS is released concurrently for all product lines following a preset quarterly schedule. Furthermore, each new version of software must include all

working features released in previous releases of the software, and must have no critical regression errors. This discipline ensures reliable operations for the entire release.

One Modular Software Architecture

Although individual modules of the Junos OS communicate through well-defined interfaces, each module runs in its own protected memory space, preventing one module from disrupting another. This separation enables the independent restart of each module as necessary. This is in contrast to monolithic operating systems where a malfunction in one module can ripple to other modules and cause a full system crash or restart. This modular architecture then provides for high performance, high availability, security, and device scalability not found in other operating systems.

The Junos OS is preinstalled on your Juniper Networks device when you receive it from the factory. Thus, when you first power on the device, all software starts automatically. You simply need to configure the software so that the device can participate in the network.

You can upgrade the device software as new features are added or software problems are fixed. You normally obtain new software by downloading the software installation packages from the Juniper Networks Support Web page onto your device or onto another system on your local network. You then install the software upgrade onto the device.

Juniper Networks routing platforms run only binaries supplied by Juniper Networks, and currently do not support third-party binaries. Each Junos OS image includes a digitally signed manifest of executables that are registered with the system only if the signature can be validated. Junos OS will not execute any binary without a registered signature. This feature protects the system against unauthorized software and activity that might compromise the integrity of your device.

- Related Documentation**
- [Junos OS Editions on page 4](#)
 - *Installation and Upgrade Guide for Security Devices*

Junos OS Editions

Junos OS is released in the following editions:

- Domestic—Junos OS for customers in the United States and Canada, and for all other customers with a valid encryption agreement. This edition includes high-encryption capabilities such as ipsec and ssh for data leaving the router or switch.
- Export—Junos OS for all other customers. This edition does not include any high-encryption capabilities for data leaving the router or switch.
- Junos-FIPS—Junos OS that provides advanced network security for customers who need software tools to configure a network of Juniper Networks routers and switches in a Federal Information Processing Standards (FIPS) 140-2 environment.

- Related Documentation**
- [Junos OS Overview on page 3](#)
 - [Installation Categories on the J Series Services Routers on page 5](#)

- *Installation and Upgrade Guide for Security Devices*

Installation Categories on the J Series Services Routers

The following installation categories are available with the J Series routers:

- Junos OS, domestic—**junos-jsr-<release>-domestic.tgz**

This software includes high-encryption capabilities for data leaving the router. Because of U.S. government export restrictions, this software can only be installed on systems within the United States and Canada. For all other customers, a valid encryption agreement is required to use this software edition. Furthermore, no router can be shipped out of the United States, or Canada without the domestic edition first being overwritten by the export edition. There are no current system-enforced restrictions when you install this software category.

- Junos OS, export—**junos-jsr-<release>-export.tgz**

This software does not include high-encryption capabilities. It can be installed on any system worldwide. There are no current system-enforced restrictions when you install this software category.

Related Documentation

- [Junos OS Editions on page 4](#)
- [Junos OS Release Numbers on page 6](#)
- [Software Naming Convention on page 5](#)
- *Installation and Upgrade Guide for Security Devices*

Software Naming Convention

All Junos OS conforms to the following naming convention:

package-release-edition-cfxxx-signed.comp

For example:

jinstall-9.2R1.8-domestic-signed.tgz

where:

- **package** is the name of the Junos OS package. For 64-bit Junos OS, the package name is **package64**.
- **cfxxx** designates the CompactFlash card size to use with the software. This value is optional.
- **signed** means that the software includes a digital signature for verification purposes. This value is not used with all software packages.

Related Documentation

- [Junos OS Editions on page 4](#)

- [Junos OS Release Numbers on page 6](#)
- *Installation and Upgrade Guide for Security Devices*

Junos OS Release Numbers

The Junos OS release number represents a particular revision of the software that runs on a Juniper Networks routing platform, for example, Junos OS Release 8.5, 9.1, or 9.2. Each Junos OS release has certain new features that complement the software processes that support Internet routing protocols, control the device's interfaces and the device chassis itself, and allow device system management. On the Juniper Networks Support Web page, you download Junos OS for a particular Junos OS release number.

The following example shows how the software release number is formatted:

m.nZb.s

For example:

9.2R1.8

Where:

- ***m*** is the major release number of the product
- ***n*** is the minor release number of the product
- ***Z*** is the type of software release. The following release types are used:
 - **R**—FRS/Maintenance release software
 - **B**—Beta release software
 - **I**—Internal release software: Private software release for verifying fixes
 - **S**—Service release software: Released to customers to solve a specific problem—this release will be maintained along with the life span of the underlying release
 - **X**—Special (eXception) release software: Releases that follow a numbering system that differs from the standard Junos OS release numbering.

Starting with Junos OS Release 12.1X44-D10, SRX Series devices follow a special naming convention for Junos OS releases. For more information, refer to the Knowledge Base article KB30092 at

<http://kb.juniper.net/InfoCenter/index?page=home>.

- ***b*** is the build number of the product
 - if **b=1**: Software is the FRS release
 - if **b>1**: Software is a maintenance release
- ***s*** is the spin number of the product

Related Documentation

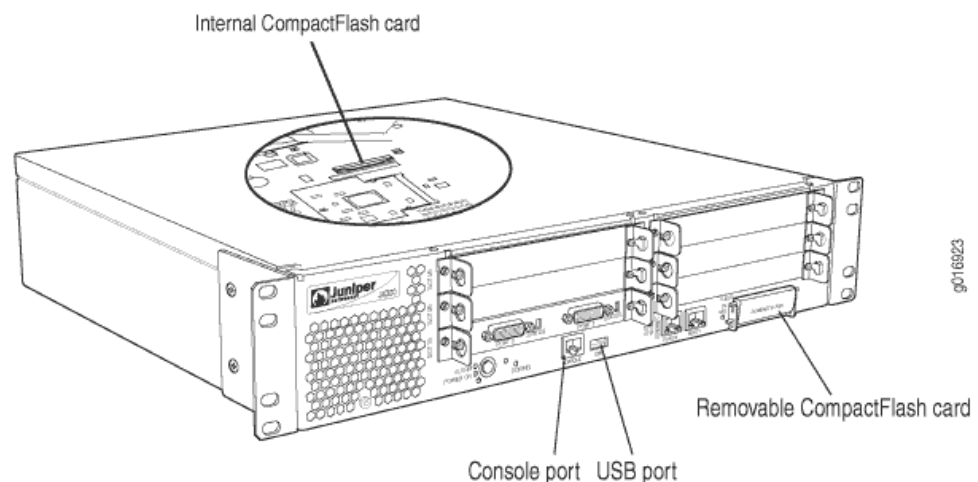
- [Junos OS Editions on page 4](#)

- [Software Naming Convention on page 5](#)
- [Installation and Upgrade Guide for Security Devices](#)

Hardware Overview (J Series Services Routers)

The Junos OS is installed on the internal CompactFlash card. This internal CompactFlash card is the primary and only boot drive on the J Series routers when they are delivered from the factory. All J Series routers have one or more USB ports. The 4300 and 6300 J Series routers also include an external CompactFlash card slot. You can install external storage devices through the USB ports and CompactFlash card slots. When external storage devices are installed, these external devices can be used as backup boot drives. You can also create a backup internal boot drive on any externally attached CompactFlash card. This CompactFlash card can then be used to replace the internal CompactFlash card on the J Series router in the event that the internal card is damaged or otherwise made unusable by the router. [Figure 1 on page 7](#) shows the location of the memory and ports on a J Series router.

Figure 1: J Series Services Routers (J4300 Shown)



The J Series routers include the following:

- [System Memory on page 7](#)
- [Storage Media on page 8](#)

System Memory

Starting with Junos OS Release 9.1, all J Series routers require a minimum of 512 MB of router memory on each Routing Engine. Any router without this minimum requires a system memory upgrade before you install Junos OS Release 9.1. To determine the amount of memory currently installed on your router, use the CLI **show chassis routing-engine** command.

For more information about memory requirements for the J Series routers, see the Customer Support Center JTAC Technical Bulletin PSN-2008-04-021:
<http://www.juniper.net/alerts/viewalert.jsp?txtAlertNumber=PSN-2008-04-021&actionBtn=Search>.

Storage Media

The J Series routers use the following media storage devices:

- Internal CompactFlash card—The CompactFlash card is the primary boot device.
- External media device—Depending on the system, this external device can be a CompactFlash card or a USB storage device. Juniper Networks recommends that you attach an external device to the system and use this external device as the backup boot device for the system.

Table 3 on page 8 specifies the storage media names used by the J Series routers. The storage media device names are displayed as the router boots.

Table 3: Routing Engines and Storage Media Names (J Series Routers)

Routing Engine	Internal CompactFlash Card	External CompactFlash Card J4300 and J6300 Routers Only	USB Storage Media Devices
J Series Routers	ad0	ad2	da0

To view the storage media currently available on your system, use the CLI **show system storage** command. For more information about this command, see the *CLI User Guide*.

The router attempts to boot from the storage media in the following order:

1. Internal CompactFlash card
2. External CompactFlash card (J4300 and J6300 routers only)
3. USB storage media device

Related Documentation

- [Junos OS Overview on page 3](#)
- *Installation and Upgrade Guide for Security Devices*

CHAPTER 2

Software Installation and Upgrade

- [Installation Type Overview on page 9](#)
- [Software Package Information Security on page 10](#)
- [Understanding Junos OS Upgrades for SRX Series Devices on page 10](#)
- [Understanding Junos OS Upgrades for J Series Devices on page 11](#)
- [Junos OS Upgrade Methods on the SRX Series Devices on page 12](#)
- [Understanding Junos OS Upgrade and Downgrade Procedures for on SRX Series Devices on page 13](#)
- [Understanding Junos OS Upgrade and Downgrade Procedures for J Series Devices on page 14](#)
- [Installation Modules on page 15](#)
- [Understanding Download Manager on page 16](#)

Installation Type Overview

The three types of installations used to upgrade or downgrade your routing platform are standard installation, category change, and recovery. The standard installation is the standard method of upgrading and downgrading the software. Use a category change installation when you are moving from one software category to another; for example, if you are changing the device from using the standard Junos OS to the Junos-FIPS category. Perform a recovery installation when the software on the device is damaged or otherwise unable to accommodate a software upgrade or downgrade.

Standard Installation

A standard installation is the typical method used to upgrade or downgrade software on the server. This method uses the installation package that matches the installation package already installed on the system. For example, you might upgrade an M120 router running the Junos OS installed using the **jinstall*** installation package. If you upgrade the router from the 9.0R2.10 release to the 9.1R1.8 release, you use the **jinstall-9.1R1.8-domestic-signed.tgz** installation package.

Category Change Installation

The category change installation process is used to move from one category of the Junos OS to another on the same router; for example, moving from a Junos OS standard

installation on an M Series, MX Series, or T Series router to a Junos-FIPS installation. When moving from one installation category to another, you need to be aware of the restrictions regarding this change.



NOTE: Juniper Networks does not support using the `request system software rollback` command to restore a different installation category on the device. When installing a different Junos OS category on a device, once the installation is complete, you should execute a `request system snapshot` command to delete the backup installation from the system.

Recovery Installation

A recovery installation is performed to repair a device with damaged software or a condition that prevents the upgrade, downgrade, or change in installation category of the software.

For example, you may need to perform a recovery installation to change a device's software category from Junos-FIPS to standard Junos OS.

Related Documentation

- [Installation and Upgrade Guide for Security Devices](#)

Software Package Information Security

All Junos OS is delivered in signed packages that contain digital signatures, Secure Hash Algorithm (SHA-1), and Message Digest 5 (MD5) checksums. A package is installed only if the checksum within it matches the hash recorded in its corresponding file. Which checksum is used depends on the software version:

- Digital signatures are used when you upgrade or downgrade between Junos OS Release 7.0 and a later version.
- The SHA-1 checksum is used when you upgrade or downgrade between Junos OS Release 6.4 and a later version.
- The MD5 checksum is used when you upgrade or downgrade between Junos OS Release 6.3 or earlier and a later version.

Related Documentation

- [Installation Type Overview on page 9](#)
- [Installation and Upgrade Guide for Security Devices](#)

Understanding Junos OS Upgrades for SRX Series Devices

SRX Series devices are delivered with Junos OS preinstalled on them. When you power on the device, it starts (boots) up using its primary boot device. These devices also support secondary boot devices, allowing you to back up your primary boot device and configuration.

As new features and software fixes become available, you must upgrade your software to use them. Before an upgrade, we recommend that you back up your primary boot device.

On a services gateway, you can configure the primary or secondary boot device with a snapshot of the current configuration, default factory configuration, or rescue configuration. You can also replicate the configuration for use on another device.

If the SRX Series device does not have a secondary boot device configured and the primary boot device becomes corrupted, you can reload the Junos OS package onto the corrupted internal media from a USB flash drive or TFTP server.

Related Documentation

- [Understanding Junos OS Upgrade and Downgrade Procedures for on SRX Series Devices on page 13](#)
- [Preparing Your SRX Series Device for Junos OS Upgrades on page 44](#)
- [Junos OS Upgrade Methods on the SRX Series Devices on page 12](#)
- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 55](#)
- [Installing Junos OS Using a USB Flash Drive on SRX Series Devices on page 62](#)
- [Installation and Upgrade Guide for Security Devices](#)

Understanding Junos OS Upgrades for J Series Devices

J Series devices are delivered with Junos OS preinstalled. When you power on the device, it starts (boots) up using its primary boot device. These devices also support secondary boot devices, allowing you to back up your primary boot device and configuration.

As new features and software fixes become available, you must upgrade Junos OS to use them. Before an upgrade, we recommend that you back up your primary boot device.

On a device, you can configure the primary or secondary boot device with a “snapshot” of the current configuration, default factory configuration, or rescue configuration. You can also replicate the configuration for use on another device, or configure a boot device to receive core dumps for troubleshooting.

If the J Series device does not have a secondary boot device configured and the primary boot device becomes corrupted, you can reload the Junos OS package onto the corrupted CompactFlash (CF) card with either a UNIX or Microsoft Windows computer.



NOTE: The terms *Junos OS (legacy services)* and *Junos OS* are used frequently in this section. Junos OS (legacy services) denotes the packet-based software for the J Series device, whereas Junos OS denotes the flow-based software for the J Series device.

Related Documentation

- [Understanding Junos OS Upgrade and Downgrade Procedures for J Series Devices on page 14](#)

- [Downloading Junos OS Upgrades for J Series Devices on page 53](#)
- [Example: Installing Junos OS Upgrades on J Series Devices on page 57](#)
- [Example: Downgrading Junos OS on J Series Devices on page 81](#)
- *Installation and Upgrade Guide for Security Devices*

Junos OS Upgrade Methods on the SRX Series Devices

SRX Series devices that ship from the factory with Junos OS Release 10.0 or later are formatted with the dual-root partitioning scheme.

Existing SRX Series devices that are running Junos OS Release 9.6 or earlier use the single-root partitioning scheme. While upgrading these devices to Junos OS Release 10.0 or later, you can choose to format the storage media with dual-root partitioning (strongly recommended) or retain the existing single-root partitioning.

Certain Junos OS upgrade methods format the internal media before installation, whereas other methods do not. To install Junos OS Release 10.0 or later with the dual-root partitioning scheme, you must use an upgrade method that formats the internal media before installation.



NOTE: If you are upgrading to Junos OS Release 10.0 without transitioning to dual-root partitioning, use the conventional CLI and J-Web user interface installation methods.

These upgrade methods format the internal media before installation:

- Installation from the boot loader using a TFTP server
- Installation from the boot loader using a USB storage device
- Installation from the CLI using the **partition** option (available in Junos OS Release 10.0)
- Installation using the J-Web user interface

These upgrade methods retain the existing partitioning scheme:

- Installation using the CLI
- Installation using the J-Web user interface



WARNING: Upgrade methods that format the internal media before installation wipe out the existing contents of the media. Only the current configuration will be preserved. Any important data should be backed up before starting the process.



NOTE: Once the media has been formatted with the dual-root partitioning scheme, you can use conventional CLI or J-Web user interface installation methods, which retain the existing partitioning and contents of the media, for subsequent upgrades.

Related Documentation

- [Installing Junos OS Upgrades from a Remote Server on the SRX Series Devices on page 63](#)
- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 55](#)
- [Example: Downgrading Junos OS on SRX Series Devices on page 79](#)
- [Installing Junos OS Using a USB Flash Drive on SRX Series Devices on page 62](#)
- *Installation and Upgrade Guide for Security Devices*

Understanding Junos OS Upgrade and Downgrade Procedures for on SRX Series Devices

Typically, you upgrade your device software by downloading a software image to your device from another system on your local network. Using the J-Web user interface or the CLI to upgrade, the device downloads the software image, decompresses the image, and installs the decompressed software. Finally, you reboot the device, at which time it boots from the upgraded software. Junos OS is delivered in signed packages that contain digital signatures to ensure official Juniper Networks software.

An upgrade software package name is in the following format:

package-name-m.nZx-distribution.tgz

- **package-name**—Name of the package; for example, junos-srxsme.
- **m.n**—Junos OS release, with m representing the major release number and n representing the minor release number; for example, 10.0.
- **Z**—Type of Junos OS release; for example, R indicates released software, and B indicates beta-level software.
- **x.y**—Junos OS build number and spin number; for example, 1.8.
- **distribution**—Area for which the Junos OS package is provided. It is domestic for the United States and Canada, and it is export for worldwide distribution.

The following package name is an example of an SRX Series device upgrade Junos OS package:

junos-srxsme-10.0R1.8-domestic-tgz

Related Documentation

- [Understanding Junos OS Upgrades for SRX Series Devices on page 10](#)
- [Preparing Your SRX Series Device for Junos OS Upgrades on page 44](#)
- [Junos OS Upgrade Methods on the SRX Series Devices on page 12](#)

- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 55](#)
- [Example: Downgrading Junos OS on SRX Series Devices on page 79](#)
- [Installing Junos OS Using a USB Flash Drive on SRX Series Devices on page 62](#)
- *Installation and Upgrade Guide for Security Devices*

Understanding Junos OS Upgrade and Downgrade Procedures for J Series Devices

Typically, you upgrade Junos OS by downloading a Junos OS image to your device from another system on your local network. Using the J-Web user interface or the CLI to upgrade, the device downloads the Junos OS image, decompresses the image, and installs the decompressed Junos OS. Finally, you reboot the device, at which time it boots from the upgraded Junos OS. Junos OS is delivered in signed packages that contain digital signatures to ensure official Juniper Networks software.

- [Junos OS Upgrade Packages on page 14](#)
- [Junos OS Recovery Packages on page 14](#)

Junos OS Upgrade Packages

A Junos OS upgrade package name is in the following format:

package-name-m.nZx-distribution.tgz.

- **package-name**—Name of the package; for example, junos-jsr.
- **m.n**—Junos OS release, with m representing the major release number and n representing the minor release number; for example, 8.5.
- **Z**—Type of Junos OS release. For example, R indicates released software, and B indicates beta-level software.
- **x.y**—Junos OS build number and spin number; for example, 1.1.
- **distribution**—Area for which the Junos OS package is provided. It is domestic for the United States and Canada, and it is export for worldwide distribution.

The following example is of a Junos OS upgrade package name:

junos-jsr-8.5R1.1-domestic.tgz.

Junos OS Recovery Packages

Download a Junos OS recovery package, also known as an install media package, to recover a primary CompactFlash (CF) card.

A Junos OS recovery package name is in the following format:

package-name-m.nZx-export-cfnnn.gz.

- **package-name**—Name of the package; for example, junos-jsr.
- **m.n** —Junos OS release, with m representing the major release number; for example, 8.5.
- **Z**—Type of Junos OS release. For example, R indicates released software, and B indicates beta-level software
- **x.y**—Junos OS build number and spin number; for example, 1.1.
- **export**—Export indicates that the Junos OS recovery package is the exported worldwide software package version.
- **cfnnn**—Size of the target CF card in megabytes; for example, cf256. The following CF card sizes are supported:
 - 512 MB
 - 1024 MB



NOTE: The CF cards with less than 512 MB of storage capacity are not supported

The following example is of a Junos OS recovery package name:

junos-jsr-8.5R1.1-export-cf256.gz

Related Documentation

- [Preparing Your J Series Services Router for Junos OS Upgrades on page 45](#)
- [Downloading Junos OS Upgrades for J Series Devices on page 53](#)
- [Example: Installing Junos OS Upgrades on J Series Devices on page 57](#)
- [Example: Downgrading Junos OS on J Series Devices on page 81](#)
- [Installation and Upgrade Guide for Security Devices](#)

Installation Modules

Installation modules are used to upgrade individual software modules within the software. For example, you can upgrade only the Routing Engine software by installing the **jroute*** installation module.



NOTE: You should only use installation module files under the direction of a Juniper Networks support representative.

The following installation module files are available for download:

Installation Module	Description
---------------------	-------------

jkernel*	The kernel and network tools package. This package contains the basic operating system files.
jbase*	The base package for the Junos OS. This package contains additions to the operating system.
jroute*	The Routing Engine package. This package contains the Routing Engine software.
jpfe*	The Packet Forwarding Engine package. This package contains the PFE software.
jdocs*	The documentation package. This package contains the documentation set for the software.
jcrypto*	The encryption package. This package contains the domestic version of the security software.
jweb*	The J-Web package. This package contains the graphical user interface software for M Series, MX Series, T Series, TX Matrix, TX Matrix Plus, and J Series routers.

- Related Documentation**
- [Installation Type Overview on page 9](#)
 - *Installation and Upgrade Guide for Security Devices*

Understanding Download Manager

This topic includes the following sections:

- [Overview on page 16](#)
- [Using Download Manager to Upgrade Junos OS on page 17](#)
- [Handling Errors on page 17](#)
- [Considerations on page 18](#)

Overview

This download manager feature facilitates download of large files over low-bandwidth links. It enables you to download large Junos OS packages over low-bandwidth/flaky links so that the system can be upgraded. This feature allows you to download multiple files while monitoring their status and progress individually. It takes automatic action when required and displays status information when requested.

This feature is supported on SRX100, SRX210, SRX220, SRX240, and SRX650 Services Gateways.

This feature provides the following functions:

- Bandwidth-limited downloads
- Scheduled downloads
- Automatic resume on error
- Automatic resume on reboot



NOTE: This feature supports only the FTP and HTTP protocols.

Using Download Manager to Upgrade Junos OS

The download manager acts as a substitute for the FTP utility. You can use the download manager CLI commands for all the functions where you previously used the FTP utility.

The download manager requires the following:

- FTP or HTTP server with a Junos OS image
- Server that is reachable from the device being upgraded

The download manager consists of the following CLI commands:

1. To download the Junos OS image to your device, use the **request system download start** command (set a bandwidth limit, if required). The file is saved to the **/var/tmp** directory on your device.

You can continue to use the device while the download runs in the background.

2. Use the **show system download** command to verify that the file has been downloaded. The command displays the state as "completed" when the downloaded file is ready to be installed.
3. Use the **request system software add** command to install the downloaded image file from the **/var/tmp** directory.

Handling Errors

If you encounter any problem with a download, use the **show system download id** command to obtain details about the download.

[Table 4 on page 17](#) lists the output fields for the **show system download** command. Use this information to diagnose problems. Output fields are listed in the approximate order in which they appear.

Table 4: show system download Output Fields

Output Field	Description
Status	State of the download.

Table 4: show system download Output Fields (*continued*)

Output Field	Description
Creation Time	Time the start command was issued.
Scheduled Time	Time the download was scheduled to start.
Start Time	Time the download actually started (if it has already started).
Retry Time	Time for next retry (if the download is in the error state).
Error Count	Number of times an error was encountered by this download.
Retries Left	Number of times the system will retry the download automatically before stopping.
Most Recent Error	Message indicating the cause of the most recent error.

Considerations

- When no download limit is specified for a specific download or for all downloads, a download uses all available network bandwidth.
- Because the download limit that you set indicates an average bandwidth limit, it is possible that certain bursts might exceed the specified limit.
- When a download from an HTTP server fails, the server returns an HTML page. Occasionally, the error page is not recognized as an error page and is downloaded in place of the Junos image file.
- Remote server logins and passwords are stored by the download manager for the duration of a download. To encrypt these credentials provided along with the login keyword, define an encryption key with the **request system set-encryption-key** command. Any changes to encryption settings while download is in progress can cause the download to fail.
- A download command issued on a particular node in a chassis cluster takes place only on that node and is not propagated to the other nodes in the cluster. Downloads on different nodes are completely independent of each other. In the event of a failover, a download continues only if the server remains reachable from the node from which the command was issued. If the server is no longer reachable on that node, the download stops and returns an error.

Related Documentation

- [Installation Type Overview on page 9](#)
- *Installation and Upgrade Guide for Security Devices*

CHAPTER 3

Dual-Root Partitioning and Autorecovery

- [Dual-Root Partitioning Scheme Overview on page 19](#)
- [Understanding Integrity Check and Autorecovery of Configuration, Licenses, and Disk Information on page 21](#)

Dual-Root Partitioning Scheme Overview

Junos OS Release 10.0 and later support dual-root partitioning on SRX Series devices. Dual-root partitioning allows the SRX Series device to remain functional even if there is file system corruption and to facilitate easy recovery of the file system.



NOTE: Junos OS Release 12.1X45 and later do not support single root partitioning.

SRX Series devices running Junos OS Release 9.6 or earlier support a single-root partitioning scheme where there is only one root partition. Because both the primary and backup Junos OS images are located on the same root partition, the system fails to boot if there is corruption in the root file system. The dual-root partitioning scheme guards against this scenario by keeping the primary and backup Junos OS images in two independently bootable root partitions. If the primary root partition becomes corrupted, the system can still boot from the backup Junos OS image located in the other root partition and remain fully functional.

SRX Series devices that ship with Junos OS Release 10.0 or later are formatted with dual-root partitions from the factory. SRX Series devices that are running Junos OS Release 9.6 or earlier can be formatted with dual-root partitions when they are upgraded to Junos OS Release 10.0 or later.



NOTE: Although you can install Junos OS Release 10.0 or later on SRX Series devices with the single-root partitioning scheme, we strongly recommend the use of the dual-root partitioning scheme.

This section contains the following topics:

- [Boot Media and Boot Partition on the SRX Series Devices on page 20](#)
- [Important Features of the Dual-Root Partitioning Scheme on page 20](#)

Boot Media and Boot Partition on the SRX Series Devices

When the SRX Series device powers on, it tries to boot the Junos OS from the default storage media. If the device fails to boot from the default storage media, it tries to boot from the alternate storage media.

[Table 5 on page 20](#) provides information on the storage media available on SRX Series devices.

Table 5: Storage Media on SRX Series Devices

SRX Series Devices	Storage Media
SRX100, SRX210, and SRX240	<ul style="list-style-type: none"> • Internal NAND flash (default; always present) • USB storage device (alternate)
SRX650	<ul style="list-style-type: none"> • Internal CF (default; always present) • External flash card (alternate) • USB storage device (alternate)

With the dual-root partitioning scheme, the SRX Series device first tries to boot the Junos OS from the primary root partition and then from the backup root partition on the default storage media. If both primary and backup root partitions of a media fail to boot, then the SRX Series device tries to boot from the next available type of storage media. The SRX Series device remains fully functional even if it boots the Junos OS from the backup root partition of the storage media.

Important Features of the Dual-Root Partitioning Scheme

The dual-root partitioning scheme has the following important features:

- The primary and backup copies of Junos OS images reside in separate partitions. The partition containing the backup copy is mounted only when required. With the single-root partitioning scheme, there is one root partition that contains both the primary and the backup Junos OS images.
- The **request system software add** command for a Junos OS package erases the contents of the other root partition. The contents of the other root partition will not be valid unless software installation is completed successfully.
- Add-on packages, such as **jais** or **jfirmware**, can be reinstalled as required after a new Junos OS image is installed.
- The **request system software rollback** command does not delete the current Junos OS image. It is possible to switch back to the image by issuing the **rollback** command again.
- The **request system software delete-backup** and **request system software validate** commands do not take any action.

- Related Documentation**
- [Understanding Junos OS Upgrades for SRX Series Devices on page 10](#)
 - [Junos OS Release 10.0 or Later Upgrades with Dual-Root Partitioning on SRX Series Devices on page 72](#)
 - [Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 72](#)
 - [Junos OS Release 9.6 or Earlier Installation on SRX Series Devices with Dual-Root Partitioning on page 71](#)
 - [Understanding How the Primary Junos OS Image with Dual-Root Partitioning Recovers on SRX Series Devices on page 69](#)
 - *Installation and Upgrade Guide for Security Devices*

Understanding Integrity Check and Autorecovery of Configuration, Licenses, and Disk Information

- [Overview on page 21](#)
- [How Autorecovery Works on page 21](#)
- [How to Use Autorecovery on page 22](#)
- [Data That Is Backed Up in an Autorecovery on page 22](#)
- [Troubleshooting Alarms on page 22](#)
- [Considerations on page 23](#)

Overview

The autorecovery feature is supported on dual-partitioned SRX100, SRX210, SRX220, SRX240, and SRX650 Services Gateways. With this feature, information on disk partitioning, configuration, and licenses is recovered automatically in the event it becomes corrupted.

Autorecovery provides the following functions:

- Detect corruption in disk partitioning during system bootup and attempt to recover partitions automatically
- Detect corruption in the Junos OS rescue configuration during system bootup and attempt to recover the rescue configuration automatically
- Detect corruption in Junos OS licenses during system bootup and attempt to recover licenses automatically

How Autorecovery Works

The feature works in the following ways:

- The feature provides the **request system autorecovery state save** command, which backs up important data such as disk partitioning information, licenses, and Junos OS rescue configuration.

- Once the backup copies are saved, they are used to check the integrity of the working copies of the data on every bootup.
- The working copies are automatically recovered if any corruption is detected.

How to Use Autorecovery

You use autorecovery in the following ways:

- Prepare the router for deployment with the necessary licenses and configuration.
- After you finalize the state, execute the **request system autorecovery state save** command to back up the state.
- After you save the state, integrity check and recovery actions (if any) occur automatically on every bootup.
- If subsequent maintenance activities change the state of the router by adding licenses or updating the configuration, you need to execute the **request system autorecovery state save** command again to update the saved state.
- Execute the **show system autorecovery state** command any time to view the status of the saved information and the integrity check status of each saved item.
- Execute the **request system autorecovery state clear** command to delete all backed up data and disable autorecovery, if required.

Data That Is Backed Up in an Autorecovery

The following data is backed up during the autorecovery process:

- Rescue configuration (regenerated from the current configuration)
- License keys
- BSD labels (disk-partitioning information)

Data is backed up only when you execute the **request system autorecovery state save** command. Disk-partitioning information is backed up automatically from factory defaults (for new systems), on installation from the boot loader, and on snapshot creation.

Troubleshooting Alarms

Table 6 on page 22 lists types of autorecovery alarms, descriptions, and required actions.

Table 6: Autorecovery Alarms

Alarm	Alarm Type	Description	Action Required
Autorecovery information needs to be saved	Minor	<p>This alarm indicates:</p> <ul style="list-style-type: none"> • Unsaved data needs to be saved, or saved data contains problems and another save is required. 	<ul style="list-style-type: none"> • Ensure that the system has all required licenses and configuration. • Execute the request system autorecovery state save command.

Table 6: Autorecovery Alarms (*continued*)

Alarm	Alarm Type	Description	Action Required
Autorecovery has recovered corrupted information	Minor	This alarm indicates: <ul style="list-style-type: none"> • Boot time integrity check failed for certain items; however, the items have been recovered successfully. 	<ul style="list-style-type: none"> • No action is required. • Alarm will be cleared on next bootup.
Autorecovery was unable to recover data completely	Major	This alarm indicates: <ul style="list-style-type: none"> • Boot time integrity check failed for certain items, which could not be recovered successfully. 	<ul style="list-style-type: none"> • The system might be experiencing a fatal malfunction.

Considerations

- Devices must have dual-root partitioning for autorecovery to work.
- The **request system configuration rescue save** command regenerates the rescue configuration from the current Junos OS configuration and then saves it. Therefore, executing the **save** command overwrites any existing rescue configuration.
- In general, the saved contents of the rescue configuration are not updated automatically. If you add licenses, you should execute the **request system autorecovery state save** command again.



NOTE: The rescue configuration is backed up. If `/config` is corrupted, the system boots from the rescue configuration.

Related Documentation

- *Installation and Upgrade Guide for Security Devices*

CHAPTER 4

BIOS Upgrade

- [Understanding Auto BIOS Upgrade Using Junos CLI on page 25](#)
- [Understanding Manual BIOS Upgrade Using Junos CLI on page 25](#)

Understanding Auto BIOS Upgrade Using Junos CLI

The BIOS version listed in the **bios-autoupgrade.conf** file is the minimum supported version. If the current device has a BIOS version earlier than the minimum compatible version, then the auto BIOS upgrade feature upgrades the BIOS automatically to the latest version.

The BIOS upgrades automatically in the following scenarios:

- During Junos OS upgrade through either the J-Web user interface or the CLI (using the **request system software add no-copy no-validate software-image**). In this case, only the active BIOS is upgraded.
- During loader installation using TFTP or USB (using the **install tftp:///software-image** command). In this case, only the active BIOS is upgraded.
- During system boot-up. In this case, both the active BIOS and the backup BIOS are upgraded.

Related Documentation

- [Understanding Junos OS Upgrades for SRX Series Devices on page 10](#)
- [Understanding Manual BIOS Upgrade Using Junos CLI on page 25](#)
- [Disabling Auto BIOS Upgrade on SRX Series Devices on page 141](#)
- *Installation and Upgrade Guide for Security Devices*

Understanding Manual BIOS Upgrade Using Junos CLI

For SRX Series appliances, the BIOS consists of a U-boot and the Junos loader. Additionally, a backup BIOS is supported which includes a backup copy of the U-boot in addition to the active copy from which the system generally boots up.

[Table 7 on page 26](#) lists the CLI commands used for manual BIOS upgrade.

Table 7: CLI Commands for Manual BIOS Upgrade

Active BIOS	Backup BIOS
<code>request system firmware upgrade re bios</code>	<code>request system firmware upgrade re bios backup</code>

BIOS upgrade procedure:

1. **Install the jloader-srxsme package.**

1. Copy the jloader-srxsme signed package to the device.



NOTE: The version of the jloader-srxsme package you install must match the version of Junos OS.

2. Install the package using the `request system software add <path to jloader-srxsme package> no-copy no-validate` command.



NOTE: Installing the jloader-srxsme package places the necessary images under `directory/boot`.

2. Verify that the required images for upgrade are installed. Use the `show system firmware` to verify that the correct BIOS image version is available for upgrade.
3. Upgrade the BIOS (Active and backup) image.

Active BIOS:

1. Initiate the upgrade using the `request system firmware upgrade re bios` command.
2. Monitor the upgrade status using the `show system firmware` command.



NOTE: The device must be rebooted for the upgraded active BIOS to take effect.

Backup BIOS:

1. Initiate the upgrade using the `request system firmware upgrade re bios backup` command.
2. Monitor the upgrade status using the `show system firmware` command.

Related Documentation

- [Understanding Junos OS Upgrades for SRX Series Devices on page 10](#)
- [Understanding Auto BIOS Upgrade Using Junos CLI on page 25](#)
- [Disabling Auto BIOS Upgrade on SRX Series Devices on page 141](#)
- *Installation and Upgrade Guide for Security Devices*

CHAPTER 5

Autoinstallation

- [Autoinstallation Overview on page 27](#)
- [Automatic Installation of Configuration Files \(J Series Services Routers and SRX Series Services Gateways\) on page 30](#)

Autoinstallation Overview

If you are setting up many devices, autoinstallation can help automate the configuration process by loading configuration files onto new or existing devices automatically over the network. You can use either the J-Web configuration editor or the CLI configuration editor to configure a device for autoinstallation.

Autoinstallation provides automatic configuration for a new device that you connect to the network and turn on, or for a device configured for autoinstallation. The autoinstallation process begins anytime a device is powered on and cannot locate a valid configuration file in the CompactFlash (CF) card. Typically, a configuration file is unavailable when a device is powered on for the first time, or if the configuration file is deleted from the CF card. The autoinstallation feature enables you to deploy multiple devices from a central location in the network.

For the autoinstallation process to work, you must store one or more host-specific or default configuration files on a configuration server in the network and have a service available—typically Dynamic Host Configuration Protocol (DHCP)—to assign an IP address to the device.

Autoinstallation takes place automatically when you connect an Ethernet or serial port on a new Juniper Networks device to the network and power on the device. To simplify the process, you can explicitly enable autoinstallation on a device and specify a configuration server, an autoinstallation interface, and a protocol for IP address acquisition.

This section contains the following topics:

- [Automatic Installation of Configuration Files on page 28](#)
- [Supported Autoinstallation Interfaces and Protocols on page 28](#)
- [Typical Autoinstallation Process on a New Device on page 29](#)

Automatic Installation of Configuration Files

On SRX Series devices, you can specify a remote server where configuration files are located. If a configuration file cannot be found on the device's CompactFlash card, the device automatically retrieves the configuration file from this remote server. For security purposes, you can encrypt these remote files using the DES cipher, and once they have been retrieved, the device decrypts them for use on the server.

To encrypt the files, we recommend the openssl tool. You can get the open SSL tool at: <http://www.openssl.org/>. To encrypt the file, use the following syntax:

```
% openssl enc -des -k passphrase -in original-file -out encrypted-file
```

- ***passphrase***—Passphrase used to encrypt the configuration file. The passphrase should be the name of the file without the path information or file extension.
- ***original-file***—Unencrypted configuration file.
- ***encrypted-file***—Name of the encrypted configuration file.

For example, if you are encrypting the active configuration file **juniper.conf.gz**, the passphrase is **juniper.conf**. The openssl syntax used to encrypt the file is:

```
% openssl enc -des -k juniper.conf -in juniper.conf.gz -out juniper.conf.gz.enc
```

Supported Autoinstallation Interfaces and Protocols

Before autoinstallation on a device can take place, the device must acquire an IP address. The protocol or protocols you choose for IP address acquisition determine the device interface to connect to the network for autoinstallation. The device detects the connected interface and requests an IP address with a protocol appropriate for the interface. Autoinstallation is supported over an Ethernet LAN interface or a serial LAN or WAN interface. [Table 8 on page 28](#) lists the protocols that the device can use on these interfaces for IP address acquisition.

Table 8: Interfaces and Protocols for IP Address Acquisition During Autoinstallation

Interface and Encapsulation Type	Protocol for Autoinstallation
Ethernet LAN interface with High-Level Data Link Control (HDLC)	DHCP, BOOTP, or Reverse Address Resolution Protocol (RARP)
Serial WAN interface with HDLC	Serial Line Address Resolution Protocol (SLARP)
Serial WAN interface with Frame Relay	BOOTP

If the server with the autoinstallation configuration file is not on the same LAN segment as the new device, or if a specific device is required by the network, you must configure an intermediate device directly attached to the new device through which the new device can send Trivial File Transfer Protocol (TFTP), BOOTP, and Domain Name System (DNS) requests. In this case, you specify the IP address of the intermediate device as the location to receive TFTP requests for autoinstallation.

Typical Autoinstallation Process on a New Device

When a device is powered on for the first time, it performs the following autoinstallation tasks:

1. The new device sends out DHCP, BOOTP, RARP, or SLARP requests on each connected interface simultaneously to obtain an IP address.

If a DHCP server responds, it provides the device with some or all of the following information:

- An IP address and subnet mask for the autoinstallation interface.
- The location of the TFTP (typically), Hypertext Transfer Protocol (HTTP), or FTP server on which the configuration file is stored.
- The name of the configuration file to be requested from the TFTP server.
- The IP address or hostname of the TFTP server.

If the DHCP server provides only the hostname, a DNS server must be available on the network to resolve the name to an IP address.

- The IP address of an intermediate device if the configuration server is on a different LAN segment from the new device.
2. After the new device acquires an IP address, the autoinstallation process on the device attempts to download a configuration file in the following ways:
 - a. If the DHCP server specifies the host-specific configuration file (boot file) **hostname.conf**, the device uses that filename in the TFTP server request. (In the filename, **hostname** is the hostname of the new device.) The autoinstallation process on the new device makes three unicast TFTP requests for **hostname.conf**. If these attempts fail, the device broadcasts three requests to any available TFTP server for the file.
 - b. If the new device cannot locate **hostname.conf**, the autoinstallation process unicasts or broadcasts TFTP requests for a default device configuration file called **network.conf**, which contains hostname-to-IP address mapping information, to attempt to find its hostname.
 - c. If **network.conf** contains no hostname entry for the new device, the autoinstallation process sends out a DNS request and attempts to resolve the new device's IP address to a hostname.
 - d. If the new device can determine its hostname, it sends a TFTP request for the **hostname.conf** file.
 - e. If the new device is unable to map its IP address to a hostname, it sends TFTP requests for the default configuration file **router.conf**.
 3. After the new device locates a configuration file on a TFTP server, autoinstallation downloads the file, installs the file on the device, and commits the configuration.



NOTE:

- If you configure the DHCP server to provide only the TFTP server hostname, add an IP address-to-hostname mapping entry for the TFTP server to the DNS database file on the DNS server in the network.
 - If the new device is not on the same network segment as the DHCP server (or other device providing IP address resolution), configure an existing device as an intermediate to receive TFTP and DNS requests and forward them to the TFTP server and the DNS server. You must configure the LAN or serial interface on the intermediate device with the IP addresses of the hosts providing TFTP and DNS service. Connect this interface to the new device.
-

Related Documentation

- *Automatic Installation of Configuration Files (J Series Routers and SRX Services Gateway)*
- [Example: Configuring Autoinstallation on page 87](#)
- *Installation and Upgrade Guide for Security Devices*

Automatic Installation of Configuration Files (J Series Services Routers and SRX Series Services Gateways)

Autoinstallation provides automatic configuration for a new device that you connect to the network and turn on, or for a device configured for autoinstallation.

J Series Automatic Installation Overview

On J Series routers, you can specify a remote server where configuration files are located. If a configuration file cannot be found on the router's CompactFlash card, the router automatically retrieves the configuration file from this remote server. For security purposes, you can encrypt these remote files using the DES cipher, and once they have been retrieved, the router decrypts them for use on the server.

To encrypt the files, we recommend the openssl tool. You can get the open SSL tool at: <http://www.openssl.org/>. To encrypt the file, use the following syntax:

```
% openssl enc -des -k passphrase -in original-file -out encrypted-file
```

- ***passphrase***—Passphrase used to encrypt the configuration file. The passphrase should be the name of the file without the path information or file extension.
- ***original-file***—Unencrypted configuration file.
- ***encrypted-file***—Name of the encrypted configuration file.

For example, if you are encrypting the active configuration file **juniper.conf.gz**, the passphrase is **juniper.conf**. The openssl syntax used to encrypt the file is:

```
% openssl enc -des -k juniper.conf -in juniper.conf.gz -out juniper.conf.gz.enc
```


SRX Series Services Gateways Automatic Installation Overview

The autoinstallation process begins any time a services gateway is powered on and cannot locate a valid configuration file in the internal flash. Typically, a configuration file is unavailable when a services gateway is powered on for the first time or if the configuration file is deleted from the internal flash. The autoinstallation feature enables you to deploy multiple services gateways from a central location in the network.

If you are setting up many devices, autoinstallation can help automate the configuration process by loading configuration files onto new or existing devices automatically over the network. You can use either the J-Web configuration editor or the CLI configuration editor to configure a device for autoinstallation.

For the autoinstallation process to work, you must store one or more host-specific or default configuration files on a configuration server in the network and have a service available—typically Dynamic Host Configuration Protocol (DHCP)—to assign an IP address to the services gateway.

Autoinstallation takes place automatically when you connect an Ethernet port on a new services gateway to the network and power on the device. To simplify the process, you can explicitly enable autoinstallation on a device and specify a configuration server, an autoinstallation interface, and a protocol for IP address acquisition.

Related Documentation

- [Autoinstallation Overview on page 27](#)
- [Example: Configuring Autoinstallation on page 87](#)
- *Installation and Upgrade Guide for Security Devices*

CHAPTER 6

Licenses

- [Junos OS License Overview on page 33](#)
- [License Enforcement on page 35](#)
- [Junos OS Feature License Model Number for J Series Services Routers and SRX Series Services Gateways on page 36](#)

Junos OS License Overview

To enable some Junos OS features, you must purchase, install, and manage separate software licenses. For those features that require a license, the presence on the device of the appropriate software license keys (passwords) determines whether you can use the feature.

For information about how to purchase software licenses for your device, contact your Juniper Networks sales representative.

Certain Junos OS features require licenses. Each license is valid for only a single device. To manage the licenses, you must understand license enforcement and the components of a license key.

This section contains the following topics:

- [License Enforcement on page 33](#)
- [License Key Components on page 34](#)
- [License Management Fields Summary on page 34](#)

License Enforcement

For features that require a license, you must install and properly configure the license to use the feature. Although the device allows you to commit a configuration that specifies a feature requiring a license when the license is not present, you are prohibited from actually using the feature.

Successful commitment of a configuration does not imply that the required licenses are installed. If a required license is not present, the system provides a warning message after it commits the configuration rather than failing to commit it because of a license violation.

License Key Components

A license key consists of two parts:

- **License ID**—Alphanumeric string that uniquely identifies the license key. When a license is generated, it is given a license ID.
- **License data**—Block of binary data that defines and stores all license key objects.

For example, in the following typical license key, the string **XXXXXXXXXX** is the license ID, and the trailing block of data is the license data:

```
XXXXXXXXXX xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
          xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
          xxxxxx xxxxxx xxx
```

The license data defines the device ID for which the license is valid and the version of the license.

License Management Fields Summary

The Licenses page displays a summary of licensed features that are configured on the device and a list of licenses that are installed on the device. The information on the license management page is summarized in [Table 9 on page 34](#).

Table 9: Summary of License Management Fields

Field Name	Definition
Feature Summary	
Feature	Name of the licensed feature: <ul style="list-style-type: none"> • Features—Software feature licenses. • All features—All-inclusive licenses
Licenses Used	Number of licenses currently being used on the device. Usage is determined by the configuration on the device. If a feature license exists and that feature is configured, the license is considered used.
Licenses Installed	Number of licenses installed on the device for the particular feature.
Licenses Needed	Number of licenses required for legal use of the feature. Usage is determined by the configuration on the device: If a feature is configured and the license for that feature is not installed, a single license is needed.
Installed Licenses	
ID	Unique alphanumeric ID of the license.
State	Valid —The installed license key is valid. Invalid —The installed license key is not valid.
Version	Numeric version number of the license key.

Table 9: Summary of License Management Fields (*continued*)

Field Name	Definition
Group	<p>If the license defines a group license, this field displays the group definition.</p> <p>If the license requires a group license, this field displays the required group definition.</p> <p>NOTE: Because group licenses are currently unsupported, this field is always blank.</p>
Enabled Features	Name of the feature that is enabled with the particular license.
Expiry	<p>Verify that the expiration information for the license is correct.</p> <p>For Junos OS, only permanent licenses are supported. If a license has expired, it is shown as invalid.</p>

- Related Documentation**
- [Junos OS Feature License Model Number for J Series Services Routers and SRX Series Services Gateways on page 36](#)
 - [Generating a License Key on page 144](#)
 - [Updating License Keys on page 146](#)
 - [Saving License Keys on page 145](#)
 - [Downloading License Keys on page 144](#)
 - *Installation and Upgrade Guide for Security Devices*
 - *Administration Guide for Security Devices*

License Enforcement

For features or scaling levels that require a license, you must install and properly configure the license to meet the requirements for using the licensable feature or scale level. The router or switch enables you to commit a configuration that specifies a licensable feature or scale without a license for a 30-day grace period. The grace period is a short-term grant that enables you to start using features in the pack or scale up to the system limits (regardless of the license key limit) without a license key installed. The grace period begins when the licensable feature or scaling level is actually used by the device (not when it is first committed). In other words, you can commit licensable features or scaling limits to the device configuration, but the grace period does not begin until the device uses the licensable feature or exceeds a licensable scaling level.



NOTE: Configurations might include both licensed and nonlicensed features. For these situations, the license is enforced up to the point where the license can be clearly distinguished. For example, an authentication-order configuration is shared by both Authentication, Authorization, and Accounting (AAA), which is licensed, and by Layer 2 Tunneling Protocol (L2TP), which is not licensed. When the configuration is committed, the device does not issue any license warnings, because it is not yet known whether AAA or L2TP is using the configuration. However, at runtime, the device checks for a license when AAA authenticates clients, but does not check when L2TP authenticates clients.

The device reports any license breach as a warning log message whenever a configuration is committed that contains a feature or scale limit usage that requires a license. Following the 30-day grace period, the device periodically reports the breach to syslog messages until a license is installed and properly configured on the device to resolve the breach.



NOTE: Successful commitment of a licensable feature or scaling configuration does not imply that the required licenses are installed or not required. If a required license is not present, the system issues a warning message after it commits the configuration.

**Related
Documentation**

- *Junos OS Feature Licenses*
- *Installation and Upgrade Guide for Security Devices*

Junos OS Feature License Model Number for J Series Services Routers and SRX Series Services Gateways

For information about how to purchase a software license, contact your Juniper Networks sales representative at <http://www.juniper.net/in/en/contact-us/>.

Each feature license is tied to exactly one software feature, and that license is valid for exactly one device. Table 10 on page 36 describes the Junos OS features that require licenses.

Table 10: Junos OS Feature Licenses

Junos OS License Requirements										
Feature	SRX100	SRX110	SRX210	SRX220	SRX240	SRX550	SRX650	SRX1400	SRX3000 line	SRX5000 line
Access Manager	X	X	X	X	X	X	X			

Table 10: Junos OS Feature Licenses (*continued*)

Junos OS License Requirements										
Feature	SRX100	SRX110	SRX210	SRX220	SRX240	SRX550	SRX650	SRX1400	SRX3000 line	SRX5000 line
BGP Route Reflectors							X			
Dynamic VPN	X	X	X	X	X	X	X			
IDP Signature Update	X *	X	X *	X *	X *	X	X	X	X	X
Application Signature Update (Application Identification)	X	X	X	X	X	X	X	X	X	X
Juniper-Kaspersky Antivirus	X	X	X	X	X	X	X			
Juniper-Sophos Antivirus	X	X	X	X	X	X	X	X	X	X
Juniper-Sophos Antispam	X	X	X	X	X	X	X	X	X	X
Juniper-Enhanced Web filtering	X	X	X	X	X	X	X	X	X	X
Juniper-Websense Web filtering	X	X	X	X	X	X	X			
Logical Systems								X	X	X
SRX100 Memory Upgrade	X									
UTM	X*	X	X *	X	X *	X	X	X	X	X

* Indicates support on high-memory devices only.

Each license allows you to run the specified advanced software features on a single device.

Related Documentation

- [Junos OS License Overview on page 33](#)
- *Installation and Upgrade Guide for Security Devices*
- *Installation and Upgrade Guide for Security Devices*
- *Administration Guide for Security Devices*

PART 2

Installation

- [Software Installation and Upgrade on page 41](#)
- [Dual-Root Partitioning and Autorecovery on page 67](#)
- [Boot Loaders and Boot Devices on page 77](#)
- [Software Downgrade on page 79](#)

CHAPTER 7

Software Installation and Upgrade

- [Upgrading Individual Software Packages on page 42](#)
- [Preparing Your SRX Series Device for Junos OS Upgrades on page 44](#)
- [Preparing Your J Series Services Router for Junos OS Upgrades on page 45](#)
- [Preparing the USB Flash Drive to Upgrade Junos OS on page 46](#)
- [Determining the Junos OS Version on page 48](#)
- [Connecting to the Console Port on page 48](#)
- [Backing Up the Current Installation \(J Series Services Routers and SRX Series Services Gateways\) on page 49](#)
- [Downloading Software on page 50](#)
- [Downloading Junos OS Upgrades for SRX Series Devices on page 52](#)
- [Downloading Junos OS Upgrades for J Series Devices on page 53](#)
- [Checking the Current Configuration and Candidate Software Compatibility on page 53](#)
- [Verifying Available Disk Space on SRX Series Devices on page 54](#)
- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 55](#)
- [Example: Installing Junos OS Upgrades on J Series Devices on page 57](#)
- [Installing Junos OS Using TFTP on SRX Series Devices on page 60](#)
- [Installing Junos OS Using a USB Flash Drive on SRX Series Devices on page 62](#)
- [Installing Junos OS Upgrades from a Remote Server on the SRX Series Devices on page 63](#)
- [Installing Junos OS Upgrades from a Remote Server on J Series Devices on page 64](#)

Upgrading Individual Software Packages

To upgrade an individual Junos OS package, follow these steps:

1. Download the software packages you need from the Juniper Networks Support Web site at <http://www.juniper.net/support/>. Choose either the Canada and U.S. Version or the Worldwide Version.

To download the software packages, you must have a service contract and an access account. If you need help obtaining an account, complete the registration form at the Juniper Networks Web site: <https://www.juniper.net/registration/Register.jsp>.



NOTE: We recommend that you upgrade all individual software packages using an out-of-band connection from the console or management Ethernet interface, because in-band connections can be lost during the upgrade process.

2. Back up the currently running and active file system so that you can recover to a known, stable environment in case something goes wrong with the upgrade:

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

High-end SRX Series devices, the root file system is backed up to **/altroot**, and **/config** is backed up to **/altconfig**. The root and **/config** file systems are on the router's CompactFlash card, and the **/altroot** and **/altconfig** file systems are on the router's hard disk or solid-state drive (SSD).



NOTE: This step is optional for branch SRX Series devices. For branch SRX Series devices, ensure that a USB flash drive is plugged into the USB port of the device.



NOTE: Running the **request system snapshot** command overwrites the previous version of the software stored in the backup media.



NOTE: After you issue the **request system snapshot** command, you cannot return to the previous version of the software, because the running copy and the backup copy of the software are identical.

3. If you are copying multiple software packages to the device, copy them to the **/var/tmp** directory on the hard disk or solid-state drive (SSD):

```
user@host> file copy ftp://username :prompt@ftp.hostname  
          .net/filename/var/tmp/filename
```

4. Add the new software package:

```
user@host> request system software add /var/tmp/ installation-package validate
```

installation-package is the full URL to the file.



WARNING: For high-end SRX Series devices, do not include the *re0 | re1* option when you install a package using the `request system software add` command, if the Routing Engine on which the package is located and the Routing Engine on which you want to install the package is the same. In such cases, the package gets deleted after a successful upgrade.

The system might display the following message:

```
pkg_delete: couldn't entirely delete package
```

This message indicates that someone manually deleted or changed an item that was in a package. You do not need to take any action; the package is still properly deleted.

If you are upgrading more than one package at the same time, add **jbase** first. If you are using this procedure to upgrade all packages at once, add them in the following order:

```
user@host> request system software add /var/tmp/jbase-release-signed.tgz
user@host> request system software add /var/tmp/jkernel-release-signed.tgz
user@host> request system software add /var/tmp/jpfe-release-signed.tgz
user@host> request system software add /var/tmp/jdocs-release-signed.tgz
user@host> request system software add /var/tmp/jweb-release-signed.tgz
user@host> request system software add /var/tmp/jroute-release-signed.tgz
user@host> request system software add /var/tmp/jcrypto-release-signed.tgz
```

5. Reboot the router to start the new software:

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

6. After you have upgraded or downgraded the software and are satisfied that the new software is successfully running, issue the `request system snapshot` command to back up the new software:

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



NOTE: This step is optional for branch SRX Series devices. For branch SRX Series devices, ensure that a USB flash drive is plugged into the USB port of the device.

For high-end SRX Series devices, the root file system is backed up to **/altroot**, and **/config** is backed up to **/altconfig**. The root and **/config** file systems are on the router's CompactFlash card, and the **/altroot** and **/altconfig** file systems are on the router's hard disk or solid-state drive (SSD).



NOTE: After you issue the `request system snapshot` command, you cannot return to the previous version of the software, because the running copy and backup copy of the software are identical.



NOTE: Running the `request system snapshot` command overwrites the previous version of the software stored in backup media.

Related Documentation

- *Installation and Upgrade Guide for Security Devices*

Preparing Your SRX Series Device for Junos OS Upgrades

Before you begin upgrading Junos OS on an SRX Series device, make sure that you have completed the following:

- Obtained a Juniper Networks Web account and a valid support contract. You must have an account to download software upgrades. To obtain an account, complete the registration form at the Juniper Networks website:
<https://www.juniper.net/registration/Register.jsp>.
- Backed up your primary boot device onto a secondary storage device.

Creating a backup has the following advantages:

- If, during an upgrade, the primary boot device fails or becomes corrupted, the device can boot from backup and come back online
- Your active configuration files and log files are retained.
- If an upgrade is unsuccessful, the device can recover using a known, stable environment.

You can use either the J-Web user interface or the CLI to back up the primary boot device on the secondary storage device.

Table 11 on page 44 lists the secondary storage devices available on an SRX Series devices.

Table 11: Secondary Storage Devices for SRX Series Devices

Storage Device	Available on Services Gateways	Minimum Storage Required
USB storage device	SRX100, SRX210, SRX220, and SRX240 Services Gateways	1 GB
	SRX650 Services Gateway	2 GB
External CompactFlash (CF)	SRX650 Services Gateway	2 GB

**NOTE:**

- During a successful upgrade, the upgrade package completely reinstalls the existing Junos OS. It retains configuration files, log files, and similar information from the previous version.
- After a successful upgrade, remember to back up the new current configuration to the secondary device.

Related Documentation

- [Upgrading Individual Software Packages on page 42](#)
- *Installation and Upgrade Guide for Security Devices*
- [Determining the Junos OS Version on page 48](#)
- [Connecting to the Console Port on page 48](#)
- [Backing Up the Current Installation \(J Series Services Routers and SRX Series Services Gateways\) on page 49](#)
- *Installation and Upgrade Guide for Security Devices*

Preparing Your J Series Services Router for Junos OS Upgrades

Before you begin upgrading Junos OS on J Series devices:

- Obtain a Juniper Networks Web account and a valid support contract. You must have an account to download Junos OS upgrades. To obtain an account, complete the registration form at the Juniper Networks website:
<https://www.juniper.net/registration/Register.jsp>
- Back up your primary boot device onto a secondary storage device. Creating a backup has the following advantages:
 - The device can boot from backup and come back online in case of failure or corruption of the primary boot device in the event of power failure during an upgrade.
 - Your active configuration files and log files are retained.
 - The device can recover from a known, stable environment in case of an unsuccessful upgrade.

You can use either the J-Web user interface or the CLI to back up the primary boot device on the secondary storage device.

[Table 12 on page 45](#) lists the secondary storage devices available in a J Series device for backup.

Table 12: Secondary Storage Devices for Backup

Storage Device	Available on J Series Devices	Minimum Storage Required
External CompactFlash (CF) card	J2320 and J2350	512 MB

**NOTE:**

- During a successful upgrade, the upgrade package completely reinstalls the existing Junos OS. It retains configuration files, log files, and similar information from the previous version.
- After a successful upgrade, back up the new current configuration to the secondary device.



NOTE: Previously, upgrading images on J Series devices with a 256 MB CF card from Junos OS Release 8.5 and earlier involved removing unwanted files in the images and removing the Swap Partition. From Junos OS Release 9.2 and later, as an alternative, Junos OS accomplishes the upgrade efficiently to take another snapshot of the CF card, install the image, and restore configurations.

Related Documentation

- [Understanding Junos OS Upgrade and Downgrade Procedures for J Series Devices on page 14](#)
- [Downloading Junos OS Upgrades for J Series Devices on page 53](#)
- [Example: Installing Junos OS Upgrades on J Series Devices on page 57](#)
- [Example: Downgrading Junos OS on J Series Devices on page 81](#)
- *Installation and Upgrade Guide for Security Devices*

Preparing the USB Flash Drive to Upgrade Junos OS



NOTE: This topic is applicable only to SRX100, SRX210, SRX220, SRX240, and SRX650 devices.

This feature simplifies the upgrading of Junos OS images in cases where there is no console access to an SRX Series device located at a remote site. This functionality allows you to upgrade the Junos OS image with minimum configuration effort by simply copying the image onto a USB flash drive, inserting it into the USB port of the SRX Series device, and performing a few simple steps. You can also use this feature to reformat a boot device and recover an SRX Series device after boot media corruption.

You can use any USB flash drive device formatted with FAT/FAT 32 file systems for the installation process.



NOTE: This feature is not supported on chassis clusters.

Before you begin:

- Copy the Junos OS upgrade image and its `autoinstall.conf` file to the USB device.
- Ensure that adequate space is available on the SRX Series device to install the software image.

To prepare the USB flash drive and copy the Junos OS image onto the USB flash drive:

1. Insert the USB flash drive into the USB port of a PC or laptop computer running Windows.
2. From My Computer, right-click the drive Devices with Removable Storage.
3. Format the drive with the FAT/FAT32 file system.
4. Copy the Junos OS image onto the USB device.

For the installation process to succeed, copy only one image onto the USB device. Only images named `junos-srxsme*` are recognized by the system.

5. Check the drive name detected in My Computer for the USB device. Open the command prompt window and type:

```
echo " " > <drive-name>:\autoinstall.conf
```

For example, if the drive detected is drive F, type `echo " " > F:\autoinstall.conf` at the command prompt. This empty file indicates to the system that the automatic installation of the Junos OS image from the USB device is supported.

6. (Optional) Create a text file named `junos-config.conf` and copy the file to the USB device. For example, the following file supports an automatic configuration update during the installation process:

```
system {
  host-name narfi-8;
  domain-name englab.juniper.net;
  domain-search [ englab.juniper.net juniper.net jnpr.net spglab.juniper.net ];
  root-authentication {
    encrypted-password "$1$6RBM/j7k$IIGQ6hBMwGxOqCnK9dlWR0"; ##
    SECRET-DATA
  }
}
...
...
routing-options {
  static {
    route 0.0.0.0/0 next-hop 10.207.31.254;
  }
}
```



NOTE: The `junos-config.conf` file is optional, and it is not necessary for the automatic installation of the Junos OS image from the USB device. You can use the `junos-config.conf` file for a backup configuration for recovery or if the existing configuration is accidentally deleted.

- Related Documentation**
- [Upgrading Individual Software Packages on page 42](#)
 - [Installation and Upgrade Guide for Security Devices](#)

Determining the Junos OS Version

To determine which software packages are running on the device and to get information about these packages, use the **show version** operational mode command at the top level of the command-line interface (CLI).



NOTE: The **show version** command does not show the software category installed, only the release number of the software.

- Related Documentation**
- [Upgrading Individual Software Packages on page 42](#)
 - [Connecting to the Console Port on page 48](#)
 - [Backing Up the Current Installation \(J Series Services Routers and SRX Series Services Gateways\) on page 49](#)
 - [Installation and Upgrade Guide for Security Devices](#)

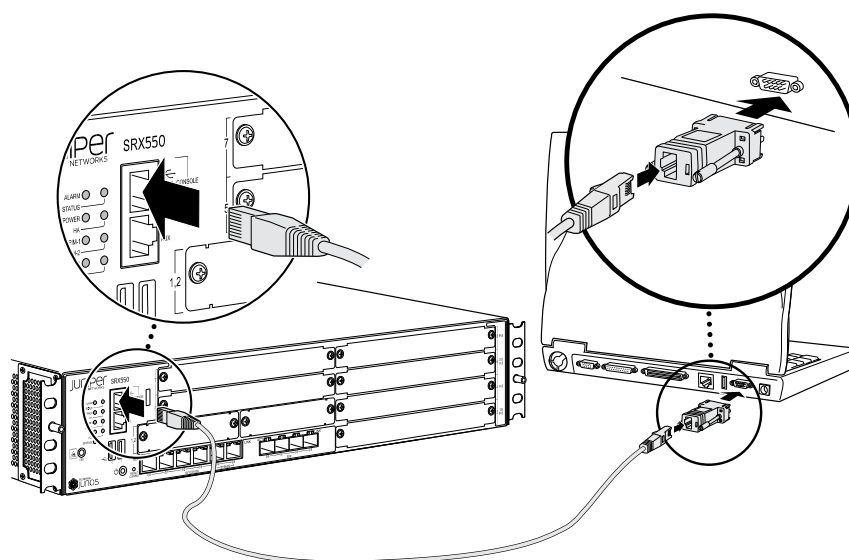
Connecting to the Console Port

The console port is a data terminal equipment (DTE) interface, providing a direct and continuous interface with the device. It is important to connect to the console during installation procedures so you can respond to any required user input and detect any errors that may occur.

Console ports allow root access to the Junos operating system (Junos OS) devices through a terminal or laptop interface, regardless of the state of the Junos OS device, unless it is completely powered off. By connecting to the console port, you can access the root level of the Junos OS device without using the network to which the device might or might not be connected. This creates a secondary path to the Junos OS device without relying on the network. Using the terminal interface provides a technician sitting in a Network Operations Center a long distance away the ability to restore a Junos OS device or perform an initialization configuration securely, using a modem, even if the primary network has failed. Without a connection to the console port, a technician would have to visit the site to perform repairs or initialization.

To configure the device initially, you must connect a terminal or laptop computer to the device through the console port, as shown in [Figure 2 on page 49](#).

Figure 2: Connecting to the Console Port on a Junos OS Device



9034114

A remote connection to the Junos OS device through a modem requires the cable and connector (provided in the device accessory box), plus a DB-9 male to DB-25 male (or similar) adapter for your modem, which you must purchase separately.

For more information about connecting to the console port, see the [Hardware Documentation](#) for your particular device.

Related Documentation

- [Upgrading Individual Software Packages on page 42](#)
- [Determining the Junos OS Version on page 48](#)
- *Installation and Upgrade Guide for Security Devices*

Backing Up the Current Installation (J Series Services Routers and SRX Series Services Gateways)

You should back up the current installation so that you can return to the current software installation. In a dual Routing Engine system, you need to back up both Routing Engines.

The installation process using the installation package (**junos-jsr***) removes all stored files on the router except the **juniper.conf** and SSH files. Therefore, you should back up your current configuration in case you need to return to the current software installation after running the installation program.

The following instructions offer the minimum steps required to create a backup on a J Series router during the installation process.

To back up the Junos OS on the J Series routers:

1. Attach an external memory device to the router.



NOTE: Even when attached to a J Series router, the USB memory device is not listed as a storage device in the `show system storage` CLI command output. You can view the installed USB memory device on the J-Web interface's system monitor screen.

2. Issue the `request system snapshot media usb` command.

The current software installation and configuration are saved on the external USB storage device.

**Related
Documentation**

- [Downloading Software on page 50](#)
- [Downloading Junos OS Upgrades for SRX Series Devices on page 52](#)
- *Installation and Upgrade Guide for Security Devices*

Downloading Software

You can download the software in one of the two ways:

- [Downloading Software with a Browser on page 50](#)
- [Downloading Software Using the Command-Line Interface on page 51](#)

Downloading Software with a Browser

You download the software package you need from the Juniper Networks Support Web site at <http://www.juniper.net/support/>.



NOTE: To access the download section, you must have a service contract and an access account. If you need help obtaining an account, complete the registration form at the Juniper Networks Web site: <https://www.juniper.net/registration/Register.jsp>.

To download the software:

1. In a browser, go to <http://www.juniper.net/support/>.
The Support page opens.
2. In the Download Software section, select the software version to download.
Depending on your location, select Junos Canada and US, or Junos Worldwide.
3. Select the current release to download.
4. Click the Software tab and select the Junos Installation Package to download.

A dialog box opens.

5. Save the file to your system. If you are placing the file on a remote system, you must make sure that the file can be accessible by the router or switch using HTTP, FTP, or scp.

Downloading Software Using the Command-Line Interface

Download the software package you need from the Juniper Networks Support Web site at <http://www.juniper.net/support/>, and place the package on a local system. You can then transfer the downloaded package to the device using either the router or switch command-line interface, or the local system command-line interface.



NOTE: To access the download section, you must have a service contract and an access account. If you need help obtaining an account, complete the registration form at the Juniper Networks Web site: <https://www.juniper.net/registration/Register.jsp>.

Before you transfer the software package, ensure that the FTP service is enabled on the device.

Enable the FTP service using the **set system services ftp** command:

```
user@host# set system services ftp
```

To transfer the software package using the device command-line interface:

1. From the router or switch command line, initiate an FTP session with the local system (host) where the package is located using the **ftp** command:

```
user@host> ftp host
```

host is the Hostname or address of the local system.

2. Log in with your customer support–supplied username and password:

```
User Name: username
331 Password required for username.
Password: password
```

Once your credentials have been validated, the FTP session opens.

3. Navigate to the software package location on the local system, and transfer the package using the **get** command:

```
user@host> get installation-package
```

Following is an example of an *installation-package* name:

```
jinstall-9.2R1.8–domestic-signed.tgz
```

4. Close the FTP session using the **bye** command:

```
user@host> bye
Goodbye
```

To transfer the package using the local system command-line interface:

1. From the local system command line, initiate an FTP session with the device using the **ftp** command:

```
user@host> ftp host
```

host is the Hostname or address of the router or switch.

2. Log in with your customer support–supplied username and password:

```
User Name: username
331 Password required for username.
Password: password
```

Once your credentials have been validated, the FTP session opens.

3. Navigate to the software package location on the local system, and transfer the package using the **put** command:

```
user@host> put installation-package
```

Following is an example of an *installation-package* name:

jinstall-9.2R1.8–domestic-signed.tgz

4. Close the FTP session using the **bye** command:

```
user@host> bye
Goodbye
```

Related Documentation

- [Upgrading Individual Software Packages on page 42](#)
- [Checking the Current Configuration and Candidate Software Compatibility on page 53](#)
- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 55](#)
- [Example: Installing Junos OS Upgrades on J Series Devices on page 57](#)
- *Installation and Upgrade Guide for Security Devices*

Downloading Junos OS Upgrades for SRX Series Devices

To download Junos OS upgrades from Juniper Networks:

1. Using a Web browser, follow the links to the download URL on the Juniper Networks webpage. Depending on your location, select the Canada and U.S. version (domestic) or the Worldwide version (ww):
 - <https://www.juniper.net/support/csc/swdist-domestic/>
 - <https://www.juniper.net/support/csc/swdist-ww/>
2. Log in to the Juniper Networks website using the username (generally your e-mail address) and password supplied by your Juniper Networks representative.
3. Select the appropriate software image for your platform.
4. Download Junos OS to a local host or to an internal software distribution site.

- Related Documentation**
- [Upgrading Individual Software Packages on page 42](#)
 - [Preparing Your SRX Series Device for Junos OS Upgrades on page 44](#)
 - [Preparing Your J Series Services Router for Junos OS Upgrades on page 45](#)
 - [Checking the Current Configuration and Candidate Software Compatibility on page 53](#)
 - *Installation and Upgrade Guide for Security Devices*

Downloading Junos OS Upgrades for J Series Devices

To download software upgrades from Juniper Networks:

1. Using a Web browser, follow the links to the download URL on the Juniper Networks webpage. Depending on your location, select either Canada and U.S. Version or Worldwide Version:
 - <https://www.juniper.net/support/csc/swdist-domestic/>
 - <https://www.juniper.net/support/csc/swdist-ww/>
2. Log in to the Juniper Networks website using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. Select the appropriate software image for your platform.
4. Download the software to a local host or to an internal software distribution site.

- Related Documentation**
- [Understanding Junos OS Upgrade and Downgrade Procedures for J Series Devices on page 14](#)
 - [Preparing Your J Series Services Router for Junos OS Upgrades on page 45](#)
 - [Example: Installing Junos OS Upgrades on J Series Devices on page 57](#)
 - [Example: Downgrading Junos OS on J Series Devices on page 81](#)
 - *Installation and Upgrade Guide for Security Devices*

Checking the Current Configuration and Candidate Software Compatibility

When you upgrade or downgrade Junos OS, we recommend that you include the **validate** option with the **request system software add** command to check that the candidate software is compatible with the current configuration. By default, when you add a package with a different release number, the validation check is done automatically.

- Related Documentation**
- [Downloading Software on page 50](#)
 - *Installation and Upgrade Guide for Security Devices*

Verifying Available Disk Space on SRX Series Devices

The amount of free disk space necessary to upgrade a device with a new version of the Junos OS can vary from one release to another. Check the Junos OS software version you are installing to determine the free disk space requirements.

If the amount of free disk space on a device is insufficient for installing the Junos OS, you might receive a warning similar to the following messages, that the /var filesystem is low on free disk space:

WARNING: The /var filesystem is low on free disk space.

WARNING: This package requires 1075136k free, but there is only 666502k available.

To determine the amount of free disk space on the device, issue the **show system storage detail** command. The command output displays statistics about the amount of free disk space in the device file systems.

A sample of the **show system storage detail** command output is shown below:

```
user@host> show system storage detail
```

Filesystem	1024-blocks	Used	Avail	Capacity	Mounted on
/dev/da0s2a	300196	154410	121772	56%	/
devfs	1	1	0	100%	/dev
/dev/md0	409000	409000	0	100%	/junos
/cf	300196	154410	121772	56%	/junos/cf
devfs	1	1	0	100%	/junos/dev/
procfs	4	4	0	100%	/proc
/dev/bo0s3e	25004	52	22952	0%	/config
/dev/bo0s3f	350628	178450	144128	55%	/cf/var
/dev/md1	171860	16804	141308	11%	/mfs
/cf/var/jail	350628	178450	144128	55%	/jail/var
/cf/var/log	350628	178450	144128	55%	/jail/var/log
devfs	1	1	0	100%	/jail/dev
/dev/md2	40172	4	36956	0%	/mfs/var/run/utm
/dev/md3	1884	138	1596	8%	/jail/mfs

When the system file storage space on the device is full, rebooting the device does not solve the problem. The following error message is displayed during a typical operation on the device after the file storage space is full.

```
user@host% cli
user@host> configure/var: write failed, filesystem is full
```

You can clean up the file storage on the device by deleting system files using the **request system storage cleanup** command as shown in following procedure:

1. Request to delete system files on the device.

```
user@host> request system storage cleanup
```

The list of files to be deleted is displayed.

List of files to delete:

Size	Date	Name
------	------	------


```

11B Oct 28 23:40 /var/jail/tmp/alarmd.ts
92.4K Jan 11 17:12 /var/log/chassisd.0.gz
92.4K Jan 11 06:06 /var/log/chassisd.1.gz
92.5K Jan 10 19:00 /var/log/chassisd.2.gz
92.5K Jan 10 07:53 /var/log/chassisd.3.gz
92.2K Jan 10 15:00 /var/log/hostlogs/auth.log.1.gz
92.2K Jan 1 18:45 /var/log/hostlogs/auth.log.2.gz
92.1K Jan 4 17:30 /var/log/hostlogs/auth.log.3.gz
92.2K Jan 1 18:45 /var/log/hostlogs/auth.log.4.gz
79.0K Jan 12 01:59 /var/log/hostlogs/daemon.log.1.gz
78.8K Jan 11 23:15 /var/log/hostlogs/daemon.log.2.gz
78.7K Jan 11 20:30 /var/log/hostlogs/daemon.log.3.gz
79.1K Jan 11 17:44 /var/log/hostlogs/daemon.log.4.gz
59.1K Jan 11 21:59 /var/log/hostlogs/debug.1.gz
59.2K Jan 11 17:44 /var/log/hostlogs/debug.2.gz
59.2K Jan 11 13:29 /var/log/hostlogs/debug.3.gz
59.3K Jan 11 09:14 /var/log/hostlogs/debug.4.gz
186.6K Oct 20 16:31 /var/log/hostlogs/kern.log.1.gz
238.3K Jan 11 23:15 /var/log/hostlogs/lcmd.log.1.gz
238.4K Jan 11 17:30 /var/log/hostlogs/lcmd.log.2.gz
238.6K Jan 11 11:45 /var/log/hostlogs/lcmd.log.3.gz
238.5K Jan 11 06:00 /var/log/hostlogs/lcmd.log.4.gz
372.5K Jan 11 17:00 /var/log/hostlogs/syslog.1.gz
372.5K Jan 11 04:45 /var/log/hostlogs/syslog.2.gz
371.9K Jan 10 16:30 /var/log/hostlogs/syslog.3.gz
372.7K Jan 10 04:15 /var/log/hostlogs/syslog.4.gz
10.1K Jan 12 02:03 /var/log/messages.0.gz
55.1K Jan 6 21:25 /var/log/messages.1.gz
81.5K Dec 1 21:30 /var/log/messages.2.gz

```

Delete these files ? [yes,no] (no)

2. Enter the option **yes** to proceed with deleting of the files.

Related Documentation

- [Downloading Software on page 50](#)
- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 55](#)
- [Example: Installing Junos OS Upgrades on J Series Devices on page 57](#)
- [Installation and Upgrade Guide for Security Devices](#)

Example: Installing Junos OS Upgrades on SRX Series Devices

This example shows how to install upgrades on the SRX Series devices.

- [Requirements on page 55](#)
- [Overview on page 56](#)
- [Configuration on page 56](#)
- [Verification on page 57](#)

Requirements

Before you begin:

- Verify the available space on the internal media. See [“Verifying Available Disk Space on SRX Series Devices” on page 54.](#)
- Download the software package. See [“Downloading Junos OS Upgrades for SRX Series Devices” on page 52.](#)
- Copy the software package to the device if you are installing the software package from a local directory on the device. We recommend that you copy it to the `/var/tmp` directory.

Overview

By default, the **request system software add *package-name*** 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 device can reboot successfully after the software package is installed. This is the default behavior when you are adding a software package.

In this example, add the software package `junos-srxsme-10.0R2-domestic.tgz` with the following options:

- **no-copy** option to install the software package but do not save the copies of package files. You should include this option if you do not have enough space on the internal media to perform an upgrade that keeps a copy of the package on the device.
- **no-validate** option to bypass the compatibility check with the current configuration before installation starts.
- **reboot** option to reboot the device after installation is completed.

Configuration

CLI Quick Configuration

To quickly install Junos OS upgrades on SRX Series devices, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

From operational mode, enter:

```
user@host> request system software add /var/tmp/junos-srxsme-10.0R2-domestic.tgz  
no-copy no-validate reboot
```

GUI Step-by-Step Procedure

To install Junos OS upgrades on SRX Series devices:

1. In the J-Web user interface, select **Maintain>Software>Upload Package**.
2. On the Upload Package page, specify the software package to upload. Click **Browse** to navigate to the software package location and select `junos-srxsme-10.0R2-domestic.tgz`.
3. Select the **Reboot If Required** check box to set the device to reboot automatically when the upgrade is complete.
4. Select the **Do not save backup** check box to bypass saving the backup copy of the current Junos OS package.

5. Click **Upload Package**. The software is activated after the device has rebooted.
6. Click **OK** to check your configuration and save it as a candidate configuration.
7. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To install Junos OS upgrades on SRX Series devices:

From operational mode, install the new package on the device with the `no-copy` and `no-validate` options, and format and re-partition the media before installation, and reboot the device after installation is completed.

```
user@host> request system software add /var/tmp/junos-srxsme-10.0R2-domestic.tgz
no-copy no-validate reboot
```

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

Results From configuration mode, confirm your configuration by entering the `show system` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter `commit` from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying the Junos OS Upgrade Installation

Purpose Verify that the Junos OS upgrade was installed.

Action From operational mode, enter the `show system` command.

Related Documentation

- [Example: Configuring Boot Devices for SRX Series Devices on page 95](#)
- [Junos OS Upgrade Methods on the SRX Series Devices on page 12](#)
- [Example: Downgrading Junos OS on SRX Series Devices on page 79](#)
- [Installing Junos OS Using a USB Flash Drive on SRX Series Devices on page 62](#)

Example: Installing Junos OS Upgrades on J Series Devices

This example shows how to install Junos OS upgrades on J Series devices.

- [Requirements on page 58](#)
- [Overview on page 58](#)

- [Configuration on page 58](#)
- [Verification on page 59](#)

Requirements

Before you begin:

- Verify the available space on the CompactFlash card. See the *Junos OS Release Notes*.
- Download the Junos OS package. See “[Downloading Junos OS Upgrades for J Series Devices](#)” on page 53.
- Copy the software package to the device if you are installing the Junos OS package from a local directory on the device. We recommend that you copy it to the `/var/tmp` directory.

Overview



NOTE: This procedure applies only to upgrading from one Junos OS software release to another or from one Junos OS services release to another.

By default, the **request system software add *package-name*** 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 device can reboot successfully after the software package is installed. This is the default behavior when you are adding a software package.

For this example, install the `junos-jsr-8.5R1.1.domestic.tgz` software package and copy it to the `/var/tmp` directory. Set the **unlink** option to remove the package at the earliest opportunity so that the device has enough storage capacity to complete the installation, and set the **no-copy** option to specify that the software package is installed but a copy of the package is not saved.

Configuration

CLI Quick Configuration

To quickly install Junos OS upgrades on J Series devices, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

From operational mode, enter:

```
user@host>  
request system software add unlink no-copy /var/tmp/junos-jsr-8.5R1.1.domestic.tgz  
request system reboot
```

GUI Step-by-Step Procedure

To install Junos OS upgrades on J Series devices:

1. In the J-Web user interface, select **Maintain>Software>Upload Package**.
2. On the Upload Package page, in the File to Upload field, type the location of the software package, or click **Browse** to navigate to the location.

3. Select the Reboot If Required check box to have the device reboot automatically when the upgrade is complete.
4. Click **Upload Package**. Junos OS is activated after the device has rebooted.
5. Click **OK** to check your configuration and save it as a candidate configuration.
6. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To install Junos OS upgrades on J Series devices:

1. From operational mode, install the new package on the device.

```
user@host> request system software add unlink no-copy
/var/tmp/junos-jsr-8.5R1.1.domestic.tgz
```

2. Reboot the device.

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

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

Results From configuration mode, confirm your configuration by entering the **show system** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying the Junos OS Upgrade Installation

Purpose Verify that the Junos OS upgrade was installed.

Action From operational mode, enter the **show system** command.

Related Documentation

- [Preparing Your J Series Services Router for Junos OS Upgrades on page 45](#)
- [Installing Junos OS Upgrades from a Remote Server on J Series Devices on page 64](#)
- [Example: Rebooting J Series Devices on page 155](#)
- [Example: Halting J Series Devices on page 159](#)
- [Installation and Upgrade Guide for Security Devices](#)

Installing Junos OS Using TFTP on SRX Series Devices

You can install the Junos OS using the Trivial File Transfer Protocol (TFTP) method. The device is shipped with the Junos OS loaded on the primary boot device. During the Junos OS installation from the loader, the device retrieves the Junos OS package from a TFTP server. The internal media is then formatted, and the Junos OS image is installed.

From the loader installation, you can:

- Install the Junos OS on the device for the first time.
- Recover the system from a file system corruption.



NOTE: Installation from a TFTP server can only be performed using the first onboard Ethernet interface.

Installation from the loader-over-TFTP method does not work reliably over slow speeds or large latency networks.

Before you begin, verify that:

- You have access to the TFTP server with the Junos OS package to be installed.
- That the TFTP server supports BOOTP or DHCP. If the TFTP server does not support BOOTP or DHCP, you must set the environment variables before performing the installation from the TFTP server.
- Functional network connectivity exists between the device and the TFTP server over the first onboard Ethernet interface.

To install the Junos OS image on the internal media of the device:

1. To access the U-boot prompt, use the console connection to connect to the device.
2. Reboot the device.

The following messages appear:

Clearing DRAM..... done BIST check passed. Net: pic init done (err = 0)octeth0 POST Passed

After this message appears, you see the following prompt:

Press SPACE to abort autoboot in 3 seconds

3. Press the space bar to stop the autoboot process.

The => U-boot prompt appears.

4. From the U-boot prompt, configure the environment variables listed in [Table 13 on page 61](#).

Table 13: Environment Variables Settings

Environment Variables	Description
gatewayip	IP address of the gateway device
ipaddr	IP address of the SRX Series device
netmask	network mask
serverip	IP address of the TFTP server

This example shows you how to configure the environment variables:

```

Clearing DRAM..... done
BIST check passed.
Net: pic init done (err = 0)octeth0
POST Passed
Press SPACE to abort autoboot in 3 seconds
=>
=> setenv ipaddr 10.157.70.170
=> setenv netmask 255.255.255.0
=> setenv gatewayip 10.157.64.1
=> setenv serverip 10.157.60.1
=> saveenv

```

5. Reboot the system using the **reset** command.
6. To access the loader prompt, enter use the console connection to connect to the device.
7. Reboot the device.

The following message appears:

Loading /boot/defaults/loader.conf

After this message appears, you see the following prompt:

Hit [Enter] to boot immediately, or space bar for command prompt.

8. Press the space bar to access the loader prompt.

The **loader>** prompt appears. Enter:

```
loader> install tftp://10.77.25.12/junos-srxsme-10.0R2-domestic.tgz
```



NOTE: The URL path is relative to the TFTP server's TFTP root directory, where the URL is in the form: `tftp://tftp-server-ipaddress/package`.

When this command is executed:

- The Junos OS package is downloaded from the TFTP server.
- The internal media on the system is formatted.
- The Junos OS package is installed on the internal media.



NOTE: The Installation from the loader-over-TFTP method installs Junos OS on the internal CF on SRX100, SRX210, SRX220, and SRX240 devices, whereas on SRX650 devices, this method can install Junos OS on the internal or external CF card.

After Junos OS is installed, the device boots from the internal media. Once the system boots up with Junos OS Release 10.0 or later, you should upgrade the U-boot and boot loader immediately.



CAUTION: When you install Junos OS using the loader-over-TFTP method, the media is formatted. The process attempts to save the current configuration. We recommend that you back up all important information on the device before using this process.

**Related
Documentation**

- [Downloading Software on page 50](#)
- [Preparing Your SRX Series Device for Junos OS Upgrades on page 44](#)
- [Downloading Junos OS Upgrades for SRX Series Devices on page 52](#)
- *Installation and Upgrade Guide for Security Devices*

Installing Junos OS Using a USB Flash Drive on SRX Series Devices

To install the Junos OS image on an SRX Series device using a USB flash drive:

1. Insert the USB flash drive into the USB port of the SRX Series device and wait for the LEDs to blink amber indicating that the SRX Series device detects the Junos OS image.

If the LEDs do not change to amber, press the Power button or turn the device off and then on again and wait for the LEDs to blink amber.

2. Press the **Reset Config** button on the SRX Series device to start the installation and wait for the LEDs to glow steadily amber.

When the LEDs glow green, the Junos OS upgrade image has been successfully installed.

If the USB device is plugged in, the **Reset Config** button always performs as an image upgrade button. Any other functionality of this button is overridden until you remove the USB flash drive.

3. Remove the USB flash drive.

The SRX Series device restarts automatically and loads the new Junos OS version.



NOTE: If an installation error occurs, the LEDs glow red, which might indicate that the Junos OS image on the USB flash drive is corrupted. An installation error can also occur if the current configuration on the SRX Series device is not compatible with the new Junos OS version on the USB or if there is not enough space on the SRX Series device to install the image. You must have console access to the SRX Series device to troubleshoot an installation error.



NOTE: You can use the `set system autoinstallation usb disable` command to prevent the automatic installation from the USB device. After using this command, if you insert the USB device into the USB port of the SRX Series device, the installation process does not work.

Related Documentation

- [Downloading Software on page 50](#)
- [Preparing Your SRX Series Device for Junos OS Upgrades on page 44](#)
- [Downloading Junos OS Upgrades for SRX Series Devices on page 52](#)
- *Installation and Upgrade Guide for Security Devices*

Installing Junos OS Upgrades from a Remote Server on the SRX Series Devices

You can use the J-Web user interface to install Junos OS packages that are retrieved with FTP or HTTP from the specified location.

Before you begin:

- Verify the available space on the internal media. See [“Verifying Available Disk Space on SRX Series Devices” on page 54](#).
- Download the Junos OS package. See [“Downloading Junos OS Upgrades for SRX Series Devices” on page 52](#).

To install Junos OS upgrades from a remote server:

1. In the J-Web user interface, select **Maintain>Software>Install Package**.
2. On the Install Remote page, enter the required information into the fields described in [Table 14 on page 64](#).

Table 14: Install Package Summary

Field	Function	Your Action
Package Location (required)	Specifies the FTP or HTTP server, file path, and Junos OS package name.	Type the full address of the Junos OS package location on the FTP or HTTP server—one of the following: <i>ftp://hostname/pathname/package-name</i> <i>http://hostname/pathname/package-name</i>
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	Specifies that the device is automatically rebooted when the upgrade is complete.	Check the box if you want the device to reboot automatically when the upgrade is complete.
Do not save backup	Specifies that the backup copy of the current Junos OS package is not saved.	Check the box if you want to save the backup copy of the Junos OS package.
Format and re-partition the media before installation	Specifies that the storage media is formatted and new partitions are created.	Check the box if you want to format the internal media with dual-root partitioning.

3. Click **Fetch and Install Package**. Junos OS is activated after the device reboots.

Related Documentation

- [Junos OS Upgrade Methods on the SRX Series Devices on page 12](#)
- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 55](#)
- [Example: Downgrading Junos OS on SRX Series Devices on page 79](#)
- [Installing Junos OS Using a USB Flash Drive on SRX Series Devices on page 62](#)
- *Installation and Upgrade Guide for Security Devices*

Installing Junos OS Upgrades from a Remote Server on J Series Devices

You can use the J-Web interface to install Junos OS packages that are retrieved with FTP or HTTP from the specified location.



NOTE: This procedure applies only to upgrading from one Junos OS release to another.

Before installing the Junos OS upgrade:

- Verify the available space on the CompactFlash (CF) card. See the *Junos OS Release Notes*.
- Download the software package.

To install Junos OS upgrades from a remote server:

1. In the J-Web user interface, select **Maintain>Software>Install Package**.
2. On the Install Remote page, enter the required information described in [Table 15 on page 65](#).

Table 15: Install Remote 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 on the FTP or HTTP server—one of the following: <i>ftp://hostname/pathname/package-name</i> <i>http://hostname/pathname/package-name</i>
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	Specifies that the device is automatically rebooted when the upgrade is complete.	Select the check the box if you want the device to reboot automatically when the upgrade is complete.

3. Click **Fetch and Install Package**. Junos OS is activated after the device reboots.

Related Documentation

- [Preparing Your J Series Services Router for Junos OS Upgrades on page 45](#)
- [Example: Rebooting J Series Devices on page 155](#)
- [Example: Halting J Series Devices on page 159](#)
- *Installation and Upgrade Guide for Security Devices*

CHAPTER 8

Dual-Root Partitioning and Autorecovery

- [Understanding Automatic Recovery of the Primary Junos OS Image with Dual-Root Partitioning on page 67](#)
- [Understanding How the Primary Junos OS Image with Dual-Root Partitioning Recovers on SRX Series Devices on page 69](#)
- [Junos OS Release 9.6 or Earlier Installation on SRX Series Devices with Dual-Root Partitioning on page 71](#)
- [Junos OS Release 10.0 or Later Upgrades with Dual-Root Partitioning on SRX Series Devices on page 72](#)
- [Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 72](#)
- [Reinstalling the Single-Root Partition Using request system software add Command on page 76](#)

Understanding Automatic Recovery of the Primary Junos OS Image with Dual-Root Partitioning

The auto-snapshot feature repairs the corrupted primary root when the device reboots from the alternate root. This is accomplished by taking a snapshot of the alternate root onto the primary root automatically rather than manually from the CLI.

```
login: user
```

```
Password:
```

```
*****
```

```
**
```

```
**
```

```
** WARNING: THIS DEVICE HAS BOOTED FROM THE BACKUP JUNOS IMAGE
```

```
**
```

```
**
```

```
**
```

```
** It is possible that the primary copy of JUNOS failed to boot up
```

```
**
```

```
** properly, and so this device has booted from the backup copy.
```

```
**
```

```
**
```

```
**
```

```
** The primary copy will be recovered by auto-snapshot feature now. **  
**  
*****
```

When this feature is enabled, and the device reboots from the alternate root (because of a corrupted primary root or power cycle during restart), the following actions take place:

1. A prominent message is displayed indicating a failure to boot from the primary root.
2. A system **boot from backup root** alarm is set. This is useful for devices that do not have console access.
3. A snapshot of the alternate root onto the primary root is made.
4. Once the snapshot is complete, the system **boot from backup root** alarm is cleared.

During the next reboot, the system determines the good image on the primary root and boots normally.



NOTE: We recommend performing the snapshot once all the processes start. This is done to avoid any increase in the reboot time.



NOTE:

- Auto-snapshot feature is supported on branch SRX Series devices.
 - By default the auto-snapshot feature is disabled.
 - If you do not maintain the same version of Junos OS in both partitions, ensure that the automatic snapshot feature remains disabled. Otherwise, if you have an earlier version of Junos OS in the alternate partition and the system reboots from the alternate root partition, the automatic snapshot feature causes the later Junos OS version to be replaced with the earlier version.
 - When automatic snapshot is disabled and the system reboots from the alternate root partition, it triggers an alarm indicating that the system has rebooted from its alternate partition.
-

Enable this feature with the **set system auto-snapshot** command. Once the primary root partition is recovered using this method, the device will successfully boot from the primary root partition on the next reboot.

Execute the **delete system auto-snapshot** command to delete all backed up data and disable auto-snapshot, if required.

Use the **show system auto-snapshot** command to check the auto-snapshot status.

When auto-snapshot is in progress, you cannot run a manual snapshot command concurrently and the following error message appears:

Snapshot already in progress. Please try after sometime.



NOTE: If you log into the device when the snapshot is in progress, the following banner appears: The device has booted from the alternate partition, auto-snapshot is in progress.

Related Documentation

- [Understanding Junos OS Upgrades for SRX Series Devices on page 10](#)
- [Dual-Root Partitioning Scheme Overview on page 19](#)
- [Understanding How the Primary Junos OS Image with Dual-Root Partitioning Recovers on SRX Series Devices on page 69](#)
- [Junos OS Release 10.0 or Later Upgrades with Dual-Root Partitioning on SRX Series Devices on page 72](#)
- [Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 72](#)
- [Junos OS Release 9.6 or Earlier Installation on SRX Series Devices with Dual-Root Partitioning on page 71](#)
- [Installation and Upgrade Guide for Security Devices](#)

Understanding How the Primary Junos OS Image with Dual-Root Partitioning Recovers on SRX Series Devices

If the SRX Series Services Gateway is unable to boot from the primary Junos OS image, and boots up from the backup Junos OS image in the backup root partition, a message appears on the console at the time of login indicating that the device has booted from the backup Junos OS image.

```
login: user
```

```
Password:
```

```
*****
**                                                                 **
**  WARNING: THIS DEVICE HAS BOOTED FROM THE BACKUP JUNOS IMAGE  **
**                                                                 **
**  It is possible that the active copy of JUNOS failed to boot up **
**  properly, and so this device has booted from the backup copy.  **
**                                                                 **
```

```

** Please re-install JUNOS to recover the active copy in case
** it has been corrupted.
**
*****

```

Because the system is left with only one functional root partition, you should immediately restore the primary Junos OS image using one of the following methods:

- Install a new image using the CLI or J-Web user interface. The newly installed image will become the primary image, and the device will boot from it on the next reboot.
- Use a snapshot of the backup root partition by entering the **request system snapshot slice alternate** command. Once the primary root partition is recovered using this method, the device will successfully boot from the primary root partition on the next reboot. After the procedure, the primary root partition will contain the same version of Junos OS as the backup root partition.



NOTE: You can use the CLI command **request system snapshot slice alternate** to back up the currently running root file system (primary or secondary) to the other root partition on the system.

You can use this command to:

- Save an image of the primary root partition in the backup root partition when system boots from the primary root partition.
- Save an image of the backup root partition in the primary root partition when system boots from the backup root partition.



WARNING: The process of restoring the alternate root by using the CLI command **request system snapshot slice alternate** takes several minutes to complete. If you terminate the operation before completion, the alternate root might not have all required contents to function properly.

Related Documentation

- [Understanding Junos OS Upgrades for SRX Series Devices on page 10](#)
- [Dual-Root Partitioning Scheme Overview on page 19](#)
- [Junos OS Release 10.0 or Later Upgrades with Dual-Root Partitioning on SRX Series Devices on page 72](#)
- [Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 72](#)
- [Junos OS Release 9.6 or Earlier Installation on SRX Series Devices with Dual-Root Partitioning on page 71](#)

- *Installation and Upgrade Guide for Security Devices*

Junos OS Release 9.6 or Earlier Installation on SRX Series Devices with Dual-Root Partitioning

Junos OS Release 9.6 and earlier is not compatible with the dual-root partitioning scheme. These releases can only be installed if the media is reformatted with single-root partitioning. Any attempt to install Junos OS Release 9.6 or earlier on a device with dual-root partitioning without reformatting the media will fail with an error. You must install the Junos OS Release 9.6 or earlier image from the boot loader using a TFTP server or USB storage device.



NOTE: Junos OS Release 12.1X45 and later do not support single root partitioning.



NOTE: You do not need to reinstall the earlier version of the boot loader if you are installing the Junos OS Release 9.6.

You cannot install a Junos OS Release 9.6 or earlier package on a system with dual-root partitioning using the Junos OS CLI or J-Web. If this is attempted, an error will be returned.

You can install the Junos OS Release 9.6 (9.6R3 and 9.6R4 [only]) on a system with dual-root partitioning using `request system software add` command with `partition` option.

Related Documentation

- [Understanding Junos OS Upgrades for SRX Series Devices on page 10](#)
- [Dual-Root Partitioning Scheme Overview on page 19](#)
- [Junos OS Release 10.0 or Later Upgrades with Dual-Root Partitioning on SRX Series Devices on page 72](#)
- [Understanding How the Primary Junos OS Image with Dual-Root Partitioning Recovers on SRX Series Devices on page 69](#)
- [Reinstalling the Single-Root Partition Using `request system software add` Command on page 76](#)
- *Installation and Upgrade Guide for Security Devices*

Junos OS Release 10.0 or Later Upgrades with Dual-Root Partitioning on SRX Series Devices



NOTE: If you are upgrading to Junos OS Release 10.0 without transitioning to dual-root partitioning, use the conventional CLI and J-Web user interface installation methods.

To format the media with dual-root partitioning while upgrading to Junos OS Release 10.0 or later, use one of the following installation methods:

- Installation from the boot loader using a TFTP server. We recommend this if console access to the system is available and a TFTP server is available in the network. See [“Installing Junos OS Using TFTP on SRX Series Devices” on page 60](#)
- Installation from the boot loader using a USB storage device. We recommend this method if console access to the system is available and the system can be physically accessed to plug in a USB storage device. See [“Installing Junos OS Using a USB Flash Drive on SRX Series Devices” on page 62](#)
- Installation from the CLI using the **partition** option. We recommend this method only if console access is not available. This installation can be performed remotely.



NOTE: After upgrading to Junos OS Release 10.0 or later, the U-boot and boot loader must be upgraded for the dual-root partitioning scheme to work properly.

Related Documentation

- [Dual-Root Partitioning Scheme Overview on page 19](#)
- [Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 72](#)
- [Junos OS Release 9.6 or Earlier Installation on SRX Series Devices with Dual-Root Partitioning on page 71](#)
- [Understanding How the Primary Junos OS Image with Dual-Root Partitioning Recovers on SRX Series Devices on page 69](#)
- *Installation and Upgrade Guide for Security Devices*

Example: Installing Junos OS on SRX Series Devices Using the Partition Option

This example shows how to install Junos OS Release 10.0 or later with the **partition** option.

- [Requirements on page 73](#)
- [Overview on page 73](#)

- [Configuration on page 74](#)
- [Verification on page 75](#)

Requirements

Before you begin, back up any important data.

Overview

This example formats the internal media and installs the new Junos OS image on the media with dual-root partitioning. Reinstall the Release 10.0 or later image from the CLI using the **request system software add** command with the **partition** option. This copies the image to the device, and then reboots the device for installation. The device boots up with the Release 10.0 or later image installed with the dual-root partitioning scheme. When the **partition** option is used, the format and install process is scheduled to run on the next reboot. Therefore, we recommend that this option be used together with the **reboot** option.



NOTE: The process might take 15 to 20 minutes. The system is not accessible over the network during this time.



WARNING: Using the **partition** option with the **request system software add** command erases the existing contents of the media. Only the current configuration is preserved. You should back up any important data before starting the process.



NOTE: Partition install is supported on the default media on SRX100, SRX210, and SRX240 devices (internal NAND flash) and on SRX650 devices (internal CF card).

Partition install is *not* supported on the alternate media on SRX100, SRX210, and SRX240 devices (USB storage key) or on SRX650 devices (external CF card or USB storage key).

In this example, add the software package `junos-srxsme-10.0R2-domestic.tgz` with the following options:

- **no-copy** option to install the software package but do not save the copies of package files. You should include this option if you do not have enough space on the internal media to perform an upgrade that keeps a copy of the package on the device.
- **no-validate** option to bypass the compatibility check with the current configuration before installation starts.
- **partition** option to format and re-partition the media before installation.
- **reboot** option to reboots the device after installation is completed.

Configuration

CLI Quick Configuration To quickly install Junos OS Release 10.0 or later with the **partition** option, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

From operational mode, enter:

```
user@host>request system software add junos-srxsme-10.0R2-domestic.tgz no-copy  
no-validate partition reboot
```

GUI Step-by-Step Procedure To install Junos OS Release 10.0 or later with the **partition** option:

1. In the J-Web user interface, select **Maintain>Software>Install Package**.
2. On the Install Package page, specify the FTP or HTTP server, file path, and software package name. Type the full address of the software package location on the FTP (<ftp://hostname/pathname/junos-srxsme-10.0R2-domestic.tgz>) or HTTP server (<http://hostname/pathname/junos-srxsme-10.0R2-domestic.tgz>).



NOTE: Specify the username and password, if the server requires one.

3. Select the **Reboot If Required** check box to set the device to reboot automatically when the upgrade is complete.
4. Select the **Do not save backup** check box to bypass saving the backup copy of the current Junos OS package.
5. Select the **Format and re-partition the media before installation** check box to format the internal media with dual-root partitioning.
6. Click **Fetch and Install Package**. The software is activated after the device reboots.

This formats the internal media and installs the new Junos OS image on the media with dual-root partitioning.

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To install Junos OS Release 10.0 or later with the **partition** option:

1. Upgrade the device to Junos OS Release 10.0 or later using the CLI.
2. After the device reboots, upgrade the boot loader to the latest version. See [“Upgrading the Boot Loader on SRX Series Devices” on page 77](#).
3. Reinstall the Release 10.0 or later image.

```
user@host>request system software add junos-srxsme-10.0R2-domestic.tgz no-copy  
no-validate partition reboot  
Copying package junos-srxsme-10.0R2-domestic.tgz to var/tmp/install  
Rebooting ...
```

Results From configuration mode, confirm your configuration by entering the **show system storage partitions** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

Sample output on a system with single root partitioning:

```
user@host> show system storage partitions

Boot Media: internal (da0)

Partitions Information:
  Partition  Size  Mountpoint
    s1a      898M  /
    s1e      24M   /config
    s1f       61M   /var
```

Sample output on a system with dual-root partitioning:

```
user@host> show system storage partitions

Boot Media: internal (da0)
Active Partition: da0s2a
Backup Partition: da0s1a
Currently booted from: active (da0s2a)

Partitions Information:
  Partition  Size  Mountpoint
    s1a      293M  altroot
    s2a      293M  /
    s3e      24M   /config
    s3f     342M   /var
    s4a       30M  recovery
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

- [Verifying the Partitioning Scheme Details on page 75](#)

Verifying the Partitioning Scheme Details

Purpose Verify that the partitioning scheme details on the SRX Series device were configured.

Action From operational mode, enter the **show system storage partitions** command.

Related Documentation

- [Dual-Root Partitioning Scheme Overview on page 19](#)
- [Junos OS Release 10.0 or Later Upgrades with Dual-Root Partitioning on SRX Series Devices on page 72](#)
- [Junos OS Release 9.6 or Earlier Installation on SRX Series Devices with Dual-Root Partitioning on page 71](#)

- [Understanding How the Primary Junos OS Image with Dual-Root Partitioning Recovers on SRX Series Devices on page 69](#)
- *Installation and Upgrade Guide for Security Devices*

Reinstalling the Single-Root Partition Using `request system software add` Command

You cannot install a Junos OS Release 9.6 or earlier package on a system with dual-root partitioning using the Junos OS CLI or J-Web. An error will be returned if this is attempted.



NOTE: Junos OS Release 12.1X45 and later do not support single root partitioning.

You can install the Junos OS Release 9.6 (9.6R3 and 9.6R4 [only]) on a system with dual-root partitioning using `request system software add` command with `partition` option.

To reinstall the single-root partition:

1. Enter the `request system software add partition` command to install the previous Junos OS version (9.6R3 and 9.6R4):

```
user@host>request system software add partition
```

2. Reboot the device

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

The previous software version gets installed after rebooting the device.



NOTE: Using the `request system software add` CLI command with the `partition` option to install Junos OS Release 9.6 (9.6R3 and 9.6R4) reformats the media with single-root partitioning. This process erases the dual-root partitioning scheme from the system, so the benefits of dual-root partitioning will no longer be available.

Related Documentation

- [Dual-Root Partitioning Scheme Overview on page 19](#)
- [Junos OS Release 9.6 or Earlier Installation on SRX Series Devices with Dual-Root Partitioning on page 71](#)
- [Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 72](#)
- *Installation and Upgrade Guide for Security Devices*

CHAPTER 9

Boot Loaders and Boot Devices

- [Installing Junos OS from the Boot Loader Using a USB Storage Device on an SRX Series Device on page 77](#)
- [Upgrading the Boot Loader on SRX Series Devices on page 77](#)

Installing Junos OS from the Boot Loader Using a USB Storage Device on an SRX Series Device

To install Junos OS Release 10.0 or later from the boot loader using a USB storage device:

1. Format a USB storage device in MS-DOS format.
2. Copy the Junos OS image onto the USB storage device.
3. Plug the USB storage device into the SRX Series device.
4. Stop the device at the loader prompt and issue the following command:

```
loader> install file:///<image-path-on-usb>
```

An example of a command is as follows:

```
loader> install file:///junos-srxsme-10.0R2-domestic.tgz
```

This formats the internal media and installs the new Junos OS image on the media with dual-root partitioning.

5. Once the system boots up with Junos OS Release 10.0 or later, upgrade the U-boot and boot loader immediately.

Related Documentation

- [Understanding Junos OS Upgrades for SRX Series Devices on page 10](#)
- [Installing Junos OS Upgrades from a Remote Server on the SRX Series Devices on page 63](#)
- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 55](#)
- [*Installation and Upgrade Guide for Security Devices*](#)

Upgrading the Boot Loader on SRX Series Devices

To upgrade the boot loader to the latest version:

1. Upgrade to Junos OS Release 10.0 or later (with or without dual-root support enabled).

The Junos OS 10.0 image contains the latest boot loader binaries in this path:
/boot/uboot, /boot/loader.

2. Enter the shell prompt using the **start shell** command.
3. Run the following command from the shell prompt:

```
bootupgrade -u /boot/uboot -l /boot/loader
```



NOTE: For the new version to take effect, you should reboot the system after upgrading the boot loader.

To verify the boot loader version on the SRX Series device, enter the **show chassis routing-engine bios** command.

```
user@host> show chassis routing-engine bios  
Routing Engine BIOS Version: 1.5
```

The command output displays the boot loader version.



NOTE: You can use the following commands to upgrade U-Boot or perform cyclic redundancy check (CRC):

- **bootupgrade -s -u** – To upgrade the secondary boot loader.
- **bootupgrade -c u-boot** – To check CRC of the boot loader.
- **bootupgrade -s -c u-boot** – To check CRC for the secondary boot loader.
- **bootupgrade -c loader** – To check CRC for the loader on boot loader.

Related Documentation

- [Understanding Junos OS Upgrades for SRX Series Devices on page 10](#)
- [Example: Configuring Boot Devices for SRX Series Devices on page 95](#)
- [Junos OS Upgrade Methods on the SRX Series Devices on page 12](#)
- *Installation and Upgrade Guide for Security Devices*

CHAPTER 10

Software Downgrade

- [Example: Downgrading Junos OS on SRX Series Devices on page 79](#)
- [Example: Downgrading Junos OS on J Series Devices on page 81](#)

Example: Downgrading Junos OS on SRX Series Devices

This example shows how to downgrade Junos OS on the SRX Series devices.

- [Requirements on page 79](#)
- [Overview on page 79](#)
- [Configuration on page 79](#)
- [Verification on page 80](#)

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

When you upgrade your software, the device creates a backup image of the software that was previously installed in addition to installing the requested software upgrade.

To downgrade the software, you can revert to the previous image using the backup image. You can use this method to downgrade to only the software release that was installed on the device before the current release. To downgrade to an earlier version, follow the procedure for upgrading, using the software image labeled with the appropriate release. This example returns software to the previous Junos OS version.

Configuration

CLI Quick Configuration

To quickly downgrade Junos OS on SRX Series devices, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

From operational mode, enter:

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

GUI Step-by-Step Procedure

To downgrade Junos OS on SRX Series devices:

1. In the J-Web user interface, select **Maintain>Software>Downgrade**. The image of the previous version (if any) appears 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. Click **Maintain>Reboot** from the J-Web user interface to reboot the device.



NOTE: To downgrade to an earlier version, follow the procedure for upgrading, using the software image labeled with the appropriate release.

4. Click **OK** to check your configuration and save it as a candidate configuration.
5. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To downgrade Junos OS on SRX Series devices:

1. From operational mode, return to the previous Junos OS version.

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

2. Reboot the device.

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

The device is now running the previous version of Junos OS. To downgrade to an earlier version, follow the procedure for upgrading, using the software image labeled with the appropriate release.

Results

From configuration mode, confirm your configuration by entering the **show system** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying the Junos OS Downgrade Installation

Purpose	Verify that the Junos OS downgrade was installed.
Action	From operational mode, enter the show system command.
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring Boot Devices for SRX Series Devices on page 95 • Junos OS Upgrade Methods on the SRX Series Devices on page 12 • Example: Installing Junos OS Upgrades on SRX Series Devices on page 55 • Example: Rebooting SRX Series Devices on page 153 • <i>Installation and Upgrade Guide for Security Devices</i>

Example: Downgrading Junos OS on J Series Devices

This example shows how to downgrade Junos OS on J Series devices.

- [Requirements on page 81](#)
- [Overview on page 81](#)
- [Configuration on page 81](#)
- [Verification on page 83](#)

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview



NOTE: This procedure applies only to downgrading from one Junos OS software release to another or from one Junos OS services release to another.

When you upgrade your software, the device creates a backup image of the software that was previously installed in addition to installing the requested software upgrade.

To downgrade the software, you can revert to the previous image using the backup image. You can use this method to downgrade to only the software release that was installed on the device before the current release. To downgrade to an earlier version, follow the procedure for upgrading, using the software image labeled with the appropriate release.

Configuration

CLI Quick Configuration	To quickly downgrade Junos OS on J Series devices, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.
--------------------------------	---

From operational mode, enter:

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

GUI Step-by-Step Procedure

To downgrade Junos OS on J Series devices:

1. In the J-Web user interface, select **Maintain>Software>Downgrade**. The image of the previous version (if any) appears 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. Click **Maintain>Reboot** from the J-Web user interface to reboot the device.



NOTE: 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, follow the procedure for upgrading, using the software image labeled with the appropriate release.

4. Click **OK** to check your configuration and save it as a candidate configuration.
5. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To downgrade Junos OS on J Series devices:

1. From operational mode, return to the previous Junos OS version.

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

2. Reboot the device.

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

The device is now running the previous version of Junos OS. To downgrade to an earlier version, follow the procedure for upgrading, using the software image labeled with the appropriate release.

Results

From configuration mode, confirm your configuration by entering the **show system** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying the Junos OS Downgrade Installation

Purpose Verify that the Junos OS downgrade was installed.

Action From operational mode, enter the **show system** command.

- Related Documentation**
- [Preparing Your J Series Services Router for Junos OS Upgrades on page 45](#)
 - [Example: Installing Junos OS Upgrades on J Series Devices on page 57](#)
 - [Example: Rebooting J Series Devices on page 155](#)
 - [Example: Halting J Series Devices on page 159](#)
 - *Installation and Upgrade Guide for Security Devices*

PART 3

Configuration

- [Autoinstallation on page 87](#)
- [Backup and Snapshot Configuration Files on page 91](#)
- [Boot Loaders and Boot Devices on page 95](#)
- [Configuration Statements on page 101](#)

CHAPTER 11

Autoinstallation

- [Example: Configuring Autoinstallation on page 87](#)

Example: Configuring Autoinstallation

This example shows how to configure a device for autoinstallation.

- [Requirements on page 87](#)
- [Overview on page 88](#)
- [Configuration on page 88](#)
- [Verification on page 89](#)

Requirements

Before you begin:

- Configure a DHCP server on your network to meet your network requirements. You can configure a device to operate as a DHCP server. See *Example: Configuring the Device as a DHCP Server*.
- Create one of the following configuration files, and store it on a TFTP server in the network:
 - A host-specific file with the name **hostname.conf** for each device undergoing autoinstallation. Replace **hostname** with the name of a device. The **hostname.conf** file typically contains all the configuration information necessary for the device with this hostname.
 - A default configuration file named **router.conf** with the minimum configuration necessary to enable you to telnet into the new device for further configuration.
- Physically attach the device to the network using one or more of the following interface types:
 - Fast Ethernet
 - Gigabit Ethernet
 - Serial with HDLC encapsulation

Overview

No configuration is required on a device on which you are performing autoinstallation, because it is an automated process. However, to simplify the process, you can specify one or more interfaces, protocols, and configuration servers to be used for autoinstallation.

The device uses these protocols to send a request for an IP address for the interface.

- BOOTP—Sends requests over all interfaces.
- RARP—Sends requests over Ethernet interfaces.

Configuration

CLI Quick Configuration To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set system autoinstallation configuration-servers tftp://tftpconfig.sp.com
set system autoinstallation interfaces ge-0/0/0 bootp rarp
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure a device for autoinstallation:

1. Enable autoinstallation and specify the URL address of one or more servers from which to obtain configuration files.

```
[edit system]
user@host# set autoinstallation configuration-servers tftp://tftpconfig.sp.com
```



NOTE: You can also use an FTP address, for example, `ftp://user:password@sftpconfig.sp.com`.

2. Configure one or more Ethernet or serial interfaces to perform autoinstallation, and configure one or two procurement protocols for each interface.

```
[edit system]
user@host# set autoinstallation interfaces ge-0/0/0 bootp rarp
```

Results From configuration mode, confirm your configuration by entering the **show system autoinstallation status** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system autoinstallation status
```

```
Autoinstallation status:
Master state: Active
```

```

Last committed file: None
Configuration server of last committed file: 10.25.100.1
Interface:
  Name: ge-0/0/0
  State: Configuration Acquisition
  Acquired:
    Address: 192.168.124.75
    Hostname: host-ge-000
    Hostname source: DNS
    Configuration filename: router-ge-000.conf
    Configuration filename server: 10.25.100.3
  Address acquisition:
    Protocol: BOOTP Client
    Acquired address: None
    Protocol: RARP Client
    Acquired address: None

```

If you are done configuring the device, enter **commit** from configuration mode.



NOTE: When there is a user-specified configuration for a particular interface, the factory default for that interface should be deleted. Having two configurations for the same device might lead to errors. For example, if PPP encapsulation is set on a T1 interface through user configuration while the factory default configuration configures CISCO HDLC on the same interface, then the interface might not come up and the following error will be logged in the message file: “DCD_CONFIG_WRITE_FAILED failed.”

Verification

Confirm that the configuration is working properly.

Verifying Autoinstallation

Purpose	Verify that the device has been configured for autoinstallation.
Action	From operational mode, enter the show system autoinstallation status command. The output shows the settings configured for autoinstallation. Verify that the values displayed are correct for the device when it is deployed on the network.
Related Documentation	<ul style="list-style-type: none"> • Autoinstallation Overview on page 27 • <i>Automatic Installation of Configuration Files (J Series Routers and SRX Services Gateway)</i> • <i>Installation and Upgrade Guide for Security Devices</i>

Backup and Snapshot Configuration Files

- [Configuring a Boot Device to Receive Junos OS Failure Memory Snapshots in J Series Devices on page 91](#)
- [Configuring External CompactFlash on SRX650 Devices on page 92](#)

Configuring a Boot Device to Receive Junos OS Failure Memory Snapshots in J Series Devices

Use the **set system dump-device** command to specify the medium to use for the device to store system software failure memory snapshots. In this way, when the operating system fails, if you have specified a system dump device in the configuration, the operating system preserves a snapshot of the state of the device when it failed.

After you reboot the system, the dump device is checked for a snapshot as part of the operating system boot process. If a snapshot is found, it is written to the crash dump directory on the device (**/var/crash**). The customer support team can examine this memory snapshot to help determine the cause of the system software failure.



NOTE: If the swap partition on the dump device medium is not large enough for a system memory snapshot, either a partial snapshot or no snapshot is written into the crash dump directory.

From operational mode, enter the **set system dump-device** command with the following syntax:

```
user@host> set system dump-device boot-device | compact-flash |
removable-compact-flash | usb
```

[Table 16 on page 91](#) describes the **set system dump-device** command options.

Table 16: CLI set system dump-device Command Options

Option	Description
boot-device	Uses whatever device was booted from as the system software failure memory snapshot device.
compact-flash	Uses the internal CompactFlash (CF) card as the system software failure memory snapshot device.

Table 16: CLI set system dump-device Command Options (*continued*)

Option	Description
removable-compact-flash	Uses the CF card on the rear of the device (J2320 and J2350 only) as the system software failure memory snapshot device.
usb	Uses the device attached to the USB port as the system software failure memory snapshot device.

**Related
Documentation**

- [Preparing Your J Series Services Router for Junos OS Upgrades on page 45](#)
- [Example: Configuring Boot Devices for J Series Devices on page 98](#)
- [Example: Rebooting J Series Devices on page 155](#)
- [Example: Halting J Series Devices on page 159](#)
- *Installation and Upgrade Guide for Security Devices*

Configuring External CompactFlash on SRX650 Devices

The SRX650 Services Gateway includes the following 2 GB CompactFlash (CF) storage device:

- The Services and Routing Engine (SRE) contains a hot-pluggable external CF storage device used to upload and download files.
- The chassis contains an internal CF used to store the operating system.

By default, only the internal CF is enabled and an option to take a snapshot of the configuration from the internal CF to the external CF is not supported. This can be done only by using a USB storage device.

To take a snapshot of the configuration from the external CF:

1. Take a snapshot from the internal CF to a USB storage device using the **request system snapshot media usb** command.
2. Reboot the device from the USB storage device using the **request system reboot media usb** command.
3. Go to the U-boot prompt.
4. Stop at U-boot and set the following variables:

```
set ext.cf.pref 1
save
reset
```
5. Once the system is booted from the USB storage device, take a snapshot from the external CF using the **request system snapshot media external** command.



NOTE: Once the snapshot is taken on the external CF, we recommend that you set the `ext.cf.pref` to 0 at the U-boot prompt.

**Related
Documentation**

- [Understanding Junos OS Upgrades for SRX Series Devices on page 10](#)
- [Preparing Your SRX Series Device for Junos OS Upgrades on page 44](#)
- [Junos OS Upgrade Methods on the SRX Series Devices on page 12](#)
- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 55](#)
- [Installing Junos OS Using a USB Flash Drive on SRX Series Devices on page 62](#)
- *Installation and Upgrade Guide for Security Devices*

Boot Loaders and Boot Devices

- [Example: Configuring Boot Devices for SRX Series Devices on page 95](#)
- [Example: Configuring Boot Devices for J Series Devices on page 98](#)

Example: Configuring Boot Devices for SRX Series Devices

This example shows how to configure a boot device.

- [Requirements on page 95](#)
- [Overview on page 95](#)
- [Configuration on page 96](#)
- [Verification on page 97](#)

Requirements

Before you begin, ensure that the backup device has a storage capacity of at least 1 GB. See [“Preparing Your SRX Series Device for Junos OS Upgrades” on page 44](#).

Overview

You can configure a boot device to replace the primary boot device on your SRX Series device or to act as a backup boot device. Use either the J-Web user interface or the CLI to take a snapshot of the configuration currently running on the device, or of the original factory configuration and a rescue configuration, and save it to an alternate medium.



NOTE: For media redundancy, we recommend that you keep a secondary storage medium attached to the SRX Series device and updated at all times.

If the primary storage medium becomes corrupted and no backup medium is in place, you can recover the primary internal media from the TFTP installation.

You can also configure a boot device to store snapshots of software failures for use in troubleshooting.



NOTE: You cannot copy software to the active boot device.



NOTE: After a boot device is created with the default factory configuration, it can operate only in an internal media slot.

This example configures a boot device to back up the currently running and active file system partitions by rebooting from internal media and including only files shipped from the factory.

Configuration

CLI Quick Configuration To quickly configure a boot device, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

From operational mode, enter:

```
user@host> request system snapshot partition media internal factory
```

GUI Step-by-Step Procedure To configure a boot device:

1. In the J-Web user interface, select **Maintain>Snapshot**.
2. On the Snapshot page, specify the boot device to copy the snapshot to. From the Target Media list, select the **internal** boot device.
3. Select the Factory check box to copy only default files that were loaded on the internal media when it was shipped from the factory, plus the rescue configuration if one has been set.
4. Select the Partition check box to partition the medium that you are copying the snapshot to. This process is usually necessary for boot devices that do not already have software installed on them.
5. Click **Snapshot**.
6. Click **OK** to check your configuration and save it as a candidate configuration.
7. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure a boot device:

From operational mode, create a boot device from the internal media including only files shipped from the factory that will be used to back up the currently running and active file system partitions.

```
user@host> request system snapshot partition media internal factory
```

Results From configuration mode, confirm your configuration by entering the **show system snapshot media internal** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host> show system snapshot media internal
```

```
Information for snapshot on      internal (/dev/ad0s1a) (backup)
Creation date: Oct 9 13:30:06 2009
JUNOS version on snapshot:
  junos : 10.0B3.10-domestic
Information for snapshot on      internal (/dev/ad0s2a) (primary)
Creation date: Jan 6 15:45:35 2010
JUNOS version on snapshot:
  junos : 10.2-20091229.2-domestic
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying the Snapshot Information

Purpose Verify that the snapshot information for both root partitions on SRX Series devices were configured.

Action From operational mode, enter the **show system snapshot media** command.

The command output displays the snapshot creation time and Junos OS Release version on a media for both the primary and backup roots.



NOTE: With the dual-root partitioning scheme, performing a snapshot to a USB storage device that is less than 1 GB is not supported.



NOTE: You can use the **show system snapshot media internal** command to determine the partitioning scheme present on the internal media. Information for only one root is displayed for single-root partitioning, whereas information for both roots is displayed for dual-root partitioning.



NOTE: Any removable media that has been formatted with dual-root partitioning will not be recognized correctly by the **show system snapshot** CLI command on systems that have single-root partitioning. Intermixing dual-root and single-root formatted media on the same system is strongly discouraged.

Related Documentation

- [Upgrading the Boot Loader on SRX Series Devices on page 77](#)
- [Junos OS Upgrade Methods on the SRX Series Devices on page 12](#)
- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 55](#)

- [Example: Rebooting SRX Series Devices on page 153](#)
- *Installation and Upgrade Guide for Security Devices*

Example: Configuring Boot Devices for J Series Devices

This example shows how to configure a boot device.

- [Requirements on page 98](#)
- [Overview on page 98](#)
- [Configuration on page 99](#)
- [Verification on page 100](#)

Requirements

Before you begin, ensure that the backup device has a storage capacity of at least 256 MB. See [“Preparing Your J Series Services Router for Junos OS Upgrades” on page 45](#).

Overview

You can configure a boot device to replace the primary boot device on your J Series device or to act as a backup boot device. Use either the J-Web user interface or the CLI to take a snapshot of the configuration currently running on the device, or of the original factory configuration and a rescue configuration, and save it to an alternate medium.



.....

NOTE: For media redundancy, we recommend that you keep a secondary storage medium attached to the J Series device and updated at all times.

.....

If the primary storage medium becomes corrupted and no backup medium is in place, you can recover the primary CF card from a special software image. You can also configure a boot device to store snapshots of software failures, for use in troubleshooting.

.....



.....

NOTE:

- You cannot copy software to the active boot device.
 - After a boot device is created with the default factory configuration, it can operate only in an internal CF slot.
 - After the boot device is created as an internal CF, it can operate only in an internal CF slot.
-

This example configures a boot device to copy the software snapshot to the device connected to the USB port.

Configuration

CLI Quick Configuration To quickly configure a boot device, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

From operational mode, enter:

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

GUI Step-by-Step Procedure To configure a boot device:

1. In the J-Web user interface, select **Maintain>Snapshot**.
2. On the Snapshot page, in the Target Media field, specify **usb** as the boot device to copy the snapshot to.
3. Click **Snapshot**.
4. Click **OK** to check your configuration and save it as a candidate configuration.
5. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure a boot device:

From operational mode, create a boot device on an alternate medium to replace the primary boot device or to serve as a backup.

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

Results From configuration mode, confirm your configuration by entering the **show system snapshot media usb** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

For USB:

```
user@host> show system snapshot media usb
Information for snapshot on      usb (/dev/dals1a) (primary)
  Creation date: Jul 24 16:16:01 2009
  JUNOS version on snapshot:
  junos   : 10.0I20090723_1017-domestic
Information for snapshot on      usb (/dev/dals2a) (backup)
  Creation date: Jul 24 16:17:13 2009
  JUNOS version on snapshot:
  junos   : 10.0I20090724_0719-domestic
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying the Snapshot Information

Purpose Verify that the snapshot information was configured.

Action From operational mode, enter the **show system snapshot media** command.

- Related Documentation**
- [Preparing Your J Series Services Router for Junos OS Upgrades on page 45](#)
 - [Configuring a Boot Device to Receive Junos OS Failure Memory Snapshots in J Series Devices on page 91](#)
 - [Example: Rebooting J Series Devices on page 155](#)
 - [Example: Halting J Series Devices on page 159](#)
 - *Installation and Upgrade Guide for Security Devices*

Configuration Statements

- [System Configuration Statement Hierarchy on page 101](#)
- [autoinstallation on page 132](#)
- [configuration-servers on page 133](#)
- [interfaces \(Autoinstallation\) on page 134](#)
- [license on page 135](#)
- [usb on page 137](#)

System Configuration Statement Hierarchy

Use the statements in the **system** configuration hierarchy to configure system management functions including addresses of the Domain Name System (DNS) servers; device's hostname, address, and domain name; health monitoring; interface filtering; properties of the device's auxiliary and console ports; security profiles for logical systems; time zones and Network Time Protocol (NTP) properties; trace options; and user login accounts, including user authentication and the root-level user account. Statement descriptions that are exclusive to the J Series and SRX Series devices running Junos OS are described in this section.

```
system {
  accounting {
    destination {
      radius {
        server server-address {
          accounting-port port-number;
          max-outstanding-requests number;
          port number;
          retry number;
          secret password;
          source-address address;
          timeout seconds;
        }
      }
    }
  }
  tacplus {
    server server-address {
      port port-number;
      secret password;
      single-connection;
      source-address source-address;
    }
  }
}
```

```
        timeout seconds;
    }
}
events [change-log interactive-commands login];
traceoptions {
    file {
        filename;
        files number;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
}
}
allow-v4mapped-packets;
archival {
    configuration {
        archive-sites url {
            password password;
        }
        transfer-interval interval;
        transfer-on-commit;
    }
}
arp {
    aging-timer minutes;
    gratuitous-arp-delay seconds;
    gratuitous-arp-on-ifup;
    interfaces {
        interface name {
            aging-timer minutes;
        }
    }
    passive-learning;
    purging;
}
authentication-order [password radius tacplus];
auto-configuration {
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        level (all | error | info | notice | verbose | warning);
        no-remote-trace;
    }
}
}
auto-snapshot;
autoinstallation {
    configuration-servers {
```



```

    url {
        password password;
    }
}
interfaces {
    interface-name {
        bootp;
        rarp;
    }
}
usb {
    disable;
}
}
auto-snapshot;
backup-router {
    address;
    destination [network];
}
commit {
    server {
        commit-interval seconds;
        days-to-keep-error-logs days;
        maximum-aggregate-pool number;
        maximum entries number;
        traceoptions {
            file {
                filename;
                files number;
                microsecond-stamp;
                size maximum-file-size;
                (world-readable | no-world-readable);
            }
            flag flag;
            no-remote-trace;
        }
    }
    synchronize;
}
compress-configuration-files;
default-address-selection;
diag-port-authentication {
    encrypted-password passsword;
    plain-text-password;
}
domain-name domain-name;
domain-search [domain-list];
do-not-disable-ip6op-ondad;
dump-device (boot-device | compact-flash | usb);
dynamic-profile-options {
    versioning;
}
encrypt-configuration-files;
extensions {
    providers {
        provider-id {

```

```
        license-type license deployment-scope [deployments];
    }
}
resource-limits {
    package package-name {
        resources {
            cpu {
                priority number;
                time seconds;
            }
            file {
                core-size bytes;
                open number;
                size bytes;
            }
            memory {
                data-size mbytes;
                locked-in mbytes;
                resident-set-size mbytes;
                socket-buffers mbytes;
                stack-size mbytes;
            }
        }
    }
}
process process-ui-name {
    resources {
        cpu {
            priority number;
            time seconds;
        }
        file {
            core-size bytes;
            open number;
            size bytes;
        }
        memory {
            data-size mbytes;
            locked-in mbytes;
            resident-set-size mbytes;
            socket-buffers mbytes;
            stack-size mbytes;
        }
    }
}
}
}
fips {
    level (0 | 1 | 2 | 3 | 4);
}
host-name hostname;
inet6-backup-router {
    address;
    destination destination;
}
internet-options {
    icmpv4-rate-limit {
```

```

    bucket-size seconds;
    packet-rate packets-per-second;
}
icmpv6-rate-limit {
    bucket-size seconds;
    packet-rate packets-per-second;
}
(ipip-path-mtu-discovery | no-ipip-path-mtu-discovery);
ipv6-duplicate-addr-detection-transmits number;
(ipv6-path-mtu-discovery | no-ipv6-path-mtu-discovery);
ipv6-path-mtu-discovery-timeout minutes;
no-tcp-reset (drop-all-tcp | drop-tcp-with-syn-only);
no-tcp-rfc1323;
no-tcp-rfc1323-paws;
(path-mtu-discovery | no-path-mtu-discovery);
source-port upper-limit upper-limit;
(source-quench | no-source-quench);
tcp-drop-synfin-set;
tcp-mss bytes;
}
kernel-replication;
license {
    autoupdate {
        url url;
        password password;
    }
    renew {
        before-expiration number;
        interval interval-hours;
    }
    traceoptions {
        file {
            filename ;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
    }
}
location {
    altitude feet;
    building name;
    country-code code;
    floor number;
    hcoord horizontal-coordinate;
    lata service-area;
    latitude degrees;
    longitude degrees;
    npa-nxx number;
    postal-code postal-code;
    rack number;
    vcoord vertical-coordinate;
}

```

```
login {
    announcement text;
    class class-name {
        access-end hh:mm;
        access-start hh:mm;
        allow-commands regular-expression;
        allow-configuration regular-expression;
        allow-configuration-regexps [regular-expression];
        allowed-days [day];
        deny-commands regular-expression;
        deny-configuration regular-expression;
        deny-configuration-regexps [regular-expression];
        idle-timeout minutes;
        logical-system logical-system;
        login-alarms;
        login-script script;
        login-tip;
        permissions [permissions ];
        security-role (audit-administrator | crypto-administrator | ids-administrator |
            security-administrator);
    }
    deny-sources {
        address [address-or-hostname];
    }
    message text;
}
password {
    change-type (character-set | set-transitions);
    format (des | md5 | sha1);
    maximum-length length;
    minimum-changes number;
    minimum-length length;
}
retry-options {
    backoff-factor seconds;
    backoff-threshold number;
    lockout-period time;
    maximum-time seconds;
    minimum-time seconds;
    tries-before-disconnect number;
}
user username {
    authentication {
        encrypted-password password;
        load-key-file url;
        plain-text-password;
        ssh-dsa public-key;
        ssh-rsa public-key;
    }
    class class-name;
    full-name complete-name;
    uid uid-value;
}
}
max-configuration-rollback number;
max-configurations-on-flash number;
```

```

mirror-flash-on-disk;
name-server ip-address;
nd-maxmcast-solicit value;
nd-retransmit-timer value;
no-compress-configuration-files;
no-debugger-on-alt-break;
no-multicast-echo;
no-neighbor-learn;
no-ping-record-route;
no-ping-time-stamp;
no-redirects;
no-saved-core-context;
ntp {
    authentication-key key-number {
        type md5;
        value password;
    }
    boot-server address;
    broadcast broadcast-address {
        key key;
        ttl value;
        version version;
    }
    broadcast-client;
    multicast-client {
        address;
    }
    peer peer-address {
        key key;
        prefer;
        version version;
    }
    server server-address {
        key key;
        prefer;
        version version;
    }
    source-address source-address;
    trusted-key [key-number];
}
pic-console-authentication {
    encrypted-password password;
    plain-text-password;
}
ports {
    auxiliary {
        disable;
        insecure;
        type (ansi | small-xterm | vt100 | xterm);
    }
    console {
        disable;
        insecure;
        log-out-on-disconnect;
        type (ansi | small-xterm | vt100 | xterm);
    }
}

```

```
}
processes {
  802.1x-protocol-daemon {
    command binary-file-path;
    disable;
  }
  adaptive-services {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
  }
  alarm-control {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
  }
  application-identification {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
  }
  application-security {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
  }
  audit-process {
    command binary-file-path;
    disable;
  }
  auto-configuration {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
  }
  bootp {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
  }
  chassis-control {
    disable;
    failover alternate-media;
  }
  class-of-service {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
  }
  craft-control {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
  }
  database-replication {
    command binary-file-path;
```

```

    disable;
    failover (alternate-media | other-routing-engine);
}
datapath-trace-service {
    disable;
    traceoptions {
        file {
            filename ;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        level (all | error | info | notice | verbose | warning);
        no-remote-trace;
    }
}
dhcp {
    command binary-file-path;
    disable;
}
dhcp-service {
    disable;
    failover (alternate-media | other-routing-engine);
    interface-traceoptions {
        file {
            filename ;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        level (all | error | info | notice | verbose | warning);
        no-remote-trace;
    }
    traceoptions {
        file {
            filename ;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        level (all | error | info | notice | verbose | warning);
        no-remote-trace;
    }
}
dialer-services {
    disable;
    traceoptions {
        file {
            filename;
            files number;

```

```
        match regular-expression;  
        size maximum-file-size;  
        (world-readable | no-world-readable);  
    }  
    flag flag;  
    no-remote-trace;  
}  
}  
diameter-service {  
    disable;  
    traceoptions {  
        file {  
            filename;  
            files number;  
            match regular-expression;  
            size maximum-file-size;  
            (world-readable | no-world-readable);  
        }  
        flag flag;  
        level (all | error | info | notice | verbose | warning);  
        no-remote-trace;  
    }  
}  
}  
disk-monitoring {  
    command binary-file-path;  
    disable;  
}  
dynamic-flow-capture {  
    command binary-file-path;  
    disable;  
}  
ecc-error-logging {  
    command binary-file-path;  
    disable;  
}  
ethernet-connectivity-fault-management {  
    command binary-file-path;  
    disable;  
    failover (alternate-media | other-routing-engine);  
}  
ethernet-link-fault-management {  
    command binary-file-path;  
    disable;  
}  
ethernet-switching {  
    command binary-file-path;  
    disable;  
}  
event-processing {  
    command binary-file-path;  
    disable;  
}  
fipsd {  
    command binary-file-path;  
    disable;  
    failover (alternate-media | other-routing-engine);
```



```

}
firewall {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
firewall-authentication-service {
    disable;
}
forwarding {
    command binary-file-path;
    disable;
}
general-authentication-service {
    disable;
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
    }
}
gprs-process {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
group-key-member {
    disable;
}
group-key-server {
    disable;
}
idp-policy {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
ilmi {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
inet-process {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
init {
    command binary-file-path;
    disable;
}

```

```
    failover (alternate-media | other-routing-engine);
}
interface-control {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
ipmi {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
ipsec-key-management {
    (disable | enable);
}
jsrp-service {
    disable;
}
jtasktest {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
kernel-replication {
    command binary-file-path;
    disable;
}
l2-learning {
    command binary-file-path;
    disable;
}
l2cpd-service {
    command binary-file-path;
    disable;
}
lACP {
    command binary-file-path;
    disable;
}
lldpd-service {
    command binary-file-path;
    disable;
}
logical-system-mux {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
logical-system-service {
    disable;
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
        }
    }
}
```

```

        (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
}
}
mib-process {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
mobile-ip {
    command binary-file-path;
    disable;
}
mountd-service {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
mspd {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
multicast-snooping {
    command binary-file-path;
    disable;
}
named-service {
    disable;
    failover (alternate-media | other-routing-engine);
}
neighbor-liveness {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
network-security {
    disable;
}
network-security-trace {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
nfsd-service {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
ntp {
    disable;
    failover (alternate-media | other-routing-engine);
}
ntpd-service {

```

```
    command binary-file-path;  
    disable;  
    failover (alternate-media | other-routing-engine);  
}  
peer-selection-service {  
    command binary-file-path;  
    disable;  
    failover (alternate-media | other-routing-engine);  
}  
periodic-packet-services {  
    command binary-file-path;  
    disable;  
    failover (alternate-media | other-routing-engine);  
}  
pgcp-service {  
    command binary-file-path;  
    disable;  
    failover (alternate-media | other-routing-engine);  
}  
pgm {  
    command binary-file-path;  
    disable;  
    failover (alternate-media | other-routing-engine);  
}  
pic-services-logging {  
    command binary-file-path;  
    disable;  
    failover (alternate-media | other-routing-engine);  
}  
ppp {  
    command binary-file-path;  
    disable;  
}  
pppoe {  
    command binary-file-path;  
    disable;  
}  
process-monitor {  
    disable;  
    traceoptions {  
        file {  
            filename;  
            files number;  
            match regular-expression;  
            size maximum-file-size;  
            (world-readable | no-world-readable);  
        }  
        flag flag;  
        level (all | error | info | notice | verbose | warning);  
        no-remote-trace;  
    }  
}  
profilerd {  
    command binary-file-path;  
    disable;  
    failover (alternate-media | other-routing-engine);
```

```

}
r2cp {
    command binary-file-path;
    disable;
}
redundancy-interface-process {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
remote-operations {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
resource-cleanup {
    disable;
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        level (all | error | info | notice | verbose | warning);
        no-remote-trace;
    }
}
routing {
    disable;
    failover (alternate-media | other-routing-engine);
}
sampling {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
sbc-configuration-process {
    disable;
    failover (alternate-media | other-routing-engine);
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
    }
}
sdk-service {
    disable;
}

```

```
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  level (all | error | info | notice | verbose | warning);
  no-remote-trace;
}
}
secure-neighbor-discovery {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
security-log {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
send {
  disable;
}
service-deployment {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
shm-rtssdbd {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
simple-mail-client-service {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
smtpd-service {
  disable;
}
snmp {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
static-subscribers {
  disable;
}
statistics-service {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
```

```

}
subscriber-management {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
subscriber-management-helper {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
system-health-management {
    disable;
}
tunnel-oamd {
    command binary-file-path;
    disable;
}
uac-service {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
usb-control {
    command binary-file-path;
    disable;
}
virtualization-service {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
vrrp {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
wan-acceleration {
    disable;
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
    }
}
watchdog {
    enable;
    disable;
    timeout value;
}

```

```
web-management {
  disable;
  failover (alternate media | other-routing-engine);
}
wireless-lan-service {
  disable;
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
  }
}
wireless-wan-service {
  disable;
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
  }
}
proxy {
  password password;
  port port-number;
  server url;
  username user-name;
}
radius-options {
  attributes {
    nas-ip-address nas-ip-address;
  }
  password-protocol mschap-v2;
}
radius-server server-address {
  accounting-port number;
  max-outstanding-requests number;
  port number;
  retry number;
  secret password;
  source-address source-address;
  timeout seconds;
}
root-authentication {
  encrypted-password password;
  load-key-file url;
```



```

plain-text-password;
ssh-dsa public-key {
    <from pattern-list>;
}
ssh-rsa public-key {
    <from pattern-list>;
}
}
saved-core-context;
saved-core-files number;
scripts {
    commit {
        allow-transients;
        direct-access;
        file filename {
            checksum (md5 | sha-256 | sha1);
            optional;
            refresh;
            refresh-from url;
            source url;
        }
        refresh;
        refresh-from url;
        traceoptions {
            file {
                filename;
                files number;
                size maximum-file-size;
                (world-readable | no-world-readable);
            }
            flag flag;
            no-remote-trace;
        }
    }
}
load-scripts-from-flash;
op {
    file filename {
        arguments name {
            description text;
        }
        checksum (md5 | sha-256 | sha1);
        command filename-alias;
        description cli-help-text;
        refresh;
        refresh-from url;
        source url;
    }
    no-allow-url;
    refresh;
    refresh-from url;
    traceoptions {
        file {
            filename;
            files number;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
    }
}

```

```
    }
    flag flag;
    no-remote-trace;
  }
}
security-profile security-profile-name {
  address-book {
    maximum amount;
    reserved amount;
  }
  appfw-profile {
    maximum amount;
    reserved amount;
  }
  appfw-rule {
    maximum amount;
    reserved amount;
  }
  appfw-rule-set {
    maximum amount;
    reserved amount;
  }
  auth-entry {
    maximum amount;
    reserved amount;
  }
  cpu {
    reserved percent;
  }
  dslite-software-initiator {
    maximum amount;
    reserved amount;
  }
  flow-gate {
    maximum amount;
    reserved amount;
  }
  flow-session {
    maximum amount;
    reserved amount;
  }
  idp-policy idp-policy-name;
  logical-system logical-system-name;
  nat-cone-binding {
    maximum amount;
    reserved amount;
  }
  nat-destination-pool {
    maximum amount;
    reserved amount;
  }
  nat-destination-rule {
    maximum amount;
    reserved amount;
  }
  nat-interface-port-ol {
```

```

        maximum amount;
        reserved amount;
    }
    nat-nopat-address {
        maximum amount;
        reserved amount;
    }
    nat-pat-address {
        maximum amount;
        reserved amount;
    }
    nat-pat-portnum {
        maximum amount
        reserved amount
    }
    nat-port-ol-ipnumber {
        maximum amount;
        reserved amount;
    }
    nat-rule-referenced-prefix {
        maximum amount;
        reserved amount;
    }
    nat-source-pool {
        maximum amount;
        reserved amount;
    }
    nat-source-rule {
        maximum amount;
        reserved amount;
    }
    nat-static-rule {
        maximum amount;
        reserved amount;
    }
    policy {
        maximum amount;
        reserved amount;
    }
    policy-with-count {
        maximum amount;
        reserved amount;
    }
    root-logical-system;
    scheduler {
        maximum amount;
        reserved amount;
    }
    zone {
        maximum amount;
        reserved amount;
    }
}
security-profile-resources {
    cpu-control;
    cpu-control-target percent;

```

```

}
services {
  database-replication {
    traceoptions {
      file {
        filename ;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
      }
      flag flag;
      no-remote-trace;
    }
  }
}
dhcp {
  boot-file filename;
  boot-server (address | hostname);
  default-lease-time (infinite | seconds);
  domain-name domain-name;
  domain-search dns-search-suffix;
  maximum-lease-time (infinite | seconds);
  name-server ip-address;
  next-server ip-address;
  option option-identifier-code array type-name [ type-values ] | byte 8-bit-value | flag
    (false | off | on | true) | integer signed-32-bit-value | ip-address address | short
    signed-16-bit-value | string text-string | unsigned-integer 32-bit-value |
    unsigned-short 16-bit-value);
  pool subnet-ip-address/mask {
    address-range {
      high address;
      low address;
    }
    boot-file filename;
    boot-server (address | hostname);
    default-lease-time (infinite | seconds);
    domain-name domain-name;
    domain-search dns-search-suffix;
    exclude-address ip-address;
    maximum-lease-time (infinite | seconds);
    name-server ip-address;
    next-server ip-address;
    option option-identifier-code array type-name [ type-values ] | byte 8-bit-value |
      flag (false | off | on | true) | integer signed-32-bit-value | ip-address address |
      short signed-16-bit-value | string text-string | unsigned-integer 32-bit-value |
      unsigned-short 16-bit-value);
    propagate-ppp-settings interface-name;
    propagate-settings interface-name;
    router ip-address;
    server-identifier dhcp-server;
    sip-server {
      address ip-address;
      name sip-server-name;
    }
    wins-server ip-address;
  }
}

```

```

propagate-ppp-settings interface-name;
propagate-settings interface-name;
router ip-address;
server-identifier dhcp-server;
sip-server {
    address ip-address;
    name sip-server-name;
}
static-binding mac-address;
traceoptions {
    file {
        filename ;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag flag;
    level (all | error | info | notice | verbose | warning);
    no-remote-trace;
}
wins-server ip-address;
}
dhcp-local-server {
    dhcpv6 {
        authentication {
            password password;
            username-include {
                circuit-type;
                client-id;
                delimiter delimiter-character;
                domain-name domain-name;
                interface-name;
                logical-system-name;
                relay-agent-interface-id;
                relay-agent-remote-id;
                relay-agent-subscriber-id;
                routing-instance-name;
                user-prefix user-prefix;
            }
        }
    }
    dynamic-profile {
        profile-name;
        aggregate-clients {
            merge;
            replace;
        }
        junos-default-profile;
        use-primary dynamic-profile-name;
    }
    group group-name {
        authentication {
            password password;
            username-include {
                circuit-type;
                client-id;

```

```
    delimiter delimiter-character;  
    domain-name domain-name;  
    interface-name;  
    logical-system-name;  
    relay-agent-interface-id;  
    relay-agent-remote-id;  
    relay-agent-subscriber-id;  
    routing-instance-name;  
    user-prefix user-prefix;  
  }  
}  
dynamic-profile {  
  profile-name;  
  aggregate-clients {  
    merge;  
    replace;  
  }  
  junos-default-profile;  
  use-primary dynamic-profile;  
}  
interface interface-name {  
  dynamic-profile {  
    profile-name;  
    aggregate-clients {  
      merge;  
      replace;  
    }  
    junos-default-profile;  
    use-primary dynamic-profile-name;  
  }  
  exclude;  
  overrides {  
    delegated-pool pool-name;  
    interface-client-limit number;  
    process-inform {  
      pool pool-name;  
    }  
    rapid-commit ;  
  }  
  service-profile service-profile-name  
  trace ;  
  upto interface-name;  
}  
liveness-detection {  
  failure-action {  
    clear-binding;  
    clear-binding-if-interface-up;  
    log-only;  
  }  
  method {  
    bfd {  
      detection-time {  
        threshold milliseconds;  
      }  
      holddown-interval interval;  
      minimum-interval milliseconds;
```

```

        minimum-receive-interval milliseconds;
        multiplier number;
        no-adaptation;
        session-mode (automatic | multihop | single-hop);
        transmit-interval {
            minimum-interval milliseconds;
            threshold milliseconds;
        }
        version (0 | 1 | automatic);
    }
}
overrides {
    delegated-pool pool-name;
    interface-client-limit number;
    process-inform {
        pool pool-name;
    }
    rapid-commit ;
}
reconfigure {
    attempts number;
    clear-on-abort;
    strict;
    timeout number;
    token token-name;
    trigger {
        radius-disconnect;
    }
}
service-profile service-profile-name;
}
liveness-detection {
    failure-action {
        clear-binding;
        clear-binding-if-interface-up;
        log-only;
    }
}
method {
    bfd {
        detection-time {
            threshold milliseconds;
        }
        holddown-interval interval;
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
        multiplier number;
        no-adaptation;
        session-mode (automatic | multihop | single-hop);
        transmit-interval {
            minimum-interval milliseconds;
            threshold milliseconds;
        }
        version (0 | 1 | automatic);
    }
}
overrides {

```

```
    delegated-pool pool-name;  
    interface-client-limit number;  
    process-inform {  
        pool pool-name;  
    }  
    rapid-commit ;  
}  
reconfigure {  
    attempts number;  
    clear-on-abort;  
    strict;  
    timeout number;  
    token token-name;  
    trigger {  
        radius-disconnect;  
    }  
}  
service-profile service-profile-name;  
}  
group group-name {  
    interface interface-name {  
        exclude;  
        upto upto-interface-name;  
    }  
}  
}  
dns {  
    dns-proxy {  
        cache hostname inet ip-address;  
        default-domain domain-name {  
            forwarders ip-address;  
        }  
        interface interface-name;  
        propagate-setting (enable | disable);  
        view view-name {  
            domain domain-name {  
                forwarders ip-address;  
            }  
            match-clients subnet-address;  
        }  
    }  
}  
dnssec {  
    disable;  
    dlv {  
        domain-name domain-name trusted-anchor trusted-anchor;  
    }  
    secure-domains domain-name;  
    trusted-keys (key dns-key | load-key-file url);  
    forwarders {  
        ip-address;  
    }  
    max-cache-ttl seconds;  
    max-ncache-ttl seconds;  
    traceoptions {  
        category {
```



```

        category-type;
    }
    debug-level level;
    file {
        filename;
        files number;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag flag;
    level (all | error | info | notice | verbose | warning);
    no-remote-trace;
}
}
dynamic-dns {
    client hostname {
        agent agent-name;
        interface interface-name;
        password server-password;
        server server-name;
        username user-name;
    }
}
finger {
    connection-limit number;
    rate-limit number;
}
ftp {
    connection-limit number;
    rate-limit number;
}
netconf {
    ssh {
        connection-limit number;
        port port-number;
        rate-limit number;
    }
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
        on-demand;
    }
}
outbound-ssh {
    client client-id {
        address {
            port port-number;
            retry number;
            timeout value;

```

```
    }
    device-id device-id;
    keep-alive {
        retry number;
        time-out value;
    }
    reconnect-strategy (in-order | sticky);
    secret secret;
    services {
        netconf;
    }
}
traceoptions {
    file {
        filename;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
}
}
service-deployment {
    local-certificate certificate-name;
    servers server-address {
        port port-number;
        security-options {
            ssl3;
            tls;
        }
        user user-name;
    }
}
source-address source-address;
traceoptions {
    file {
        filename;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
}
}
ssh {
    ciphers [cipher];
    client-alive-count-max number;
    client-alive-interval seconds;
    connection-limit number;
    hostkey-algorithm {
        (ssh-dss | no-ssh-dss);
        (ssh-ecdsa | no-ssh-ecdsa);
        (ssh-rsa | no-ssh-rsa);
    }
}
```

```

}
key-exchange [algorithm];
macs [algorithm];
max-sessions-per-connection number;
protocol-version {
    v1;
    v2;
}
rate-limit number;
root-login (allow | deny | deny-password);
(tcp-forwarding | no-tcp-forwarding);
}
subscriber-management {
    enforce-strict-scale-limit-license;
    gres-route-flush-delay;
    maintain-subscriber interface-delete;
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
    }
}
subscriber-management-helper {
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
    }
}
telnet {
    connection-limit number;
    rate-limit number;
}
web-management {
    control {
        max-threads number;
    }
    http {
        interface [interface-name];
        port port-number;
    }
    https {
        interface [interface-name];
        local-certificate name;
    }
}

```

```
    pki-local-certificate name;  
    port port-number;  
    system-generated-certificate;  
  }  
  management-url url;  
  session {  
    idle-timeout minutes;  
    session-limit number;  
  }  
  traceoptions {  
    file {  
      filename;  
      files number;  
      match regular-expression;  
      size maximum-file-size;  
      (world-readable | no-world-readable);  
    }  
    flag flag;  
    level (all | error | info | notice | verbose | warning);  
    no-remote-trace;  
  }  
}  
xnm-clear-text {  
  connection-limit number;  
  rate-limit number;  
}  
xnm-ssl {  
  connection-limit number;  
  local-certificate name;  
  rate-limit number;  
}  
}  
static-host-mapping hostname {  
  alias [host-name-alias];  
  inet [ip-address];  
  inet6 [ipv6-address];  
  sysid system-identifier;  
}  
syslog {  
  allow-duplicates;  
  archive {  
    binary-data;  
    files number;  
    size maximum-file-size;  
    (world-readable | no-world-readable);  
  }  
  console {  
    (any | facility) severity;  
  }  
  file filename {  
    allow-duplicates;  
    archive {  
      archive-sites url {  
        password password;  
      }  
      (binary-data | no-binary-data);  
    }  
  }  
}
```

```

    files number;
    size maximum-file-size;
    start-time "YYYY-MM-DD.hh:mm";
    transfer-interval minutes;
    (world-readable | no-world-readable);
  }
  structure-data {
    brief;
  }
  (any | facility) severity;
}
host (hostname | other-routing-engine) {
  (any | facility) severity;
}
log-rotate-frequency minutes;
source-address source-address;
time-format {
  millisecond;
  year;
}
user (username | *) {
  (any | facility) severity;
}
}
tacplus-options {
  (exclude-cmd-attribute | no-cmd-attribute-value);
  service-name service-name;
}
tacplus-server server-address {
  port port-number;
  secret password;
  single-connection;
  source-address source-address;
  timeout seconds;
}
time-zone (GMThour-offset | time-zone);
tracing {
  destination-override {
    syslog {
      host address;
    }
  }
}
}
use-imported-time-zones;
}

```

Related Documentation

- *Master Administrator for Logical Systems Feature Guide for Security Devices*
- *Firewall User Authentication Feature Guide for Security Devices*
- *Infranet Authentication Feature Guide for Security Devices*
- *Installation and Upgrade Guide for Security Devices*

autoinstallation

Syntax

```
autoinstallation {
  configuration-servers {
    url {
      password password;
    }
  }
  interfaces {
    interface-name {
      bootp;
      rarp;
    }
  }
  usb {
    disable;
  }
}
```

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the configuration for autoinstallation.

Options The remaining statements are explained separately.

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

Related Documentation

- [Example: Configuring Autoinstallation on page 87](#)
- *Installation and Upgrade Guide for Security Devices*

configuration-servers

Syntax	<pre>configuration-servers { url { password <i>password</i>; } }</pre>
Hierarchy Level	[edit system autoinstallation]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>Configure the URL address of a server from which the configuration files must be obtained.</p> <p>You can download a configuration file automatically from an FTP, Hypertext Transfer Protocol (HTTP), or Trivial FTP (TFTP) servers. Examples of URLs:</p> <ul style="list-style-type: none"> • tftp://hostname/path/filename • ftp://username:password@ftp.hostname.net • http://hostname/path/filename • http://username:password@httpconfig.sp.com
Options	<ul style="list-style-type: none"> • url—Specify the URL address of the server containing the configuration files. • password—Specify the password for authentication with the configuration server. Specifying a password in URLs and in the <i>password</i> option might result in commit failure. We recommend you to use the <i>password</i> option for specifying the password.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Installation and Upgrade Guide for Security Devices</i>

interfaces (Autoinstallation)

Syntax	<pre>interfaces { <i>interface-name</i> { bootp; rarp; } }</pre>
Hierarchy Level	[edit system autoinstallation]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the interface on which to perform autoinstallation. A request for an IP address is sent from the interface. Specify the IP address procurement protocol.
Options	<ul style="list-style-type: none">• bootp—Enables BOOTP or DHCP during autoinstallation.• rarp—Enables RARP during autoinstallation.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Configuring Autoinstallation on page 87• <i>Installation and Upgrade Guide for Security Devices</i>

license

Syntax	<pre> license { autoupdate { url <i>url</i>; password <i>password</i>; } renew { before-expiration <i>number</i>; interval <i>interval-hours</i>; } traceoptions { file { <i>filename</i> ; files <i>number</i>; match <i>regular-expression</i>; size <i>maximum-file-size</i>; (world-readable no-world-readable); } flag <i>flag</i>; no-remote-trace; } } </pre>
Hierarchy Level	[edit system]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify license information for the device.
Options	<ul style="list-style-type: none"> • autoupdate—Autoupdate license keys from license servers. <ul style="list-style-type: none"> • url—URL of a license server. • renew—License renewal lead time and checking interval. <ul style="list-style-type: none"> • before-expiration <i>number</i>—License renewal lead time before expiration in days. Range : 0 through 60 days • interval <i>interval-hours</i>—License checking interval in hours. Range : 1 through 336 hours • traceoptions—Set the trace options. <ul style="list-style-type: none"> • file—Configure the trace file information. <ul style="list-style-type: none"> • <i>filename</i>—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory /var/log. By default, the name of the file is the name of the process being traced. • files <i>number</i>— Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the **size *maximum file-size*** option.

Range : 2 through 1000 files

Default : 10 files

- **match *regular-expression***—Refine the output to include lines that contain the regular expression.
- **size *maximum-file-size***—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).

Range : 10 KB through 1 GB

Default : 128 KB

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files *number*** option.

- **(world-readable | no-world-readable)**— By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.
- **flag *flag***—Specify which tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags.
 - **all**—Trace all operations
 - **config**—Trace license configuration processing.
 - **events**—Trace licensing events and their processing.
 - **no-remote-trace**—Disable the remote tracing.

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

Related Documentation	<ul style="list-style-type: none">• Junos OS License Overview on page 33• <i>Installation and Upgrade Guide for Security Devices</i>
------------------------------	---

usb

Syntax	<pre>usb { disable; }</pre>
Hierarchy Level	[edit system autoinstallation]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Disable the USB autoinstallation process.
Options	disable —Disable the process.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Configuring Autoinstallation on page 87• <i>Installation and Upgrade Guide for Security Devices</i>

PART 4

Administration

- [Auto BIOS on page 141](#)
- [Licenses on page 143](#)
- [Software Stop and Restart on page 153](#)
- [Operational Commands on page 165](#)

CHAPTER 15

Auto BIOS

- [Disabling Auto BIOS Upgrade on SRX Series Devices on page 141](#)

Disabling Auto BIOS Upgrade on SRX Series Devices

The auto BIOS upgrade feature is enabled by default. You can disable the feature using the CLI in operational mode.

To disable the automatic upgrade of the BIOS on an SRX Series device, set the **chassis routing-engine bios** command.

```
user@host> set chassis routing-engine bios no-auto-upgrade
```



NOTE: The command disables automatic upgrade of the BIOS only during Junos OS upgrade or system boot-up. It does not disable automatic BIOS upgrade during loader installation.

Related Documentation

- [Understanding Junos OS Upgrades for SRX Series Devices on page 10](#)
- [Understanding Auto BIOS Upgrade Using Junos CLI on page 25](#)
- *Installation and Upgrade Guide for Security Devices*

CHAPTER 16

Licenses

- [Displaying License Keys on page 143](#)
- [Generating a License Key on page 144](#)
- [Downloading License Keys on page 144](#)
- [Saving License Keys on page 145](#)
- [Updating License Keys on page 146](#)
- [Example: Adding a New License Key on page 146](#)
- [Example: Deleting a License Key on page 150](#)

Displaying License Keys

To display license keys installed on the device:

1. In the J-Web interface, select **Maintain>Licenses**.
2. Under Installed Licenses, click **Display Keys** to display all the license keys installed on the device.

A screen displaying the license keys in text format appears. Multiple licenses are separated by a blank line.

Related Documentation

- [Junos OS Feature License Model Number for J Series Services Routers and SRX Series Services Gateways on page 36](#)
- [Generating a License Key on page 144](#)
- [Updating License Keys on page 146](#)
- [Saving License Keys on page 145](#)
- [Downloading License Keys on page 144](#)
- [Example: Adding a New License Key on page 146](#)
- [Example: Deleting a License Key on page 150](#)
- *Installation and Upgrade Guide for Security Devices*
- *Administration Guide for Security Devices*

Generating a License Key

To generate a license key:

1. Gather the authorization code that you received when you purchased your license as well as your device serial number.
2. Go to the Juniper Networks licensing page at:
<https://www.juniper.net/lcrs/generateLicense.do>
3. Enter the device serial number and authorization code in the webpage and click **Generate**. Depending on the type of license you purchased, you will receive one of the following responses:
 - License key—If you purchased a perpetual license, you will receive a license key from the licensing management system. You can enter this key directly into the system to activate the feature on your device.
 - License key entitlement—If you purchased a subscription-based license, you will receive a license key entitlement from the licensing management system. You can use this entitlement to validate your license on the Juniper Networks licensing server and download the feature license from the server to your device.

Related Documentation

- [Junos OS Feature License Model Number for J Series Services Routers and SRX Series Services Gateways on page 36](#)
- [Updating License Keys on page 146](#)
- [Saving License Keys on page 145](#)
- [Displaying License Keys on page 143](#)
- [Downloading License Keys on page 144](#)
- [Example: Adding a New License Key on page 146](#)
- [Example: Deleting a License Key on page 150](#)
- *Installation and Upgrade Guide for Security Devices*

Downloading License Keys

To download license keys installed on the device:

1. In the J-Web interface, select **Maintain>Licenses**.
2. Under Installed Licenses, click **Download Keys** to download all the license keys installed on the device to a single file.
3. Select **Save it to disk** and specify the file to which the license keys are to be written.

Related Documentation

- [Junos OS Feature License Model Number for J Series Services Routers and SRX Series Services Gateways on page 36](#)

- [Generating a License Key on page 144](#)
- [Updating License Keys on page 146](#)
- [Saving License Keys on page 145](#)
- [Displaying License Keys on page 143](#)
- [Example: Adding a New License Key on page 146](#)
- [Example: Deleting a License Key on page 150](#)
- *Installation and Upgrade Guide for Security Devices*

Saving License Keys

To save license keys installed on the device:

1. From operational mode, save the installed license keys to a file or URL.

```
user@host>request system license save filename | url
```

For example, the following command saves the installed license keys to a file named **license.config**:

```
request system license save ftp://user@host/license.conf
```

Related Documentation

- [Junos OS Feature License Model Number for J Series Services Routers and SRX Series Services Gateways on page 36](#)
- [Generating a License Key on page 144](#)
- [Updating License Keys on page 146](#)
- [Displaying License Keys on page 143](#)
- [Downloading License Keys on page 144](#)
- [Example: Adding a New License Key on page 146](#)
- [Example: Deleting a License Key on page 150](#)
- *Installation and Upgrade Guide for Security Devices*

Updating License Keys

To update a license key from the device:

1. From operational mode, do one of the following tasks:

- Update the license keys automatically.

```
user@host> request system license update
```



NOTE: The `request system license update` command will always use the default Juniper license server <https://ae1.juniper.net>

You can only use this command to update subscription-based licenses (such as UTM).

- Update the trial license keys automatically.

```
user@host> request system license update trial
```

Related Documentation

- [Junos OS Feature License Model Number for J Series Services Routers and SRX Series Services Gateways on page 36](#)
- [Generating a License Key on page 144](#)
- [Saving License Keys on page 145](#)
- [Displaying License Keys on page 143](#)
- [Downloading License Keys on page 144](#)
- [Example: Adding a New License Key on page 146](#)
- [Example: Deleting a License Key on page 150](#)
- *Installation and Upgrade Guide for Security Devices*

Example: Adding a New License Key

This example shows how to add a new license key.

- [Requirements on page 146](#)
- [Overview on page 147](#)
- [Configuration on page 147](#)
- [Verification on page 148](#)

Requirements

Before you begin, confirm that your Junos OS feature requires you to purchase, install, and manage a separate software license.

Overview

You can add a license key from a file or URL, from a terminal, or from the J-Web user interface. Use the **filename** option to activate a perpetual license directly on the device. (Most feature licenses are perpetual.) Use the **url** to send a subscription-based license key entitlement (such as UTM) to the Juniper Networks licensing server for authorization. If authorized, the server downloads the license to the device and activates it.

In this example, the file name is `bgp-reflection`.

Configuration

CLI Quick Configuration To quickly add a new license key, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

From operational mode, you can add a license key in either way:

- From a file or URL:

```
user@hostname> request system license add bgp-reflection
```
- From the terminal:

```
user@hostname> request system license add terminal
```

GUI Step-by-Step Procedure To add a new license key:

1. In the J-Web user interface, select **Maintain>Licenses**.
2. Under Installed Licenses, click **Add** to add a new license key.
3. Do one of the following, using a blank line to separate multiple license keys:
 - In the **License File URL** box, type the full URL to the destination file containing the license key to be added.
 - In the **License Key Text** box, paste the license key text, in plain-text format, for the license to be added.
4. Click **OK** to add the license key.



NOTE: If you added the SRX100 Memory Upgrade license, the device reboots immediately and comes back up as a high-memory device.

5. Click **OK** to check your configuration and save it as a candidate configuration.
6. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure To add a new license key:

1. From operational mode, add a license key in either way:
 - From a file or URL:

```
user@host> request system license add bgp-reflection
```

- From the terminal:

```
user@host>request system license add terminal
```

2. When prompted, enter the license key, separating multiple license keys with a blank line. If the license key you enter is invalid, an error is generated when you press Ctrl-D to exit license entry mode.



NOTE: If you added the SRX100 Memory Upgrade license, the device reboots immediately and comes back up as a high-memory device.

Results From operational mode, confirm your configuration by entering the **show system license** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@hostname> show system license
```

License usage:

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
bgp-reflection	0	1	0	permanent

Licenses installed:

License identifier: G03000002223

License version: 2

Valid for device: JN001875AB

Features:

bgp-reflection - Border Gateway Protocol route reflection
permanent

License identifier: G03000002225

License version: 2

Valid for device: JN001875AB

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

- [Verifying Installed Licenses on page 148](#)
- [Verifying License Usage on page 149](#)
- [Verifying Installed License Keys on page 149](#)

Verifying Installed Licenses

Purpose Verify that the expected licenses have been installed and are active on the device.

Action From operational mode, enter the **show system license** command.

The output shows a list of the licenses used and a list of the licenses installed on the device and when they expire.

Verifying License Usage

Purpose Verify that the licenses fully cover the feature configuration on the device.

Action From operational mode, enter the **show system license usage** command.

```
user@hostname> show system license usage
```

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
bgp-reflection	1	1	0	permanent

The output shows a list of the licenses installed on the device and how they are used.

Verifying Installed License Keys

Purpose Verify that the license keys were installed on the device.

Action From operational mode, enter the **show system license keys** command.

```
user@hostname> show system license keys
```

```
XXXXXXXXXX xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
      xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
      xxxxxx xxxxxx xxx
```

The output shows a list of the license keys installed on the device. Verify that each expected license key is present.

- Related Documentation**
- [Junos OS Feature License Model Number for J Series Services Routers and SRX Series Services Gateways on page 36](#)
 - [Generating a License Key on page 144](#)
 - [Updating License Keys on page 146](#)
 - [Saving License Keys on page 145](#)
 - [Displaying License Keys on page 143](#)
 - [Downloading License Keys on page 144](#)
 - [Example: Deleting a License Key on page 150](#)
 - *Installation and Upgrade Guide for Security Devices*

Example: Deleting a License Key

This example shows how to delete a license key.

- [Requirements on page 150](#)
- [Overview on page 150](#)
- [Configuration on page 150](#)
- [Verification on page 151](#)

Requirements

Before you delete a license key, confirm that it is no longer needed.

Overview

You can delete a license key from the CLI or J-Web user interface. In this example, the license ID is G03000002223.

Configuration

CLI Quick Configuration

To quickly delete a license key, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

```
user@host> request system license delete G03000002223
```

GUI Step-by-Step Procedure

To delete a license key:

1. In the J-Web user interface, select **Maintain>Licenses**.
2. Select the check box of the license or licenses you want to delete.
3. Click **Delete**.



NOTE: If you deleted the SRX100 Memory Upgrade license, the device reboots immediately and comes back up as a low-memory device.

4. Click **OK** to check your configuration and save it as a candidate configuration.
5. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

To delete a license key:

1. From operational mode, for each license, enter the following command and specify the license ID. You can delete only one license at a time.

```
user@host> request system license delete G03000002223
```



NOTE: If you deleted the SRX100 Memory Upgrade license, the device reboots immediately and comes back up as a low-memory device.

Results From configuration mode, confirm your deletion by entering the **show system license** command. The license key you deleted will be removed. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying Installed Licenses

Purpose Verify that the expected licenses have been removed from the device.

Action From operational mode, enter the **show system license** command.

Related Documentation

- [Junos OS Feature License Model Number for J Series Services Routers and SRX Series Services Gateways on page 36](#)
- [Generating a License Key on page 144](#)
- [Updating License Keys on page 146](#)
- [Saving License Keys on page 145](#)
- [Displaying License Keys on page 143](#)
- [Downloading License Keys on page 144](#)
- [Example: Adding a New License Key on page 146](#)
- *Installation and Upgrade Guide for Security Devices*

CHAPTER 17

Software Stop and Restart

- [Example: Rebooting SRX Series Devices on page 153](#)
- [Example: Rebooting J Series Devices on page 155](#)
- [Restarting the Chassis on SRX Series Devices on page 157](#)
- [Restarting the Chassis on J Series Devices on page 157](#)
- [Example: Halting SRX Series Devices on page 158](#)
- [Example: Halting J Series Devices on page 159](#)
- [Bringing Chassis Components Online and Offline on SRX Series Devices on page 161](#)
- [Bringing Chassis Components Online and Offline on J Series Devices on page 162](#)

Example: Rebooting SRX Series Devices

This example shows how to reboot a device.

- [Requirements on page 153](#)
- [Overview on page 153](#)
- [Configuration on page 153](#)
- [Verification on page 154](#)

Requirements

Before rebooting the device, save and commit any Junos OS updates.

Overview

This example shows how to reboot a device fifty minutes from when you set the time from the internal media while sending a text message of 'stop' to all system users before the device reboots.

Configuration

CLI Quick Configuration

To quickly reboot a device, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

From operational mode, enter:

```
user@host> request system reboot at 5 in 50 media internal message stop
```

GUI Step-by-Step Procedure

To reboot a device:

1. In the J-Web user interface, select **Maintain>Reboot**.
2. Select **Reboot in 50 minutes** to reboot the device fifty minutes from the current time.
3. Select the **internal** boot device from the Reboot From Media list.
4. In the Message box, type **stop** as the message to display to any user on the device before the reboot occurs.
5. Click **Schedule**. The J-Web user interface requests confirmation to perform the reboot.
6. Click **OK** to confirm the operation.
 - If the reboot is scheduled to occur immediately, the device reboots. You cannot access J-Web until the device has restarted and the boot sequence is complete. After the reboot is complete, refresh the browser window to display the J-Web login page.
 - If the reboot is scheduled to occur in the future, the Reboot page displays the time until reboot. You have the option to cancel the request by clicking **Cancel Reboot** on the J-Web user interface Reboot page.
7. Click **OK** to check your configuration and save it as a candidate configuration.
8. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To reboot a device:

From operational mode, schedule a reboot of the SRX Series device to occur fifty minutes from when you set the time from the internal media while sending a text message of 'stop' to all system users before the device reboots.

```
user@host> request system reboot at 5 in 50 media internal message stop
```

Results

From configuration mode, confirm your configuration by entering the **show system** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying the Device Reboot

Purpose

Verify that the device rebooted.

Action

From operational mode, enter the **show system** command.

- Related Documentation**
- [Example: Configuring Boot Devices for SRX Series Devices on page 95](#)
 - [Junos OS Upgrade Methods on the SRX Series Devices on page 12](#)
 - [Example: Installing Junos OS Upgrades on SRX Series Devices on page 55](#)
 - [Example: Halting SRX Series Devices on page 158](#)
 - *Installation and Upgrade Guide for Security Devices*

Example: Rebooting J Series Devices

This example shows how to reboot a J Series device.

- [Requirements on page 155](#)
- [Overview on page 155](#)
- [Configuration on page 155](#)
- [Verification on page 156](#)

Requirements

Before rebooting the device, save and commit any Junos OS updates.

Overview

This example shows how to reboot a device fifty minutes from when you set the time from the USB media while sending a text message of 'stop' to all system users before the device reboots.

Configuration

CLI Quick Configuration To quickly reboot a J Series device, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

From operational mode, enter:

```
user@host> request system reboot at 5 in 50 media usb message stop
```

- GUI Step-by-Step Procedure** To reboot a J Series device:
1. In the J-Web user interface, select **Maintain>Reboot**.
 2. Select **Reboot in 50 minutes** to reboot the device fifty minutes from the current time.
 3. Select the **usb** boot device from the Reboot From Media list.
 4. In the Message box, type **stop** as the message to display to any user on the device before the reboot occurs.
 5. Click **Schedule**. The J-Web user interface requests confirmation to perform the reboot.
 6. Click **OK** to confirm the operation.
 - If the reboot is scheduled to occur immediately, the device reboots. You cannot access J-Web until the device has restarted and the boot sequence is complete.

After the reboot is complete, refresh the browser window to display the J-Web login page.

- If the reboot is scheduled to occur in the future, the Reboot page displays the time until reboot. You have the option to cancel the request by clicking **Cancel Reboot** on the J-Web user interface Reboot page.
7. Click **OK** to check your configuration and save it as a candidate configuration.
 8. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To reboot a J Series device:

From operational mode, schedule a reboot of the J Series device to occur fifty minutes from when you set the time from the USB media while sending a text message of 'stop' to all system users before the device reboots.

```
user@host> request system reboot at 5 in 50 media usb message stop
```

Results From configuration mode, confirm your configuration by entering the **show system** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying the Device Reboot

Purpose Verify that the device rebooted.

Action From operational mode, enter the **show system** command.

Related Documentation

- [Preparing Your J Series Services Router for Junos OS Upgrades on page 45](#)
- [Example: Installing Junos OS Upgrades on J Series Devices on page 57](#)
- [Example: Downgrading Junos OS on J Series Devices on page 81](#)
- [Example: Halting J Series Devices on page 159](#)
- *Installation and Upgrade Guide for Security Devices*

Restarting the Chassis on SRX Series Devices

You can restart the chassis using the **restart chassis-control** command with the following options:

- To restart the process gracefully:
`user@host> restart chassis-control gracefully`
- To restart the process immediately:
`user@host> restart chassis-control immediately`
- To restart the process softly:
`user@host> restart chassis-control soft`

Related Documentation

- [Example: Configuring Boot Devices for SRX Series Devices on page 95](#)
- [Junos OS Upgrade Methods on the SRX Series Devices on page 12](#)
- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 55](#)
- [Upgrading the Boot Loader on SRX Series Devices on page 77](#)
- *Installation and Upgrade Guide for Security Devices*

Restarting the Chassis on J Series Devices

You can restart the chassis using the **restart chassis-control** command with the following options:

- To restart the process.
`user@host> restart chassis-control |`
- To restart the process gracefully:
`user@host> restart chassis-control gracefully`
- To restart the process immediately:
`user@host> restart chassis-control immediately`
- To restart the process softly:
`user@host> restart chassis-control soft`

Related Documentation

- [Preparing Your J Series Services Router for Junos OS Upgrades on page 45](#)
- [Example: Installing Junos OS Upgrades on J Series Devices on page 57](#)
- [Bringing Chassis Components Online and Offline on J Series Devices on page 162](#)
- [Example: Rebooting J Series Devices on page 155](#)
- *Installation and Upgrade Guide for Security Devices*

Example: Halting SRX Series Devices

This example shows how to halt a device.

- [Requirements on page 158](#)
- [Overview on page 158](#)
- [Configuration on page 158](#)
- [Verification on page 159](#)

Requirements

Before halting the device, save and commit any Junos OS updates.

Overview

When the device is halted, all software processes stop and you can access the device through the console port only. Reboot the device by pressing any key on the keyboard.



NOTE: If you cannot connect to the device through the console port, shut down the device by pressing and holding the power button on the front panel until the **POWER LED** turns off. After the device has shut down, you can power on the device by pressing the power button again. The **POWER LED** turns on during startup and remains steadily green when the device is operating normally.

This example shows how to halt the system and stop software processes on the device immediately.

Configuration

CLI Quick Configuration

To quickly halt a device immediately, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

From operational mode, enter:

```
user@host>request system halt at now
```

GUI Step-by-Step Procedure

To halt a device immediately:

1. In the J-Web user interface, select **Maintain>Reboot**.
2. Select **Halt Immediately**. After the software stops, you can access the device through the console port only.
3. Click **Schedule**. The J-Web user interface requests confirmation to halt.
4. Click **OK** to confirm the operation. If the device halts, all software processes stop and you can access the device through the console port only. Reboot the device by pressing any key on the keyboard.

5. Click **OK** to check your configuration and save it as a candidate configuration.
6. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To halt a device:

From operational mode, halt the SRX Series device immediately.

```
user@host>request system halt at now
```

Results From configuration mode, confirm your configuration by entering the **show system** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying the Device Halt

Purpose Verify that the device halted.

Action From operational mode, enter the **show system** command.

Related Documentation

- [Example: Configuring Boot Devices for SRX Series Devices on page 95](#)
- [Junos OS Upgrade Methods on the SRX Series Devices on page 12](#)
- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 55](#)
- [Bringing Chassis Components Online and Offline on SRX Series Devices on page 161](#)
- [Installation and Upgrade Guide for Security Devices](#)

Example: Halting J Series Devices

This example shows how to halt a J Series device.

- [Requirements on page 160](#)
- [Overview on page 160](#)
- [Configuration on page 160](#)
- [Verification on page 161](#)

Requirements

Before halting the device, save and commit any Junos OS updates.

Overview

When the device is halted, all software processes stop and you can access the device through the console port only. Reboot the device by pressing any key on the keyboard.



NOTE: If you cannot connect to the device through the console port, shut down the device by pressing and holding the power button on the front panel until the **POWER** LED turns off. After the device has shut down, you can power on the device by pressing the power button again. The **POWER** LED turns on during startup and remains steadily green when the device is operating normally.

This example shows how to halt the system and stop software processes on the device immediately.

Configuration

CLI Quick Configuration

To quickly halt a J Series device, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

From operational mode, enter:

```
user@host>request system halt at now
```

GUI Step-by-Step Procedure

To halt a J Series device immediately:

1. In the J-Web user interface, select **Maintain>Reboot**.
2. Select **Halt Immediately**. After the software stops, you can access the device through the console port only.
3. Click **Schedule**. The J-Web user interface requests confirmation to halt.
4. Click **OK** to confirm the operation. If the device halts, all software processes stop and you can access the device through the console port only. Reboot the device by pressing any key on the keyboard.
5. Click **OK** to check your configuration and save it as a candidate configuration.
6. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To halt a device:

From operational mode, halt the J Series device immediately.

```
user@host>request system halt at now
```

Results From configuration mode, confirm your configuration by entering the **show system** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying the Device Halt

Purpose Verify that the device halted.

Action From operational mode, enter the **show system** command.

Related Documentation

- [Understanding Junos OS Upgrades for J Series Devices on page 11](#)
- [Preparing Your J Series Services Router for Junos OS Upgrades on page 45](#)
- [Example: Downgrading Junos OS on J Series Devices on page 81](#)
- [Example: Rebooting J Series Devices on page 155](#)
- *Installation and Upgrade Guide for Security Devices*

Bringing Chassis Components Online and Offline on SRX Series Devices

You can use the **request** commands to bring chassis components online and offline.

To bring chassis components online and offline, enter these **request chassis** commands:

```
user@host> request chassis <fru> slot <slot#> pic <pic#> online
```

```
user@host> request chassis <fru> slot <slot#> pic <pic#> offline
```

Where **<fru>** in the request chassis command can be any of the following (for Branch SRX Series devices):

- **fpc**—Changes the Flexible PIC Concentrator (FPC) status.

Where **<fru>** in the request chassis command can be any of the following (for High-End SRX Series devices):

- **cb**—Changes the control board status.
- **fabric**—Changes the fabric status.
- **fpc**—Changes the Flexible PIC Concentrator (FPC) status.
- **fpm**—Changes the craft interface status.
- **pic**—Changes the physical interface card status.
- **routing-engine**—Changes the routing engine status.



NOTE: The **request chassis** command is not supported for bringing SPCs online and offline.



NOTE: On SRX3000 Series devices, the Network Processing I/O card (NP-IOC) is not hot-swappable and the **request chassis** command is not supported for bringing NP-IOC online and offline. You must power off the services gateway before removing or installing the cards.

Example:

To bring specific pic and the corresponding fpc slot online, from operational mode enter the following **request chassis** command:

```
user@host> request chassis pic pic-slot 1 fpc-slot 1 online
```

**Related
Documentation**

- [Example: Configuring Boot Devices for SRX Series Devices on page 95](#)
- [Junos OS Upgrade Methods on the SRX Series Devices on page 12](#)
- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 55](#)
- [Restarting the Chassis on SRX Series Devices on page 157](#)
- *Installation and Upgrade Guide for Security Devices*

Bringing Chassis Components Online and Offline on J Series Devices

You can use the **request** commands to bring all chassis components (except Power Entry Modules and fans) online and offline.

To bring chassis components online and offline, enter these **request chassis** commands:

```
user@host> request chassis <fru> slot <slot#> pic <pic#> offline
user@host> request chassis <fru> slot <slot#> pic <pic#> online
```

Where **<fru>** in the **request chassis** command can be any of the following:

- **cb**—Changes the control board status.
- **cluster**—Changes the chassis cluster status.
- **fabric**—Changes the fabric status.
- **fpc**—Changes the Flexible PIC Concentrator (FPC) status.
- **fpm**—Changes the craft interface status.
- **pic**—Changes the physical interface card status.
- **routing-engine**—Changes the routing engine status.

To bring specific pic and the corresponding fpc slot online, from operational mode enter the following **request chassis** command:

```
user@host> request chassis pic pic-slot 1 fpc-slot 1 online
```

**Related
Documentation**


- [Preparing Your J Series Services Router for Junos OS Upgrades on page 45](#)
- [Example: Installing Junos OS Upgrades on J Series Devices on page 57](#)
- [Restarting the Chassis on J Series Devices on page 157](#)
- [Example: Rebooting J Series Devices on page 155](#)
- *Installation and Upgrade Guide for Security Devices*

CHAPTER 18

Operational Commands

- request system autorecovery state
- request system download abort
- request system download clear
- request system download pause
- request system download resume
- request system download start
- request system firmware upgrade
- request system license update
- request system partition compact-flash
- request system power-off fpc
- request system snapshot (Maintenance)
- request system software abort in-service-upgrade (ICU)
- request system software add (Maintenance)
- request system reboot
- request system software rollback (Maintenance)
- show chassis usb storage
- show system autorecovery state
- show system auto-snapshot
- show system download
- show system license (View)
- show system login logout
- show system snapshot media
- show system storage (View SRX Series)
- show system storage partitions (View SRX Series)
- show version

request system autorecovery state

Syntax	request system autorecovery state (save recover clear)
Release Information	Command introduced in Junos Release 11.2.
Description	Prepares the system for autorecovery of configuration, licenses, and disk information.
Options	<p>save—Save the current state of the disk partitioning, configuration, and licenses for autorecovery.</p> <p>The active Junos OS configuration is saved as the Junos rescue configuration, after which the rescue configuration, licenses, and disk partitioning information is saved for autorecovery. Autorecovery information must be initially saved using this command for the autorecovery feature to verify integrity of data on every bootup.</p>
	<div> NOTE:</div> <ul style="list-style-type: none">Any recovery performed at a later stage will restore the data to the same state as it was when the save command was executed.A fresh rescue configuration is generated when the command is executed. Any existing rescue configuration will be overwritten.
	<p>recover—Recover the disk partitioning, configuration, and licenses.</p> <p>After autorecovery data has been saved, the integrity of saved items is always checked automatically on every bootup. The recovery command allows you to forcibly re-run the tests at any time if required.</p>
	<p>clear—Clear all saved autorecovery information.</p> <p>Only the autorecovery information is deleted; the original copies of the data used by the router are not affected. Clearing the autorecovery information also disables all autorecovery integrity checks performed during bootup.</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">show system autorecovery state on page 185<i>Installation and Upgrade Guide for Security Devices</i>
List of Sample Output	request system autorecovery state save on page 167 request system autorecovery state recover on page 167 request system autorecovery state clear on page 167
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system autorecovery state save

```
user@host> request system autorecovery state save
Saving config recovery information
Saving license recovery information
Saving bsdlablel recovery information
```

Sample Output

request system autorecovery state recover

```
user@host> request system autorecovery state recover


Configuration:
File           Recovery Information  Integrity Check  Action / Status
rescue.conf.gz Saved                Passed           None
Licenses:
File           Recovery Information  Integrity Check  Action / Status
JUNOS282736.lic Saved                Passed           None
JUNOS282737.lic Saved                Failed           Recovered
BSD Labels:
Slice          Recovery Information  Integrity Check  Action / Status
s1             Saved                Passed           None
s2             Saved                Passed           None
s3             Saved                Passed           None
s4             Saved                Passed           None
```

Sample Output

request system autorecovery state clear

```
user@host> request system autorecovery state clear
Clearing config recovery information
Clearing license recovery information
Clearing bsdlablel recovery information
```

request system download abort

Syntax	<code>request system download abort <download-id></code>
Release Information	Command introduced in Release 11.2 of Junos OS.
Description	Abort a download. The download instance is stopped and cannot be resumed. Any partially downloaded file is automatically deleted to free disk space. Information regarding the download is retained and can be displayed with the show command until a Clear operation is performed.
<div> NOTE: Only downloads in the active, paused, and error states can be aborted.</div>	
Options	download-id —(Required) The ID number of the download to be paused.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• request system download start on page 172• request system download pause on page 170• request system download resume on page 171• request system download clear on page 169• <i>Installation and Upgrade Guide for Security Devices</i>
List of Sample Output	request system download abort on page 168
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system download abort

```
user@host> request system download abort 1
Aborted download #1
```

request system download clear


Syntax	request system download clear
Release Information	Command introduced in Release 11.2 of Junos OS.
Description	Delete the history of completed and aborted downloads.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• request system download start on page 172• request system download pause on page 170• request system download resume on page 171• request system download abort on page 168• <i>Installation and Upgrade Guide for Security Devices</i>
List of Sample Output	request system download clear on page 169
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system download clear

```
user@host> request system download clear
Cleared information on completed and aborted downloads
```

request system download pause


Syntax	request system download pause <download-id>
Release Information	Command introduced in Release 11.2 of Junos OS.
Description	Suspend a particular download instance.
<div> NOTE: Only downloads in the active state can be paused.</div>	
Options	download-id —(Required) The ID number of the download to be paused.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• request system download start on page 172• request system download resume on page 171• request system download abort on page 168• request system download clear on page 169• <i>Installation and Upgrade Guide for Security Devices</i>
List of Sample Output	request system download pause on page 170
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system download pause

```
user@host> request system download pause 1
Paused download #1
```

request system download resume

Syntax	<code>request system download resume <i>download-id</i> <max-rate></code>
Release Information	Command introduced in Release 11.2 of Junos OS.
Description	Resume a download that has been paused. Download instances that are not in progress because of an error or that have been explicitly paused by the user can be resumed by the user. The file will continue downloading from the point where it paused. By default, the download resumes with the same bandwidth specified with the request system download start command. The user can optionally specify a new (maximum) bandwidth with the request system download resume command.
<div>  NOTE: Only downloads in the paused and error states can be resumed. </div>	
Options	<p>download-id—(Required) The ID number of the download to be paused.</p> <p>max-rate—(Optional) The maximum bandwidth for the download.</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • request system download start on page 172 • request system download pause on page 170 • request system download abort on page 168 • request system download clear on page 169 • <i>Installation and Upgrade Guide for Security Devices</i>
List of Sample Output	request system download resume on page 171
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system download resume

```
user@host> request system download resume 1
Resumed download #1
```

request system download start

Syntax	<code>request system download start (url max-rate save as login delay)</code>
Release Information	Command introduced in Release 11.2 of Junos OS.
Description	Creates a new download instance and identifies it with a unique integer called the download ID.
Options	<p>url—(Required) The FTP or HTTP URL location of the file to be downloaded.</p> <p>max-rate—(Optional) The maximum average bandwidth for the download. Numbers with the suffix k or K, m or M, and g or G are interpreted as kbps, mbps, or gbps, respectively.</p> <p>save-as—(Optional) The filename to be used for saving the file in the <code>/var/tmp</code> location.</p> <p>login—(Optional) The username and password for the server in the format <code>username:password</code>.</p> <p>delay—(Optional) The number of hours after which the download should start.</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• request system download pause on page 170• request system download resume on page 171• request system download abort on page 168• request system download clear on page 169• <i>Installation and Upgrade Guide for Security Devices</i>
List of Sample Output	request system download start on page 172
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system download start

```
user@host> request system download start login user:passwd ftp://ftp-server/tftpboot/1m_file
max-rate 1k
Starting download #1
```

request system firmware upgrade

Syntax	request system firmware upgrade
Release Information	Command introduced in Release 10.2 of Junos OS.
Description	Upgrade firmware on a system.
Options	<p>fpc—Upgrade FPC ROM monitor.</p> <p>pic—Upgrade PIC firmware.</p> <p>re—Upgrade baseboard BIOS/FPGA. There is an active BIOS image and a backup BIOS image.</p> <p>vcpu—Upgrade VCPU ROM monitor.</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • <i>Installation and Upgrade Guide for Security Devices</i> • <i>Administration Guide for Security Devices</i>
List of Sample Output	request system firmware upgrade on page 173
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system firmware upgrade

```

user@host> request system firmware upgrade re bios
Part          Type          Tag Current Available Status
              version      version
Routing Engine 0 RE BIOS      0   1.5      1.9      OK
Routing Engine 0 RE BIOS Backup 1 1.7      1.9      OK
Perform indicated firmware upgrade ? [yes,no] (no) yes

user@host> request system firmware upgrade re bios backup
Part          Type          Tag Current Available Status
              version      version
Routing Engine 0 RE BIOS      0   1.5      1.9      OK
Routing Engine 0 RE BIOS Backup 1 1.7      1.9      OK
Perform indicated firmware upgrade ? [yes,no] (no) yes

```

request system license update

Syntax	request system license update
Release Information	Command introduced in Junos OS Release 9.5.
Description	Start autoupdating license keys from the LMS server.
Options	trial —Starts autoupdating trial license keys from the LMS server.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• <i>Administration Guide for Security Devices</i>• <i>UTM Overview Feature Guide for Security Devices</i>• <i>Installation and Upgrade Guide for Security Devices</i>
List of Sample Output	request system license update on page 174 request system license update trial on page 174
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system license update

```
user@host> request system license update
```

```
Request to automatically update license keys from https://ae1.juniper.net has  
been sent, use show system license to check status.
```

request system license update trial

```
user@host> request system license update trial
```

```
Request to automatically update trial license keys from https://ae1.juniper.net  
has been sent, use show system license to check status.
```


request system partition compact-flash

Syntax	request system partition compact-flash
Release Information	Command introduced in Release 9.2 of Junos OS.
Description	Reboots the device and repartitions the compact flash. The compact flash is repartitioned only if it is possible to restore all the data on the compact flash. Otherwise, the operation is aborted, and a message is displayed indicating that the current disk usage needs to be reduced.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 72 • <i>Installation and Upgrade Guide for Security Devices</i>
List of Sample Output	request system partition compact-flash (If Yes) on page 175 request system partition compact-flash (If No) on page 175
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system partition compact-flash (If Yes)

```

user@host> request system partition compact-flash
Are you sure you want to reboot
and partition the compact-flash ? [yes,no] yes
Initiating repartition operation.
The operation may take several minutes to complete.
System will reboot now...
<System reboots>
<Repartition operation is performed>
<System reboots and starts up normally>

```

Sample Output

request system partition compact-flash (If No)

```

user@host> request system partition compact-flash
Are you sure you want to reboot
and partition the compact-flash ? [yes,no] no

```

request system power-off fpc

Syntax	request system (halt power-off reboot) power-off fpc
Release Information	Command introduced in Junos OS Release 11.4.
Description	Bring Flexible PIC Concentrators (FPCs) offline before Routing Engines are shut down.
Options	<ul style="list-style-type: none">• halt—Bring FPC offline and then halt the system.• power-off—Bring FPC offline and then power off the system.• reboot—Bring FPC offline and then reboot the system.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• <i>Installation and Upgrade Guide for Security Devices</i>
List of Sample Output	request system halt power-off fpc on page 176 request system power-off power-off fpc on page 176 request system reboot power-off fpc on page 176
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system halt power-off fpc

```
user@host> request system halt power-off fpc
Halt the system ? [yes,no] (no) yes

Offline fpc slot 0
```

request system power-off power-off fpc

```
user@host> request system power-off power-off fpc
Power off the system ? [yes,no] (no) yes

Offline fpc slot 0
```

request system reboot power-off fpc

```
user@host> request system reboot power-off fpc
Reboot the system ? [yes,no] (no) yes

Offline fpc slot 0
```

request system snapshot (Maintenance)

Syntax request system snapshot
 <factory>
 <media (compact-flash | hard-disk | internal | usb)>
 <node (all | local | node-id | primary)>
 <partition>
 <slice (alternate) >

Release Information Command introduced in Release 10.2 of Junos OS.

Description Back up the currently running and active file system partitions on the device.

- Options**
- **factory**— (Optional) Specifies that only the files shipped from the factory are included in the snapshot.
 - **media**— (Optional) Specifies the media to be included in the snapshot:
 - **compact-flash**— Copies the snapshot to an external compact flash.
 - **hard-disk**— Copies the snapshot to a hard disk.
 - **usb**— Copies the snapshot to the USB storage device.
 - **internal**— Copies the snapshot to internal media. This is the default.



NOTE: USB option is available on all SRX series devices; hard disk and compact-flash options are available only on high-end SRX series devices; media internal option is available only on branch SRX series devices.

- **node**— (Optional) Specifies to archive the data and executable areas of a specific node.
 - **node-id**—Archive a specific node. The range of node ID is (0,1)
 - **all**—Archive all nodes.
 - **local**—Archive only local nodes.
 - **primary**—Archive only primary nodes.
- **partition** - (Default) Specifies that the target media should be repartitioned before the backup is saved to it.

**NOTE:**

- The target media is partitioned whether or not it is specified in the command, because this is a mandatory option.
- You cannot partition a hard-disk as it is mounted on /var directory.

- slice— (Optional) Takes a snapshot of the root partition the system has currently booted from to another slice in the same media.
- alternate— (Optional) Stores the snapshot on the other root partition in the system.

**NOTE:**

- The slice option cannot be used along with the other request system snapshot options, because the options are mutually exclusive. If you use the factory, media, or partition option, you cannot use the slice option; if you use the slice option, you cannot use any of the other options.
- The slice partition is supported only on branch SRX Series devices.

Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 72 • <i>Installation and Upgrade Guide for Security Devices</i>
List of Sample Output	request system snapshot media hard-disk on page 178 request system snapshot media usb (when usb device is missing on page 178 request system snapshot media compact-flash on page 179 request system snapshot media internal on page 179 request system snapshot partition on page 179
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

[request system snapshot media hard-disk](#)

```
user@host> request system snapshot media hard-disk
Verifying compatibility of destination media partitions...
Running newfs (880MB) on hard-disk media / partition (ad2s1a)...
Running newfs (98MB) on hard-disk media /config partition (ad2s1e)...
Copying '/dev/ad0s1a' to '/dev/ad2s1a' .. (this may take a few minutes)
...
```

[request system snapshot media usb \(when usb device is missing](#)

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

```
Verifying compatibility of destination media partitions...
Running newfs (254MB) on usb media / partition (da1s1a)...
Running newfs (47MB) on usb media /config partition (da1s1e)...
Copying '/dev/da0s2a' to '/dev/da1s1a' .. (this may take a few minutes)
Copying '/dev/da0s2e' to '/dev/da1s1e' .. (this may take a few minutes)
The following filesystems were archived: / /config
```

request system snapshot media compact-flash

```
user@host> request system snapshot media compact-flash
error: cannot snapshot to current boot device
```

request system snapshot media internal

```
user@host> request system snapshot media internal
error: cannot snapshot to current boot device
```

request system snapshot partition

```
user@host> request system snapshot partition
Verifying compatibility of destination media partitions...
Running newfs (439MB) on internal media / partition (da0s1a)...
Running newfs (46MB) on internal media /config partition (da0s1e)...
Copying '/dev/da1s1a' to '/dev/da0s1a' .. (this may take a few minutes)
Copying '/dev/da1s1e' to '/dev/da0s1e' .. (this may take a few minutes)
The following filesystems were archived: / /config
```

request system software abort in-service-upgrade (ICU)

Syntax	request system software abort in-service-upgrade
Release Information	Command introduced in Release 11.2 of Junos OS.
Description	Abort an in-band cluster upgrade (ICU). This command must be issued from a router session other than the one on which you issued the request system in-service-upgrade command that launched the ICU. If an ICU is in progress, this command aborts it. If the node is being upgraded, this command will cancel the upgrade. The command is also helpful in recovering the node in case of a failed ICU.
Options	This command has no options.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• <i>request system software in-service-upgrade (Maintenance)</i>• <i>Installation and Upgrade Guide for Security Devices</i>
List of Sample Output	request system software abort in-service-upgrade on page 180
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system software abort in-service-upgrade

```
user@host> request system software abort in-service-upgrade
In-Service-Upgrade aborted
```

request system software add (Maintenance)

Syntax	<code>request system software add <i>package-name</i></code>
Release Information	Partition option introduced in the command in Release 10.1. of Junos OS.
Description	Installs the new software package on the device. For example: request system software add junos-srxsme-10.0R2-domestic.tgz no-copy no-validate partition reboot.
Options	<ul style="list-style-type: none"> • <code>delay-restart</code> — Installs the software package but does not restart the software process • <code>best-effort-load</code> — Activate a partial load and treat parsing errors as warnings instead of errors • <code>no-copy</code> — Installs the software package but does not saves the copies of package files • <code>no-validate</code> — Does not check the compatibility with current configuration before installation starts • <code>partition</code> — Formats and re-partitions the media before installation • <code>reboot</code> — Reboots the device after installation is completed • <code>unlink</code> — Removes the software package after successful installation • <code>validate</code> — Checks the compatibility with current configuration before installation starts
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • <i>Installation and Upgrade Guide for Security Devices</i> • <i>Administration Guide for Security Devices</i>

request system reboot

Syntax	<code>request system reboot <at time> <in minutes><media><message 'text'></code>
Release Information	Command introduced in Junos OS Release 10.1.
Description	Reboots the software.
Options	<ul style="list-style-type: none">• <i>at time</i>— Specifies the time at which to reboot the device . You can specify time in one of the following ways:<ul style="list-style-type: none">• <i>now</i>— Reboots the device immediately. This is the default.• <i>+minutes</i>— Reboots the device in the number of minutes from now that you specify.• <i>yymmddhhmm</i>— Reboots the device at the absolute time on the date you specify. Enter the year, month, day, hour (in 24-hour format), and minute.• <i>hh:mm</i>— Reboots the device at the absolute time you specify, on the current day. Enter the time in 24-hour format, using a colon (:) to separate hours from minutes.• <i>in minutes</i>— Specifies the number of minutes from now to reboot the device. This option is a synonym for the <i>at +minutes</i> option• <i>media type</i>— Specifies the boot device to boot the device from:<ul style="list-style-type: none">• <i>disk/internal</i>— Reboots from the internal media. This is the default.• <i>usb</i>— Reboots from the USB storage device.• <i>compact flash</i>— Reboots from the external compact flash. This option is available on the SRX650 Services Gateway.• <i>message text</i>— Provides a message to display to all system users before the device reboots. <p>Example: request system reboot at 5 in 50 media internal message stop</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• request system software rollback (Maintenance) on page 183

request system software rollback (Maintenance)

Syntax	request system software rollback <node <i>node-id</i> > <all> <local> <primary> <reboot>
Release Information	Command introduced in Junos OS Release 10.1.
Description	Revert to the software that was loaded at the last successful request system software add command. Example: request system software rollback .
Options	<ul style="list-style-type: none"> • node <i>node-id</i>—(High-end SRX Series devices only) Roll back the software to the previous set of packages on a specific node. • all— Roll back the software on all the nodes. • local— Roll back the software on the local node. • primary— Roll back the software on the primary node. • reboot— Reboot the system after a roll back.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • <i>Installation and Upgrade Guide for Security Devices</i> • <i>Administration Guide for Security Devices</i>

show chassis usb storage

Syntax	show chassis usb storage
Release Information	Command introduced in Junos OS Release 11.4 R2.
Description	Displays the current status of any USB mass storage device and whether the USB ports are enabled or disabled.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• <i>Installation and Upgrade Guide for Security Devices</i>
List of Sample Output	show chassis hardware detail on page 184 show chassis usb storage on page 184

Sample Output

show chassis hardware detail

```
user@host> show chassis hardware detail
Hardware inventory:
Item              Version  Part number  Serial number  Description
Chassis
Routing Engine    REV 01   750-043613   BV4911AA0005   SRX240H2-POE
usb0 (addr 1)     DWC OTG  root hub 0   vendor 0x0000   uhub0
usb0 (addr 2)     product 0x005a 90   vendor 0x0409   uhub1
usb0 (addr 3)     ST72682  High Speed Mode 64218 STMicroelectronics umass0
usb0 (addr 4)     Mass Storage Device 4096 JetFlash   umass1
FPC 0
PIC 0
Power Supply 0    FPC
                  16x GE Base PIC
```

show chassis usb storage

```
user@host> show chassis usb storage
USB Disabled
```

show system autorecovery state

Syntax	show system autorecovery state
Release Information	Command introduced in Release 11.2 of Junos OS.
Description	Performs checks and shows status of all autorecovered items.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • request system autorecovery state on page 166 • <i>Installation and Upgrade Guide for Security Devices</i> • <i>Administration Guide for Security Devices</i>
List of Sample Output	show system autorecovery state on page 185
Output Fields	Table 17 on page 185 lists the output fields for the show system autorecovery state command. Output fields are listed in the approximate order in which they appear.

Table 17: show system autorecovery state Output Fields

Field Name	Field Description
File	The name of the file on which autorecovery checks are performed.
Slice	The disk partition on which autorecovery checks are performed.
Recovery Information	Indicates whether autorecovery information for the file or slice has been saved.
Integrity Check	Displays the status of the file's integrity check (passed or failed).
Action / Status	Displays the status of the item, or the action required to be taken for that item.

Sample Output

show system autorecovery state

```
user@host> show system autorecovery state
```

```

Configuration:
File          Recovery Information  Integrity Check  Action / Status
rescue.conf.gz Saved                Passed          None
Licenses:
File          Recovery Information  Integrity Check  Action / Status
JUNOS282736.lic Saved                Passed          None
JUNOS282737.lic Not Saved           Not checked     Requires save
BSD Labels:
Slice         Recovery Information  Integrity Check  Action / Status
s1            Saved                Passed          None
s2            Saved                Passed          None

```

s3	Saved	Passed	None
s4	Saved	Passed	None

show system auto-snapshot

Syntax	show system auto-snapshot
Release Information	Command introduced in Junos OS Release 12.1X45-D10.
Description	<p>Display the status of the auto-snapshot information on SRX Series devices. When the automatic snapshot feature is enabled and the system reboots from the alternate root partition, the switch automatically takes a snapshot of the root file system in the alternate root partition and copies it to the primary root partition. This automatic snapshot procedure takes place whenever the system reboots from the alternate partition, regardless of whether the reboot from the alternate partition is due to a command or due to a corruption of the primary partition.</p> <p>When the automatic snapshot procedure is in progress, you cannot run the manual snapshot command, request system snapshot.</p>
Required Privilege Level	View
Related Documentation	<ul style="list-style-type: none"> • show system snapshot media on page 195 • <i>Installation and Upgrade Guide for Security Devices</i>
List of Sample Output	show system auto-snapshot on page 188
Output Fields	<p>Table 18 on page 187 lists the output fields for the show system auto-snapshot command. Output fields are listed in the approximate order in which they appear.</p>

Table 18: show system auto-snapshot Output Fields

Field Name	Field Description
Auto-snapshot Configuration	<p>Displays the configuration status of auto-snapshot.</p> <p>Status of the configuration:</p> <ul style="list-style-type: none"> • Enabled—If the system reboots from the alternate partition, the automatic snapshot feature automatically takes a snapshot of the alternate partition and copies it to the primary partition. • Disabled—The system does not automatically take a snapshot of the alternate partition. You must use the manual snapshot command, request system snapshot, to take a snapshot of one partition and copy it to the other.
Auto-snapshot State	<p>Displays the current state of auto-snapshot.</p> <p>Status of the automatic snapshot procedure:</p> <ul style="list-style-type: none"> • Completed—The automatic snapshot procedure has completed copying the alternate partition to the primary partition and the alarm has been cleared. • Disabled—The automatic snapshot procedure is inactive. • In progress—The automatic snapshot procedure is in progress. It takes about 10 to 15 minutes to complete, depending upon disk size.

Sample Output

show system auto-snapshot

```
user@host> show system auto-snapshot
```

```
Auto-snapshot Configuration:  Enabled  
Auto-snapshot State: Completed
```

show system download

Syntax	<code>show system download <download-id></code>
Release Information	Command introduced in Release 11.2 of Junos OS.
Description	Display a brief summary of all the download instances along with their current state and extent of progress. If a download-id is provided, the command displays a detailed report of the particular download instance.
Options	<ul style="list-style-type: none"> download-id—(Optional) The ID number of the download instance.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> request system download start on page 172 <i>Installation and Upgrade Guide for Security Devices</i> <i>Administration Guide for Security Devices</i>
List of Sample Output	show system download on page 189 show system download 1 on page 190
Output Fields	Table 19 on page 189 lists the output fields for the show system download command. Output fields are listed in the approximate order in which they appear.

Table 19: show system download Output Fields

Field Name	Field Description
ID	Displays the download identification number.
Status	Displays the state of a particular download.
Start Time	Displays the start time of a particular download.
Progress	Displays the percentage of a download that has been completed.
URL	Displays the location of the downloaded file.

Sample Output

show system download

```

user@host> show system download
Download Status Information:
ID  Status  Start Time      Progress  URL
1   Active   May 4 06:28:36  5%        ftp://ftp-server//tftpboot/1m_file
2   Active   May 4 06:29:07  3%        ftp://ftp-server//tftpboot/5m_file
3   Error    May 4 06:29:22  Unknown   ftp://ftp-server//tftpboot/badfile

```

4 Completed May 4 06:29:40 100% ftp://ftp-server//tftpboot/smallfile

show system download 1

```
user@host> show system download 1
```

```
Download ID      : 1
Status           : Active
Progress         : 6%
URL              : ftp://ftp-server//tftpboot/1m_file
Local Path       : /var/tmp/1m_file
Maximum Rate     : 1k
Creation Time    : May 4 06:28:36
Scheduled Time   : May 4 06:28:36
Start Time       : May 4 06:28:37
Error Count      : 0
```


show system license (View)

Syntax	show system license <installed keys status usage>
Release Information	Command introduced in Junos OS Release 9.5. Logical system status option added in Junos OS Release 11.2.
Description	Display licenses and information about how licenses are used.
Options	<p>none—Display all license information.</p> <p>installed—(Optional) Display installed licenses only.</p> <p>keys—(Optional) Display a list of license keys. Use this information to verify that each expected license key is present.</p> <p>status—(Optional) Display license status for a specified logical system or for all logical systems.</p> <p>usage—(Optional) Display the state of licensed features.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • <i>Administration Guide for Security Devices</i> • <i>Installation and Upgrade Guide for Security Devices</i>
List of Sample Output	<p>show system license on page 192</p> <p>show system license installed on page 192</p> <p>show system license keys on page 193</p> <p>show system license usage on page 193</p> <p>show system license status logical-system all on page 193</p>
Output Fields	Table 20 on page 191 lists the output fields for the show system license command. Output fields are listed in the approximate order in which they appear.

Table 20: show system license Output Fields

Field Name	Field Description
Feature name	Name assigned to the configured feature. You use this information to verify that all the features for which you installed licenses are present.
Licenses used	Number of licenses used by the device. You use this information to verify that the number of licenses used matches the number configured. If a licensed feature is configured, the feature is considered used.

Table 20: show system license Output Fields (*continued*)

Field Name	Field Description
Licenses installed	Information about the installed license key: <ul style="list-style-type: none"> • License identifier—Identifier associated with a license key. • License version—Version of a license. The version indicates how the license is validated, the type of signature, and the signer of the license key. • Valid for device—Device that can use a license key. • Features—Feature associated with a license.
Licenses needed	Number of licenses required for features being used but not yet properly licensed.
Expiry	Time remaining in the grace period before a license is required for a feature being used.
Logical system license status	Displays whether a license is enabled for a logical system.

Sample Output

show system license

```
user@host> show system license
```

```
License usage:
```

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
av_key_kaspersky_engine 01:00:00 IST	1	1	0	2012-03-30
wf_key_surfcontrol_cpa 01:00:00 IST	0	1	0	2012-03-30
dynamic-vpn	0	1	0	permanent
ax411-wlan-ap	0	2	0	permanent

```
Licenses installed:
```

```
License identifier: JUNOS301998
```

```
License version: 2
```

```
Valid for device: AG4909AA0080
```

```
Features:
```

```
av_key_kaspersky_engine - Kaspersky AV
```

```
date-based, 2011-03-30 01:00:00 IST - 2012-03-30 01:00:00 IST
```

```
License identifier: JUNOS302000
```

```
License version: 2
```

```
Valid for device: AG4909AA0080
```

```
Features:
```

```
wf_key_surfcontrol_cpa - Web Filtering
```

```
date-based, 2011-03-30 01:00:00 IST - 2012-03-30 01:00:00 IST
```

show system license installed

```
user@host> show system license installed
```

```
License identifier: JUNOS301998
```

```
License version: 2
```

```
Valid for device: AG4909AA0080
```

```
Features:
```

```
av_key_kaspersky_engine - Kaspersky AV
date-based, 2011-03-30 01:00:00 IST - 2012-03-30 01:00:00 IST
```

```
License identifier: JUNOS302000
```

```
License version: 2
```

```
Valid for device: AG4909AA0080
```

```
Features:
```

```
wf_key_surfcontrol_cpa - Web Filtering
```

```
date-based, 2011-03-30 01:00:00 IST - 2012-03-30 01:00:00 IST
```

show system license keys

```
user@host> show system license keys
```

```
XXXXXXXXXX xxxxxxx xxxxxxx xxxxxxx xxxxxxx xxxxxxx xxxxxxx
xxxxxxx xxxxxxx xxxxxxx xxxxxxx xxxxxxx xxxxxxx xxxxxxx
xxxxxxx xxxxxxx xxx
```

show system license usage

```
user@host> show system license usage
```

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
av_key_kaspersky_engine	1	1	0	2012-03-30
01:00:00 IST				
wf_key_surfcontrol_cpa	0	1	0	2012-03-30
01:00:00 IST				
dynamic-vpn	0	1	0	permanent
ax411-wlan-ap	0	2	0	permanent

show system license status logical-system all

```
user@host> show system license status logical-system all
Logical system license status:
```

logical system name	license status
root-logical-system	enabled
LSYS0	enabled
LSYS1	enabled
LSYS2	enabled

show system login logout

Syntax	show system login logout
Release Information	Command introduced in Release 11.2 of Junos OS.
Description	Display the user names locked after unsuccessful login attempts.
Required Privilege Level	view and system
Related Documentation	<ul style="list-style-type: none">• <i>Administration Guide for Security Devices</i>• <i>Installation and Upgrade Guide for Security Devices</i>
List of Sample Output	show system login logout on page 194
Output Fields	Table 21 on page 194 lists the output fields for the show system login logout command. Output fields are listed in the approximate order in which they appear. Field names might be abbreviated (as shown in parentheses) when no level of output is specified or when the detail keyword is used.

Table 21: show system login logout

Field Name	Field Description	Level of Output
User	Username	All levels
Lockout start	Date and time the username was locked	All levels
Lockout end	Date and time the username was unlocked	All levels

Sample Output

show system login logout

```
user@host>show system login logout
```

User	Lockout start	Lockout end
root	2011-05-11 09:11:15 UTC	2011-05-11 09:13:15 UTC

show system snapshot media

Syntax	<code>show system snapshot media <i>media-type</i></code>
Release Information	Command introduced in Release 10.2 of Junos OS.
Description	Display the snapshot information for both root partitions on SRX Series devices
Options	<ul style="list-style-type: none"> • <code>internal</code>— Show snapshot information from internal media. • <code>usb</code>— Show snapshot information from device connected to USB port. • <code>external</code>— Show snapshot information from the external compact flash. This option is available on the SRX650 Services Gateway.
Required Privilege Level	View
Related Documentation	<ul style="list-style-type: none"> • <i>Installation and Upgrade Guide for Security Devices</i>

show system snapshot media internal

```

show system snapshot media internal
Information for snapshot on      internal (/dev/da0s1a) (primary)
Creation date: Jan 15 10:43:26 2010
JUNOS version on snapshot:
  junos   : 10.1B3-domestic
Information for snapshot on      internal (/dev/da0s2a) (backup)
Creation date: Jan 15 10:15:32 2010
JUNOS version on snapshot:
  junos   : 10.2-20100112.0-domestic

```

show system snapshot media usb

```

show system snapshot media usb
Information for snapshot on      usb (/dev/da1s1a) (primary)
Creation date: Jul 24 16:16:01 2009
JUNOS version on snapshot:
  junos   : 10.0I20090723_1017-domestic
Information for snapshot on      usb (/dev/da1s2a) (backup)
Creation date: Jul 24 16:17:13 2009
JUNOS version on snapshot:
  junos   : 10.0I20090724_0719-domestic

```

show system storage (View SRX Series)

Syntax show system storage
 <detail>
 <node *node-id* | all | local | primary>
 <partitions>

Release Information Command introduced in Junos OS Release 10.2.

Description Display the local storage data currently available on the SRX Series devices.

- Options**
- **none**—Display standard information about the amount of free disk space in the device file system.
 - **detail**—(Optional) Display detailed output about the amount of free disk space in the device file system.
 - **node**—(Optional) Display local storage data for a specific node.



NOTE: The **node** option is supported only on high-end SRX Series devices.

- **node-id**—Identification number of the node. It can be 0 or 1.
- **all**—(Optional) Display the local storage data for all nodes.
- **local**—(Optional) Display the local storage data for the local node.
- **primary**—(Optional) Display the local storage data for the primary node.
- **partitions**—(Optional) Display partitions information for the boot media.



NOTE: The **partitions** option is supported only on branch SRX Series devices.

Required Privilege Level View

Output Fields [Table 22 on page 196](#) describes the output fields for the **show system storage** command. Output fields are listed in the approximate order in which they appear.

Table 22: show system storage Output Fields

Field Name	Field Description
Filesystem	Name of the file system.
Size	Size of the file system.
Used	Amount of space used in the file system.

Table 22: show system storage Output Fields (*continued*)

Field Name	Field Description
Avail	Amount of space available in the file system.
Capacity	Percentage of the file system space that is being used.
Mounted on	Directory in which the file system is mounted.

show system storage

```
user@host>show system storage
```

Filesystem	Size	Used	Avail	Capacity	Mounted on
/dev/ad0s2a	621M	169M	402M	30%	/
devfs	1.0K	1.0K	0B	100%	/dev
/dev/md0	20M	6.3M	12M	35%	/junos
/cf/packages	621M	169M	402M	30%	/junos/cf/packages
devfs	1.0K	1.0K	0B	100%	/junos/cf/dev
/dev/md1	494M	494M	0B	100%	/junos
/cf	20M	6.3M	12M	35%	/junos/cf
devfs	1.0K	1.0K	0B	100%	/junos/dev/
/cf/packages	621M	169M	402M	30%	/junos/cf/packages
1					
procfs	4.0K	4.0K	0B	100%	/proc
/dev/bo0s3e	49M	24K	45M	0%	/config
/dev/bo0s3f	616M	399M	168M	70%	/cf/var
/dev/md2	336M	20M	289M	7%	/mfs
/cf/var/jail	616M	399M	168M	70%	/jail/var
/cf/var/log	616M	399M	168M	70%	/jail/var/log
devfs	1.0K	1.0K	0B	100%	/jail/dev
/dev/md3	63M	4.0K	58M	0%	/mfs/var/run/utm
/dev/md4	1.8M	228K	1.5M	13%	/jail/mfs

show system storage partitions (View SRX Series)

Syntax	show system storage partitions
Release Information	Command introduced in Release 10.2 of Junos OS.
Description	Displays the partitioning scheme details on SRX Series devices.
Required Privilege Level	View
Related Documentation	<ul style="list-style-type: none">• <i>Installation and Upgrade Guide for Security Devices</i>

show system storage partitions (dual root partitioning)

```
show system storage partitions
Boot Media: internal (da0)
Active Partition: da0s2a
Backup Partition: da0s1a
Currently booted from: active (da0s2a)
```

```
Partitions Information:
Partition  Size  Mountpoint
s1a       293M  altroot
s2a       293M  /
s3e        24M  /config
s3f       342M  /var
s4a        30M  recovery
```

show system storage partitions (single root partitioning)

```
show system storage partitions
Boot Media: internal (da0)
Partitions Information:
Partition  Size  Mountpoint
s1a       898M  /
s1e        24M  /config
s1f         61M  /var
```

show system storage partitions (USB)

```
show system storage partitions
Boot Media: usb (da1)
Active Partition: da1s1a
Backup Partition: da1s2a
Currently booted from: active (da1s1a)
```

```
Partitions Information:
Partition  Size  Mountpoint
s1a       293M  /
s2a       293M  altroot
s3e        24M  /config
s3f       342M  /var
s4a        30M  recovery
```


show version

Syntax	show version <brief detail> <node <i>node-id</i> local primary>
Release Information	Command introduced in Junos OS Release 10.4.
Description	Display the hostname and version information about the software running on the device.
Options	<p>none—Display standard information about the hostname and version of the software running on the device.</p> <p>brief—Display brief output.</p> <p>detail—Display detailed output.</p> <p>node <i>node-id</i>—Display the software version on a specific node. Range: 0 through 1</p> <p>local—Display the software version on the local node.</p> <p>primary—Display the software version on the primary node.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Determining the Junos OS Version on page 48
List of Sample Output	show version on page 199

Sample Output

show version

```

user@host> show version
node0:
-----
Hostname: srx01
Model: srx1400
JUNOS Software Release [12.3I20141112_x_srx_12q3_x48_intgr.0-681573]
JUNOS wmi Daemon [12.1I20140304_0803_tjzhang]
```


PART 5

Index

- [Index on page 203](#)

Index

Symbols

#, comments in configuration statements.....	xvi
(), in syntax descriptions.....	xvi
< >, in syntax descriptions.....	xvi
[], in configuration statements.....	xvi
{ }, in configuration statements.....	xvi
(pipe), in syntax descriptions.....	xvi

A

autoinstallation.....	132
automatic configuration process.....	29
CLI configuration editor.....	87
default configuration file.....	29
establishing.....	27
host-specific configuration file.....	29
interfaces.....	28
IP address procurement process.....	29
J-Web configuration editor.....	87
overview.....	27, 31
protocols for procuring an IP address.....	28
requirements.....	87
status.....	89
TFTP server.....	29
verifying.....	89
automatic configuration See autoinstallation	

B

backing up current installation	
J Series Services Routers.....	49
BOOTP, for autoinstallation.....	87
braces, in configuration statements.....	xvi
brackets	
angle, in syntax descriptions.....	xvi
square, in configuration statements.....	xvi
browser	
downloading software.....	50

C

category change software installation.....	9
chassis-control	
restart options.....	157

CLI configuration editor	
autoinstallation.....	87
command-line interface	
downloading software.....	51
comments, in configuration statements.....	xvi
configuration	
autoinstallation of.....	27
downgrading software (CLI).....	79
downgrading software (J-Web).....	79
installation on multiple devices.....	27
upgrading (CLI).....	55
configuration files	
automatic installation.....	30
configuration-servers.....	133
conventions	
text and syntax.....	xv
curly braces, in configuration statements.....	xvi
customer support.....	xvii
contacting JTAC.....	xvii

D

default configuration file, for autoinstallation.....	29
deleting	
licenses (CLI).....	150
licenses (J-Web).....	150
device	
autoinstallation.....	27
multiple, deploying See autoinstallation	
displaying	
licenses (J-Web).....	143
documentation	
comments on.....	xvii
downgrading	
software, with J-Web.....	79
software, with the CLI	79
download URL.....	52
downloading	
configuration, with autoinstallation.....	29
licenses (J-Web).....	144
software upgrades.....	52
downloading Junos OS.....	50
dual-root partitioning.....	10
dual-root partitioning scheme.....	19

E

Ethernet ports	
autoinstallation on.....	28

F

feature licenses See licenses	
font conventions.....	xv

G

group licenses.....	35
---------------------	----

H

hard disk.....	8
hardware architecture overview	
J Series routers.....	7
host-specific configuration file, for	
autoinstallation.....	29
hostname.conf file, for autoinstallation.....	29, 87

I

Install Remote page	
field summary.....	64, 72
installation	
licenses (CLI).....	146
licenses (J-Web).....	146
memory requirements	
J Series routers.....	7
software upgrades (CLI).....	55
software upgrades, from a remote server.....	63
software upgrades, uploading.....	55
installation modules.....	15
installation types.....	9
interfaces (autoinstallation).....	134

J

J Series	
licenses.....	33
J series	
install remote page	
field summary.....	65
J series device	
boot devices.....	98
storing memory snapshots.....	91
See also CompactFlash card	
bring components online/offline.....	162
chassis-control	
restart options.....	157
compactFlash.....	11
CompactFlash card	
configuring.....	98
configuring for failure snapshot	
storage.....	91

configuration	
downgrading software (CLI).....	81
upgrading (CLI).....	57
configuration, downgrading software	
(J-Web).....	81
device	
halting (J-Web).....	155
downgrading	
software, with the CLI	81
downgrading software (J-Web).....	81
downloading.....	53
halting (CLI).....	159
halting a	
with J-Web.....	155
installation	
software upgrades (CLI).....	57
software upgrades, from a remote	
server.....	64
installing by uploading.....	57
internal CompactFlash card See CompactFlash	
card	
rebooting	
with J-Web	155
rebooting (CLI).....	155
request system halt command.....	159
request system reboot command.....	155
request system snapshot command.....	98
options.....	98
reverting to a previous configuration file	
(J-Web).....	81
rolling back a configuration file.....	81
snapshots	
configuring for failure snapshot	
storage.....	91
software.....	11
software upgrades.....	11, 53
software upgrades, uploading.....	57
storage media	
configuring boot devices.....	98
upgrades	
installing (CLI).....	57
installing from remote server.....	64
upgrades requirements.....	45
upgrading.....	11
USB	
configuring.....	98
configuring for failure snapshot	
storage.....	91

- J series device boot devices
 - configuring (CLI).....98
 - configuring (J-Web).....98
 - J-Web configuration editor
 - autoinstallation.....87
 - J-Web interface
 - managing licenses.....34
 - Junos OS
 - autoinstallation.....27
 - downloading.....50
 - editions.....4
 - Canada and U.S.....4
 - Junos-FIPS.....4
 - worldwide.....4
 - generating licenses.....144
 - information security.....10
 - installation
 - current configuration, confirming.....53
 - installation modules.....15
 - introduction.....3
 - naming convention.....5
 - packages
 - digital signatures.....10
 - MD5 checksum.....10
 - naming conventions.....6
 - SHA-1 checksum.....10
 - release naming conventions.....6
 - release numbers.....6
 - software installation types.....9
 - storage media.....8
 - device names.....8
 - upgrading.....10
 - version, displaying.....48
 - Junos OS versions *See* Junos OS editions
- L**
- license infringement
 - identifying any licenses needed.....34
 - verifying license usage.....149
 - verifying licenses installed.....148, 151
 - license keys
 - components.....34
 - displaying (CLI).....149
 - status.....34
 - version.....34
 - licenses
 - adding (CLI).....146
 - adding (J-Web).....146
 - deleting (CLI).....150
 - deleting (J-Web).....150
 - displaying.....191
 - displaying (CLI).....148, 151
 - displaying (J-Web).....34, 143
 - displaying usage.....149
 - downloading (J-Web).....144
 - generating.....144
 - group.....35
 - infringement, preventing.....34
 - See also* license infringement
 - key.....34
 - See also* license keys
 - managing (J-Web).....34
 - overview.....33
 - saving (CLI).....145
 - updating (CLI).....146
 - verifying.....148, 151
 - limitations
 - software downgrade cannot be undone.....79
 - login lockout.....194
- M**
- managing
 - software.....10
 - manuals
 - comments on.....xvii
 - MD5 (Message Digest 5) checksum.....10
 - memory requirements
 - J Series routers.....7
 - multiple devices
 - deploying *See* autoinstallation
- N**
- naming conventions, software.....5
 - network.conf file, default for
 - autoinstallation.....29, 87
- P**
- parentheses, in syntax descriptions.....xvi
 - passwords
 - for downloading software upgrades.....52
- R**
- RARP, for autoinstallation.....87
 - recovery software installation.....10
 - registration form, for software upgrades.....44
 - release names.....6
 - remote server, upgrading from.....63
 - request system autorecovery state command.....166

request system download abort command.....	168
request system download clear command.....	169
request system download pause command.....	170
request system download resume command.....	171
request system download start command.....	172
request system firmware upgrade command.....	173
request system license add command.....	146
request system license add terminal command.....	146
request system license delete command.....	150
request system license save command.....	145
request system license update command.....	146, 174
request system partition compact-flash command.....	175
request system power-off fpc command.....	176
request system reboot.....	182
request system snapshot.....	10, 177
request system software abort in-service-upgrade command.....	180
request system software add	181
request system software rollback.....	10, 183
Reverse Address Resolution Protocol (RARP), for autoinstallation.....	87
reverting to a previous configuration file (J-Web).....	79
rolling back a configuration file, to downgrade software (CLI).....	79
router.conf file, for autoinstallation.....	29
routers storage media.....	8
Routing Engines storage media J Series routers.....	8
S	
saving licenses (CLI).....	145
Serial Line Address Resolution Protocol (SLARP), for autoinstallation.....	87
serial ports autoinstallation on.....	28
services gateway autoinstallation.....	31
Services Gateway licenses.....	33
Services Router licenses.....	33
SHA-1 (Secure Hash Algorithm) checksum.....	10
show chassis routing-engine.....	7
show chassis routing-engine bios.....	77
show chassis usb storage command.....	184
show system auto-snapshot command.....	187
show system autoinstallation status command.....	89
show system autorecovery state command.....	185
show system download command.....	189
show system license command.....	148, 151, 191
explanation.....	148, 151
show system license keys command.....	149
show system license usage command.....	149
explanation.....	149
show system login lockout command.....	194
show system snapshot media.....	97, 100, 195
show system storage.....	7
show system storage partitions.....	196, 198
show version.....	48
show version command.....	48
SLARP, for autoinstallation.....	87
software installation category change installation description.....	9
recovery installation description.....	10
standard installation description.....	9
software installation packages.....	5
standard Junos OS for J Series routers, domestic description.....	5
software packages upgrading individual.....	42
SRX Series licenses.....	33
SRX Series devices software upgrades.....	10
SRX Series Services Gateway.....	95 See storage
m e d i a	
auto bios upgrade methods.....	25
boot devices configuring (CLI).....	95
configuring (J-Web).....	95
Chassis Components Offline.....	161
Online.....	161
configuring boot devices.....	95
dual-root partitioning.....	19
halting a with J-Web.....	158
halting immediately (CLI)	158
halting with the CLI.....	158

Install Remote page	
field summary.....	95
installing earlier version of Junos OS	
with dual-root.....	71
installing software	
with CLI.....	72
with J-Web.....	72
Junos OS Release 10.0	
upgrading with dual-root.....	72
upgrading without dual-root.....	12
multiple devices, using snapshots to replicate configurations	
J-Web.....	95
rebooting (CLI).....	153
rebooting with J-Web	153
reboots.....	153, 158
recover of primary image.....	69
request system halt command.....	158
request system reboot command.....	153
request system snapshot command.....	95
show system storage partitions.....	75
Snapshot page.....	95
snapshots.....	95
software upgrade methods.....	12
<i>See also</i> boot devices	
standard software installation.....	9
status	
autoinstallation.....	89
license key.....	34
storage media.....	8
device names	
J Series routers.....	8
J Series routers.....	8
support, technical <i>See</i> technical support	
syntax conventions.....	xv
system	
login lockout.....	194
System Configuration Statement Hierarchy.....	101
system memory	
J Series routers.....	7
T	
technical support	
contacting JTAC.....	xvii
TFTP, for autoinstallation.....	29
Trivial File Transfer Protocol (TFTP), for	
autoinstallation.....	29
U	
updating	
licenses (CLI).....	146
upgrades	
downloading.....	52
installing (CLI).....	55
installing by uploading.....	55
installing from remote server.....	63
requirements.....	44
upgrading or downgrading Junos OS.....	42
URLs	
software downloads.....	52
usb.....	137
V	
validating software compatibility.....	53
verification	
active licenses.....	148, 151
autoinstallation.....	89
license usage.....	149
licenses	148, 151
version, license key.....	34

