



Junos[®] OS

Initial Configuration Guide for Security Devices

Release
12.1



Published: 2012-03-06

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

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.

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

Junos OS Initial Configuration Guide for Security Devices

Release 12.1

Copyright © 2012, Juniper Networks, Inc.

All rights reserved.

Revision History

March 2012—R1 Junos OS 12.1

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.

SOFTWARE LICENSE

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions. Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details. For complete product documentation, please see the Juniper Networks website at www.juniper.net/techpubs.

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.

Abbreviated Table of Contents

	About This Guide	xiii
Part 1	Device Configuration	
Chapter 1	Junos OS User Interface Overview	3
Chapter 2	Secure Web Access Configuration	11
Chapter 3	User Authentication and Access	19
Chapter 4	Telnet and SSH Device Control	43
Chapter 5	USB Modems for Remote Management Setup	51
Chapter 6	DHCP for IP Address Device Configuration	69
Chapter 7	DHCPv6 Local Server Configuration	91
Chapter 8	Autoinstallation Configuration	101
Chapter 9	Licenses	107
Part 2	Upgrades and Reboots	
Chapter 10	Junos OS Upgrades and Reboots for the SRX Series Devices	121
Chapter 11	Junos OS Upgrades and Reboots for J Series Devices	169
Part 3	Index	
	Index	191

Table of Contents

	About This Guide	xiii
	J Series and SRX Series Documentation and Release Notes	xiii
	Objectives	xiv
	Audience	xiv
	Supported Routing Platforms	xiv
	Document Conventions	xiv
	Documentation Feedback	xvi
	Requesting Technical Support	xvi
	Self-Help Online Tools and Resources	xvi
	Opening a Case with JTAC	xvii
Part 1	Device Configuration	
Chapter 1	Junos OS User Interface Overview	3
	Understanding the User Interfaces	3
	J-Web User Interface	3
	CLI	4
	J-Web User Interface	5
	Starting the J-Web User Interface	5
	Understanding the J-Web Interface Layout	6
	J-Web Commit Options Guidelines	8
	Getting Help in the J-Web User Interface	9
	Establishing J-Web Sessions	10
Chapter 2	Secure Web Access Configuration	11
	Secure Web Access Overview	11
	Generating SSL Certificates	12
	Generating an SSL Certificate Using the openssl Command	12
	Generating a Self-Signed SSL Certificate	12
	Manually Generating Self-Signed SSL Certificates	13
	Configuring Management Access	14
	Configuring Device Addresses	14
	Enabling Access Services	14
	Adding, Editing, and Deleting Certificates on the Device	15
	Example: Configuring Secure Web Access	16

Chapter 3	User Authentication and Access	19
	Understanding User Authentication Methods	19
	User Accounts	20
	Understanding User Accounts	20
	Example: Configuring a RADIUS Server for System Authentication	21
	Example: Configuring a TACACS+ Server for System Authentication	23
	Example: Configuring Authentication Order	26
	Login Classes	28
	Understanding Login Classes	28
	Permission Bits	29
	Denying or Allowing Individual Commands	31
	Example: Configuring New Users	31
	User Authentication	34
	Handling Authorization Failure	35
	Example: Configuring System Retry Options	36
	Template Accounts	39
	Understanding Template Accounts	39
	Example: Creating Template Accounts	40
Chapter 4	Telnet and SSH Device Control	43
	Securing the Console Port Configuration Overview	43
	Accessing Remote Devices with the CLI	44
	The telnet Command	44
	The ssh Command	45
	Configuring Password Retry Limits for Telnet and SSH Access	46
	Reverse Telnet	48
	Reverse Telnet Overview	48
	Reverse Telnet Options	48
	Reverse Telnet Restrictions	48
	Configuring Reverse Telnet and Reverse SSH	49
Chapter 5	USB Modems for Remote Management Setup	51
	USB Modem Interface Overview	51
	USB Modem Interfaces	52
	Dialer Interface Rules	52
	How the Device Initializes USB Modems	53
	USB Modem Configuration Overview	54
	Example: Configuring a USB Modem Interface	56
	Example: Configuring a Dialer Interface	59
	Example: Configuring a Dialer Interface for USB Modem Dial-In	62
	Remote Device Connection	64
	Configuring a Dial-Up Modem Connection Remotely	64
	Connecting to the Device Remotely	65
	USB Modem Administration	66
	Modifying USB Modem Initialization Commands	66
	Resetting USB Modems	67

Chapter 6	DHCP for IP Address Device Configuration	69
	DHCP Server, Client, and Relay Agent Overview	69
	DHCP Configuration Overview	70
	DHCP Operations	71
	Understanding DHCP Server Operation	71
	DHCP Options	72
	Compatibility with Autoinstallation	72
	Example: Configuring the Device as a DHCP Server	72
	Understanding DHCP Client Operation	78
	Example: Configuring the Device as a DHCP Client	79
	Understanding DHCP Relay Agent Operation	83
	Example: Configuring the Device as a BOOTP or DHCP Relay Agent	83
	DHCP Settings and Restrictions Overview	88
	Propagation of TCP/IP Settings for DHCP	88
	DHCP Conflict Detection and Resolution	88
	DHCP Interface Restrictions	89
Chapter 7	DHCPv6 Local Server Configuration	91
	DHCPv6 Server Overview	91
	Example: Configuring DHCPv6 Server Options	92
	Example: Configuring an Address-Assignment Pool	95
	Configuring Address-Assignment Pool and Address Features	98
	Configuring a Named Address Range for Dynamic Address Assignment	98
	Configuring Address-Assignment Pool Linking	98
	Configuring DHCP Client-Specific Attributes	99
	Configuring an Address-Assignment Pool for Router Advertisement	99
	Creating a Security Policy for DHCPv6	100
Chapter 8	Autoinstallation Configuration	101
	Autoinstallation Overview	101
	Supported Autoinstallation Interfaces and Protocols	101
	Typical Autoinstallation Process on a New Device	102
	Example: Configuring Autoinstallation	104
Chapter 9	Licenses	107
	Junos OS License Overview	107
	License Enforcement	107
	License Key Components	108
	License Management Fields Summary	108
	License Key Generation	109
	Generating a License Key	109
	Example: Adding a New License Key	110
	Example: Deleting a License Key	113
	Managing License Keys	115
	Updating License Keys	116
	Saving License Keys	116
	Displaying License Keys	116
	Downloading License Keys	116

Part 2

Chapter 10

Upgrades and Reboots

Junos OS Upgrades and Reboots for the SRX Series Devices	121
Understanding Junos OS Upgrades for SRX Series Devices	121
Understanding Junos OS Upgrade and Downgrade Procedures for on SRX Series Devices	122
Configuring External CompactFlash on SRX650 Devices	123
Junos OS Initial Installation and Upgrade Tasks	124
Preparing Your SRX Series Device for Junos OS Upgrades	124
Verifying Available Disk Space on SRX Series Devices	125
Downloading Junos OS Upgrades for SRX Series Devices	125
Preparing the USB Flash Drive to Upgrade Junos OS	126
Junos OS Upgrades, Downgrades, and Reboots	128
Junos OS Upgrade Methods on the SRX Series Devices	128
Installing Junos OS Upgrades from a Remote Server on the SRX Series Devices	129
Example: Installing Junos OS Upgrades on SRX Series Devices	130
Example: Downgrading Junos OS on SRX Series Devices	133
Example: Configuring Boot Devices for SRX Series Devices	135
Example: Rebooting SRX Series Devices	138
Example: Halting SRX Series Devices	140
Bringing Chassis Components Online and Offline on SRX Series Devices . .	141
Restarting the Chassis on SRX Series Devices	142
Upgrading the Boot Loader on SRX Series Devices	142
Installing Junos OS	143
Installing Junos OS Using TFTP on SRX Series Devices	144
Installing Junos OS Using a USB Device on SRX Series Devices	146
Installing Junos OS from the Boot Loader Using a USB Storage Device on an SRX Series Device	147
Download Manager	147
Understanding Download Manager	147
Overview	148
Using Download Manager to Upgrade Junos OS	148
Handling Errors	149
Considerations	149
Dual-Root Partitioning	150
Dual-Root Partitioning Scheme Overview	150
Boot Media and Boot Partition on the SRX Series Devices	151
Important Features of the Dual-Root Partitioning Scheme	151
Junos OS Release 10.0 or Later Upgrades with Dual-Root Partitioning on SRX Series Devices	152
Example: Installing Junos OS on SRX Series Devices Using the Partition Option	153
Junos OS Release 9.6 or Earlier Installation on SRX Series Devices with Dual-Root Partitioning	156
Understanding How the Primary Junos OS Image with Dual-Root Partitioning Recovers on SRX Series Devices	157
Reinstalling the Single-Root Partition Using “request system software add” Command	158

	Autorecovery	159
	Understanding Integrity Check and Autorecovery of Configuration, Licenses, and Disk Information	159
	Overview	159
	How Autorecovery Works	160
	How to Use Autorecovery	160
	Data That Is Backed Up in an Autorecovery	160
	Troubleshooting Alarms	161
	Considerations	161
	Auto BIOS Upgrade on SRX Series Devices	162
	Understanding Auto BIOS Upgrade Methods on the SRX Series Devices	162
	Disabling Auto BIOS Upgrade on SRX Series Devices	164
	Manual BIOS Upgrade on SRX Series Devices	164
	Understanding Manual BIOS Upgrade Using the Junos CLI	164
Chapter 11	Junos OS Upgrades and Reboots for J Series Devices	169
	Understanding Junos OS Upgrades for J Series Devices	169
	Junos OS Upgrades and Downloads	170
	Understanding Junos OS Upgrade and Downgrade Procedures for J Series Devices	170
	Junos OS Upgrade Packages	170
	Junos OS Recovery Packages	171
	Preparing Your J Series Services Router for Junos OS Upgrades	172
	Downloading Junos OS Upgrades for J Series Devices	173
	Installing Junos OS Upgrades from a Remote Server on J Series Devices	173
	Example: Installing Junos OS Upgrades on J Series Devices	175
	Example: Downgrading Junos OS on J Series Devices	177
	Boot Device Configuration	179
	Example: Configuring Boot Devices for J Series Devices	179
	Configuring a Boot Device to Receive Junos OS Failure Memory Snapshots in J Series Devices	182
	Example: Rebooting J Series Devices	183
	Example: Halting J Series Devices	184
	Chassis Configuration	186
	Bringing Chassis Components Online and Offline on J Series Devices	186
	Restarting the Chassis on J Series Devices	187
Part 3	Index	
	Index	191

About This Guide

This preface provides the following guidelines for using the *Junos OS Initial Configuration Guide for Security Devices*:

- [J Series and SRX Series Documentation and Release Notes on page xiii](#)
- [Objectives on page xiv](#)
- [Audience on page xiv](#)
- [Supported Routing Platforms on page xiv](#)
- [Document Conventions on page xiv](#)
- [Documentation Feedback on page xvi](#)
- [Requesting Technical Support on page xvi](#)

J Series and SRX Series Documentation and Release Notes

For a list of related J Series documentation, see <http://www.juniper.net/techpubs/software/junos-jseries/index-main.html>.

For a list of related SRX Series documentation, see <http://www.juniper.net/techpubs/hardware/srx-series-main.html>.

If the information in the latest release notes differs from the information in the documentation, follow the *Junos OS 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/>.

Juniper Networks supports a technical book program to publish books by Juniper Networks engineers and subject matter experts with book publishers around the world. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration using the Junos operating system (Junos OS) and Juniper Networks devices. In addition, the Juniper Networks Technical Library, published in conjunction with O'Reilly Media, explores improving network security, reliability, and availability using Junos OS configuration techniques. All the books are for sale at technical bookstores and book outlets around the world. The current list can be viewed at <http://www.juniper.net/books>.

Objectives

This guide describes how to use and configure key security features on J Series Services Routers and SRX Series Services Gateways running Junos OS. It provides conceptual information, suggested workflows, and examples where applicable.

Audience

This manual is designed for anyone who installs, sets up, configures, monitors, or administers a J Series Services Router or an SRX Series Services Gateway running Junos OS. The manual is intended for the following audiences:

- Customers with technical knowledge of and experience with networks and network security, the Internet, and Internet routing protocols
- Network administrators who install, configure, and manage Internet routers

Supported Routing Platforms

This manual describes features supported on J Series Services Routers and SRX Series Services Gateways running Junos OS.

Document Conventions

Table 1 on page xiv defines the 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.

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
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 important new terms. Identifies book 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 System Basics Configuration 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; interface names; 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)	Enclose optional keywords or variables.	stub <default-metric <i>metric</i> >;
(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 (<i>string1</i> <i>string2</i> <i>string3</i>)
# (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)	Enclose a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identify a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

J-Web GUI Conventions

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

Convention	Description	Examples
Bold text like this	Represents J-Web 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.
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web 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 send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release 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 JNASC support contract, or are covered under warranty, and need postsales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at <http://www.juniper.net/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/>
- Find product documentation: <http://www.juniper.net/techpubs/>

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

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

Opening a Case with JTAC

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

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

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

PART 1

Device Configuration

- [Junos OS User Interface Overview on page 3](#)
- [Secure Web Access Configuration on page 11](#)
- [User Authentication and Access on page 19](#)
- [Telnet and SSH Device Control on page 43](#)
- [USB Modems for Remote Management Setup on page 51](#)
- [DHCP for IP Address Device Configuration on page 69](#)
- [DHCPv6 Local Server Configuration on page 91](#)
- [Autoinstallation Configuration on page 101](#)
- [Licenses on page 107](#)

CHAPTER 1

Junos OS User Interface Overview

- [Understanding the User Interfaces on page 3](#)
- [J-Web User Interface on page 5](#)

Understanding the User Interfaces

You can use two user interfaces to configure, monitor, manage, and troubleshoot your device—the J-Web user interface and the command-line interface (CLI) for Junos OS.



NOTE: Other user interfaces facilitate the configuration of one or, in some cases, many devices on the network through a common API. Among the supported interfaces are the Junos Scope and Session and Resource Control (SRC) applications.

You can operate the device either in secure or router context. With the J-Web user interface and the CLI, you configure the routing protocols that run on the device and the device security features, including stateful firewall policies, Network Address Translation (NAT) attack prevention screens, Application Layer Gateways (ALGs), and IPsec VPNs. You also set the properties of its network interfaces. After activating a software configuration, you can use either user interface to monitor the system and the protocol traffic passing through the device, manage operations, and diagnose protocol and network connectivity problems.

This section contains the following topics:

- [J-Web User Interface on page 3](#)
- [CLI on page 4](#)

J-Web User Interface

The J-Web user interface allows you to monitor, configure, troubleshoot, and manage your device by means of a Web browser enabled with Hypertext Transfer Protocol (HTTP) or HTTP over Secure Sockets Layer (HTTPS). J-Web provides access to all the configuration statements supported by the device, so you can fully configure it without using the CLI editor.

You can perform the following tasks with the J-Web user interface:

- Dashboard (SRX Series devices only)—Views high-level details of Chassis View, system identification, resource utilization, security resources, system alarms, file usage, login sessions, chassis status, threats activity, and storage usage.
- Configuring—View the current configurations at a glance, configure the device, and manage configuration files. The J-Web user interface provides the following configuration methods:
 - Edit a graphical version of the Junos OS CLI configuration statements and hierarchy.
 - Edit the configuration in a text file.
 - Upload a configuration file.
 - Use wizards to configure basic setup, firewall, VPN, and NAT settings on SRX100, SRX210, SRX220, SRX240, and SRX650 devices.

The J-Web user interface also allows you to manage configuration history and set a rescue configuration.

- Monitoring—Display the current configuration and information about the system, interfaces, chassis, routing protocols, routing tables, routing policy filters, and other features.
- Managing—Manage log, temporary, and core (crash) files and schedule reboots on your devices. You can also manage software packages and licenses, and copy a snapshot of the system software to a backup device.
- Diagnosing—Diagnose routing problems by running the ping or traceroute diagnostic tool. The diagnostic tools also allow you to capture and analyze control traffic on the devices.
- Configuring and monitoring events—Filter and view system log messages that record events occurring on the device. You can configure files to log system log messages and also assign attributes, such as severity levels, to messages.
- Configuring and monitoring alarms—Monitor and diagnose the device by monitoring active alarms that alert you to the conditions on a network interface. You can also set the conditions that trigger alarms on an interface.

CLI

The CLI is a straightforward command-line interface in which you type commands on a line and press Enter to execute them. The CLI provides command Help, command completion, and Emacs-style keyboard sequences for moving around on the command line and scrolling through a buffer of recently executed commands.

The CLI has two modes:

- Operational mode—Complete set of commands to control the CLI environment, monitor and troubleshoot network connectivity, manage the device, and enter configuration mode.
- Configuration mode—Complete set of commands to configure the device. This topic refers to configuration mode as the *CLI configuration editor*.

- Related Documentation**
- [Starting the J-Web User Interface on page 5](#)
 - [Understanding the J-Web Interface Layout on page 6](#)
 - [Getting Help in the J-Web User Interface on page 9](#)
 - [SRC PE Getting Started Guide](#)
 - [Junos OS CLI User Guide](#)
 - [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
 - [Junos Scope Software User Guide](#)

J-Web User Interface

This section contains the following topics:

- [Starting the J-Web User Interface on page 5](#)
- [Understanding the J-Web Interface Layout on page 6](#)
- [J-Web Commit Options Guidelines on page 8](#)
- [Getting Help in the J-Web User Interface on page 9](#)
- [Establishing J-Web Sessions on page 10](#)

Starting the J-Web User Interface

Before you start the user interface, you must perform the initial device configuration described in the Getting Started Guide for your device. After the initial configuration, you use your username and password, and the hostname or IP address of the device, to start the user interface.

[Table 3 on page 5](#) shows the maximum number of concurrent Web sessions on SRX100, SRX210, SRX220, SRX240, and SRX650 devices.

Table 3: Concurrent Web Sessions on SRX Series Devices

SRX100	SRX210	SRX220	SRX240	SRX650
3	3	3	5	5

To start the J-Web user interface:

1. Launch your HTTP-enabled or HTTPS-enabled Web browser.

To use HTTPS, you must have installed the certificate provided by the device.



NOTE: If the device is running the worldwide version of the Junos OS and you are using the Microsoft Internet Explorer Web browser, you must disable the Use SSL 3.0 option in the Web browser to access the device.

2. Type **http://** or **https://** in your Web browser followed by the hostname or IP address of the device, and press Enter.

The J-Web login page appears.

3. Type your username and password, and click **Log In**.

To correct or change the username or password you typed, click **Reset**, type the new entry or entries, and click **Log In**.



NOTE: The default username is **root** with no password. You must change this during initial configuration or the system does not accept the configuration.

To explicitly terminate a J-Web session at any time, click **Logout** in the top pane.

Related Documentation

- [Understanding the User Interfaces on page 3](#)
- [Understanding the J-Web Interface Layout on page 6](#)
- [J-Web Commit Options Guidelines on page 8](#)
- [Getting Help in the J-Web User Interface on page 9](#)
- [Establishing J-Web Sessions on page 10](#)
- [J-Web Interface User Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

Understanding the J-Web Interface Layout

The top pane of the J-Web user interface comprises the following elements:

- *hostname—model*—The hostname and model of the device are displayed in the upper-left corner.
- Logged in as: *username*—The username you used to log in to the device is displayed in the upper-left corner.
- Chassis—The chassis view of the device.
- Commit Options—A set of global options that allow you to commit multiple changes at the same time.
 - Commit—Commits the candidate configuration of the current user session, along with changes from other user sessions.
 - Compare—Displays the XML log of pending uncommitted configurations on the device.

- **Discard**—Discards the candidate configuration of the current user session, along with changes from other user sessions.
- **Preference**—Indicates your choice of committing all global configurations together or committing each configuration change immediately. The two behavior modes to which you can set your commit options are:
 - **Validate and commit configuration changes**—Sets the system to force an immediate commit on every screen after every configuration change.
 - **Validate configuration changes**—Loads all the configuration changes for an accumulated single commit. If there are errors in loading the configuration, the errors are logged. This is the default mode.
- **Help**—Links to information on Help and the J-Web user interface.
 - **Help Contents**—Displays context-sensitive Help topics.
 - **About**—Displays information about the J-Web user interface, such as the version number.
- **Logout**—The Logout link, which ends your current login session and returns you to the login page, is available in the upper-right corner.
- **Taskbar**—A menu of J-Web tasks is displayed as tabs across the top of the J-Web user interface. Select a tab to access a task.
 - **Dashboard**—Displayd current activity on the system.
 - **Configure**—Configures the device and views configuration history.
 - **Monitor**—Displays information about configuration and hardware on the device.
 - **Maintain**—Manages files and licenses, upgrades software, and reboots the device.
 - **Troubleshoot**—Troubleshoots network connectivity problems.

The main pane of the J-Web user interface includes the following elements to help you configure the device:

- **Red asterisk (*)**—Appears next to all required fields.
- **Help (?) icon**—Displays useful information when you move the cursor over the question mark. This Help displays field-specific information, such as the definition, format, and valid range of the field.

The left pane of the J-Web user interface displays subtasks related to the selected task in the J-Web taskbar.

**Related
Documentation**

- [Understanding the User Interfaces on page 3](#)
- [Starting the J-Web User Interface on page 5](#)
- [J-Web Commit Options Guidelines on page 8](#)
- [Getting Help in the J-Web User Interface on page 9](#)

- [Establishing J-Web Sessions on page 10](#)
- [J-Web Interface User Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

J-Web Commit Options Guidelines

Using the J-Web Commit Preference, you can configure the commit options either to commit all global configurations together or to commit each configuration change immediately. Do one of the following to commit a configuration:

- Set Commit Preference to **Validate and commit configuration changes**, and then click **OK**.
- Set Commit Preference to **Validate configuration changes**, click **OK** to check your configuration and save it as a candidate configuration, and then click **Commit Options>Commit**.

For example, suppose you want to delete a firewall and add a new one.

- If Commit Preference is set to **Validate and commit configuration changes**, then you would need to commit your changes twice for each action.
- If Commit Preference is set to **Validate configuration changes**, then you work in a copy of the current configuration to create a candidate configuration. The changes you make to the candidate configuration are visible through the user interface immediately, allowing other users to edit those configurations, but the changes do not take effect on the device platform until you commit them. When you commit the configuration, the candidate file is checked for proper syntax, activated, and marked as the current, operational software configuration file. If multiple users are editing the configuration when you commit the candidate configuration, changes made by all the users take effect.

You use the single commit feature to commit all your configurations in J-Web simultaneously. This helps to reduce the time J-Web takes to commit configurations because when changes are committed at every step, rollback configurations pile up quickly.



NOTE: If you end a session with a particular Commit Preference, the subsequent sessions for that particular browser will automatically come up with the preference you previously selected. If you start the subsequent session on a different browser, the session will come up with the default commit preference.



NOTE: There are some pages whose configurations would need to be committed immediately. For such pages, even if you configure the commit options to perform a single global commit for them, the system displays appropriate information notification windows to remind you to commit your changes immediately. Examples of such pages are Switching, Interfaces, and Class of Service.

Related Documentation

- [Understanding the User Interfaces on page 3](#)
- [Starting the J-Web User Interface on page 5](#)
- [Understanding the J-Web Interface Layout on page 6](#)
- [Getting Help in the J-Web User Interface on page 9](#)
- [Establishing J-Web Sessions on page 10](#)
- [J-Web Interface User Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

Getting Help in the J-Web User Interface

To get Help in the J-Web user interface, use the following methods:

- **Field-sensitive Help**—Move the cursor over the question mark (?) next to the field for which you want more information. Typically, this Help includes one line of information about what this field does or what you must enter in a given text box. For example, Help for the Peer Autonomous System Number text box states, “The value should be a number between 1 and 65535.”
- **Context-sensitive Help**—Click **Help** in the taskbar to open a separate page displaying the summary of all the fields on that page. To exit Help, close the page. You can navigate Help pages using hypertext links connecting related topics, or click the following options (if available) at the top and bottom of each page.
 - **Prev**—Access the previous page.
 - **Next**—Access the next page.
 - **Report an Error**—Access a form for providing feedback.
- **Wizard Help** (SRX100, SRX210, SRX220, SRX240, and SRX650)—Use the Firewall Policy, VPN, and NAT wizards to perform basic configurations. Click a field in a wizard page to display information about that field in the lower left corner of the wizard page.

Related Documentation

- [Understanding the User Interfaces on page 3](#)
- [Starting the J-Web User Interface on page 5](#)
- [Understanding the J-Web Interface Layout on page 6](#)
- [J-Web Commit Options Guidelines on page 8](#)

- [Establishing J-Web Sessions on page 10](#)
- [J-Web Interface User Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

Establishing J-Web Sessions

You establish a J-Web session through an HTTP-enabled or HTTPS-enabled Web browser. The HTTPS protocol, which uses 128-bit encryption, is available only in domestic versions of the Junos OS. To use HTTPS, you must have installed the certificate provided by the device.

When you attempt to log in through the J-Web interface, the system authenticates your username with the same methods used for Telnet and SSH.

The device can support multiple J-Web sessions for a single user who logs in to each session. However, if a single user attempts to launch multiple J-Web *windows*—for example, by right-clicking a link to launch another instance of a Web browser—the session can have unpredictable results.

If the device does not detect any activity through the J-Web user interface for 15 minutes, the session times out and is terminated. You must log in again to begin a new session.

To explicitly terminate a J-Web session at any time, click **Logout** in the top pane.

Related Documentation

- [Understanding the User Interfaces on page 3](#)
- [Starting the J-Web User Interface on page 5](#)
- [Understanding the J-Web Interface Layout on page 6](#)
- [J-Web Commit Options Guidelines on page 8](#)
- [Getting Help in the J-Web User Interface on page 9](#)
- [J-Web Interface User Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

CHAPTER 2

Secure Web Access Configuration

- [Secure Web Access Overview on page 11](#)
- [Generating SSL Certificates on page 12](#)
- [Configuring Management Access on page 14](#)
- [Example: Configuring Secure Web Access on page 16](#)

Secure Web Access Overview

You can manage a Juniper Networks device remotely through the J-Web interface. To communicate with the device, the J-Web interface uses the Hypertext Transfer Protocol (HTTP). HTTP allows easy Web access but no encryption. The data that is transmitted between the Web browser and the device by means of HTTP is vulnerable to interception and attack. To enable secure Web access, the Juniper Networks devices support HTTP over Secure Sockets Layer (HTTPS). You can enable HTTP or HTTPS access on specific interfaces and ports as needed.

The Juniper Networks device uses the Secure Sockets Layer (SSL) protocol to provide secure device management through the Web interface. SSL uses public-private key technology that requires a paired private key and an authentication certificate for providing the SSL service. SSL encrypts communication between your device and the Web browser with a session key negotiated by the SSL server certificate.

An SSL certificate includes identifying information such as a public key and a signature made by a certificate authority (CA). When you access the device through HTTPS, an SSL handshake authenticates the server and the client and begins a secure session. If the information does not match or the certificate has expired, you cannot access the device through HTTPS.

Without SSL encryption, communication between your device and the browser is sent in the open and can be intercepted. We recommend that you enable HTTPS access on your WAN interfaces.

HTTP access is enabled by default on the built-in management interfaces. By default, HTTPS access is supported on any interface with an SSL server certificate.

Related Documentation

- [Generating an SSL Certificate Using the openssl Command on page 12](#)
- [Generating a Self-Signed SSL Certificate on page 12](#)

- [Configuring Device Addresses on page 14](#)
- [Example: Configuring Secure Web Access on page 16](#)
- [J-Web Interface User Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

Generating SSL Certificates

To enable secure Web access, you must first establish basic connectivity, and then generate a digital SSL certificate and enable HTTPS access on the device. You can generate the SSL certificate on the Juniper Networks Services Gateway or by using another device.

This section contains the following topics:

- [Generating an SSL Certificate Using the openssl Command on page 12](#)
- [Generating a Self-Signed SSL Certificate on page 12](#)
- [Manually Generating Self-Signed SSL Certificates on page 13](#)

Generating an SSL Certificate Using the openssl Command

To generate an SSL certificate using the **openssl** command:

1. Enter **openssl** in the CLI. The **openssl** command generates a self-signed SSL certificate in privacy-enhanced mail (PEM) format. It writes the certificate and an unencrypted 1024-bit RSA private key to the specified file.



NOTE: Run this command on a LINUX or UNIX device because Juniper Networks Services Gateways do not support the **openssl** command.

```
% openssl req -x509 -nodes -newkey rsa:1024 -keyout filename.pem -out  
filename.pem
```

Replace **filename** with the name of a file in which you want the SSL certificate to be written—for example, **new.pem**.

2. When prompted, type the appropriate information in the identification form. For example, type **US** for the country name.
3. Display the contents of the file **new.pem**.

```
cat new.pem
```

Copy the contents of this file for installing the SSL certificate.

Generating a Self-Signed SSL Certificate

To generate a self-signed SSL certificate on Juniper Networks devices:

1. Establish basic connectivity.

2. Reboot the system. The self-signed certificate is automatically generated at bootup time.

```
user@host> request system reboot
Reboot the system ? [yes,no] yes
```

3. Specify **system-generated-certificate** under HTTPS Web management.

```
[edit]
user@host# show system services web-management https
system-generated-certificate
```

Manually Generating Self-Signed SSL Certificates

To manually generate a self-signed SSL certificate on Juniper Networks devices:

1. Establish basic connectivity.
2. If you have root login access, you can manually generate the self-signed certificate by using the following commands:

```
root@host> request security pki generate-size 512 certificate-id certname
```

Generated key pair sslcert, key size 512 bits

```
root@host> request security pki local-certificate generate-self-signed certificate-id
cert-name email email domain-name domain-name ip-address ip-address subject
"DC= Domain name, CN= Common-Name, OU= Organizational-Unit-name, O=
Organization-Name, ST= state, C= Country"
```

Self-signed certificate generated and loaded successfully



NOTE: When generating the certificate, you must specify the subject, e-mail address, and either domain-name or ip-address.

3. Specify **local-certificate** under HTTPS Web management.

```
[edit]
root@host# show system services web-management https local-certificate certname
```

Related Documentation

- [Secure Web Access Overview on page 11](#)
- [Configuring Device Addresses on page 14](#)
- [Enabling Access Services on page 14](#)
- [Adding, Editing, and Deleting Certificates on the Device on page 15](#)
- [Example: Configuring Secure Web Access on page 16](#)
- [J-Web Interface User Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

Configuring Management Access

To configure device access options, such as HTTPS and certificates, select **Configure>System Properties>Management Access** in the J-Web user interface.

This section contains the following topics:

- [Configuring Device Addresses on page 14](#)
- [Enabling Access Services on page 14](#)
- [Adding, Editing, and Deleting Certificates on the Device on page 15](#)

Configuring Device Addresses

You can use the Management tab to configure IPv4 and loopback addresses on the device.

To configure IPv4 and loopback addresses:

1. In the J-Web user interface, select **Configure>System Properties>Management Access**.
2. Click **Edit**. The Edit Management Access dialog box appears.
3. Select the **Management** tab.
4. If you want to enable a loopback address for the device, enter an address and corresponding subnet mask in the **Loopback address** section.
5. If you want to enable an IPv4 address for the device, select **IPv4 address** and enter a corresponding management port, subnet mask, and default gateway.
6. Click **OK** to save the configuration or **Cancel** to clear it.

Enabling Access Services

You can use the Services tab to specify the type of connections that users can make to the device. For instance, you can enable secure HTTPS sessions to the device or enable access to the Junos XML protocol XML scripting API.

To enable access services:

1. In the J-Web user interface, select **Configure>System Properties>Management Access**.
2. Click **Edit**. The Edit Management Access dialog box appears.
3. Select the **Services** tab.
4. If you want to enable users to create secure Telnet or secure SSH connections to the device, select **Enable Telnet** or **Enable SSH**.
5. If you want to enable access to the Junos XML protocol XML scripting API, select **Enable Junos XML protocol over clear text** or **Enable Junos XML protocol over SSL**.

If you enable Junos XML protocol over SSL, select the certificate you want to use for encryption from the **Junos XML protocol certificate** drop-down list.

6. Select **Enable HTTP** if you want users to connect to device interfaces over an HTTP connection. Then specify the interfaces that should use the HTTP connection:
 - **Enable on all interfaces**—Select this option if you want to enable HTTP on all device interfaces.
 - **Selected interfaces**—Use the arrow buttons to populate this list with individual interfaces if you want to enable HTTP on only some of the device interfaces.
7. If you want users to connect to device interfaces over a secure HTTPS connection, select **Enable HTTPS**. Then select which certificate you want to use to secure the connection from the **HTTPS certificates** list and specify the interfaces that should use the HTTPS connection:
 - **Enable on all interfaces**—Select this option if you want to enable HTTPS on all device interfaces.
 - **Selected interfaces**—Use the arrow buttons to populate this list with individual interfaces if you want to enable HTTPS on only some of the device interfaces.
8. Click **OK** to save the configuration or **Cancel** to clear it.

To verify that Web access is enabled correctly, connect to the device using one of the following methods:

- For HTTP access—In your Web browser, type **http://URL** or **http://IP address**.
- For HTTPS access—In your Web browser, type **https://URL** or **https://IP address**.
- For SSL Junos XML protocol access—A Junos XML protocol client such as Junos Scope is required.

Adding, Editing, and Deleting Certificates on the Device

You can use the Certificates tab to upload SSL certificates to the device, edit existing certificates on the device, or delete certificates from the device. You can use the certificates to secure HTTPS and Junos XML protocol sessions.

To add, edit, or delete a certificate:

1. In the J-Web user interface, select **Configure>System Properties>Management Access**.
2. Click **Edit**. The Edit Management Access dialog box appears.
3. Select the **Certificates** tab.
4. Choose one of the following options:
 - If you want to add a new certificate, click **Add**. The Add Certificate section is expanded.
 - If you want to edit the information for an existing certificate, select it and click **Edit**. The Edit Certificate section is expanded.

- If you want to delete an existing certificate, select it and click **Delete**. (You can skip the remaining steps in this section.)
- 5. In the **Certificate Name** box, type a name—for example, **new**.
- 6. In the **Certificate content** box, paste the generated certificate and RSA private key.
- 7. Click **Save**.
- 8. Click **OK** to save the configuration or **Cancel** to clear it.

Related Documentation

- [Secure Web Access Overview on page 11](#)
- [Generating an SSL Certificate Using the openssl Command on page 12](#)
- [Generating a Self-Signed SSL Certificate on page 12](#)
- [Manually Generating Self-Signed SSL Certificates on page 13](#)
- [Example: Configuring Secure Web Access on page 16](#)
- [J-Web Interface User Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

Example: Configuring Secure Web Access

This example shows how to configure secure Web access on your device.

- [Requirements on page 16](#)
- [Overview on page 16](#)
- [Configuration on page 17](#)
- [Verification on page 18](#)

Requirements

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



.....
NOTE: You can enable HTTPS access on specified interfaces. If you enable HTTPS without specifying an interface, HTTPS is enabled on all interfaces.
.....

Overview

In this example, you import the SSL certificate that you have generated as a new and private key in PEM format. You then enable HTTPS access and specify the SSL certificate to be used for authentication. Finally, you specify the port as 8443 on which HTTPS access is to be enabled.

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 security certificates local new load-key-file /var/tmp/new.pem
set system services web-management https local-certificate new port 8443
```

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* in the [Junos OS CLI User Guide](#).

To configure secure Web access on your device:

1. Import the SSL certificate and private key.

```
[edit security]
user@host# set certificates local new load-key-file /var/tmp/new.pem
```

2. Enable HTTPS access and specify the SSL certificate and port.

```
[edit system]
user@host# set services web-management https local-certificate new port 8443
```

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

```
[edit]
user@host# show security
certificates {
  local {
    new {
      "-----BEGIN RSA PRIVATE KEY-----\nMIICXQIBAAKBgQC/C5UI4frNqbi
      qPwbTiOkJvqoDw2YgYse0Z5zzVJyErgSg954T\nEuHM67Ck8hAOrCnb0YO+SY
      Y5rCXLf4+2s8k9EypLtYRw/Ts66DZoXI4viqE7HSsK\n5sQw/UDBlw7/MJ+OpA
      ... KYiFf4CbBBbjlMQJ0HFudW6ISVBslONkzX+FT\ni95ddka6ilRnArEb4VFCRh+
      e1QBdp1UjziYf7NuzDx4Z\n -----END RSA PRIVATE KEY-----\n-----BEGIN
      CERTIFICATE-----\nMIIDjDCCAvWgAwIBAgIBADANBgkqhkiG9w0BAQQ ...
      FADCBkTElMAkGAIUEBhMCdXMx\nCzAJBgNVBAGTAzAmNhMRlWEAYDVQQHEWlzdW5ue
      HB1YnMxDTALBgNVBAMTBGpucHlxdAIBgkqhkiG9w0w0BCQEFW5iaGFyZ2F2YUB
      fLUYAnBYmsYWOH\n -----END CERTIFICATE-----\n"; ## SECRET-DATA
    }
  }
}
```

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

Verification

Confirm that the configuration is working properly.

- [Verifying an SSL Certificate Configuration on page 18](#)
- [Verifying a Secure Access Configuration on page 18](#)

Verifying an SSL Certificate Configuration

Purpose Verify the SSL certificate configuration.

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

Verifying a Secure Access Configuration

Purpose Verify the secure access configuration.

Action From operational mode, enter the **show system services** command. The following sample output displays the sample values for secure Web access:

```
[edit]
user@host# show system services
web-management {
  http;
  https {
    port 8443;
    local-certificate new;
  }
}
```

- Related Documentation**
- [Secure Web Access Overview on page 11](#)
 - [Generating an SSL Certificate Using the openssl Command on page 12](#)
 - [Generating a Self-Signed SSL Certificate on page 12](#)
 - [Configuring Device Addresses on page 14](#)
 - [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
 - [Junos OS Interfaces Configuration Guide for Security Devices](#)

CHAPTER 3

User Authentication and Access

- [Understanding User Authentication Methods on page 19](#)
- [User Accounts on page 20](#)
- [Login Classes on page 28](#)
- [User Authentication on page 34](#)
- [Template Accounts on page 39](#)

Understanding User Authentication Methods

Junos OS supports three methods of user authentication: local password authentication, Remote Authentication Dial-In User Service (RADIUS), and Terminal Access Controller Access Control System Plus (TACACS+).

With local password authentication, you configure a password for each user allowed to log into the device.

RADIUS and TACACS+ are authentication methods for validating users who attempt to access the device using Telnet. Both are distributed client/server systems—the RADIUS and TACACS+ clients run on the device, and the server runs on a remote network system.

You can configure the device to use RADIUS or TACACS+ authentication, or both, to validate users who attempt to access the device. If you set up both authentication methods, you also can configure which method the device will try first.

Related Documentation

- [Understanding User Accounts on page 20](#)
- [Understanding Login Classes on page 28](#)
- [Understanding Template Accounts on page 39](#)
- [*Junos OS Security Configuration Guide*](#)
- [*Junos OS System Basics Configuration Guide*](#)
- [*Junos OS Feature Support Reference for SRX Series and J Series Devices*](#)

User Accounts

This section contains the following topics:

- [Understanding User Accounts on page 20](#)
- [Example: Configuring a RADIUS Server for System Authentication on page 21](#)
- [Example: Configuring a TACACS+ Server for System Authentication on page 23](#)
- [Example: Configuring Authentication Order on page 26](#)

Understanding User Accounts

User accounts provide one way for users to access the device. Users can access the device without accounts if you configured RADIUS or TACACS+ servers. After you have created an account, the device creates a home directory for the user. An account for the user **root** is always present in the configuration. For each user account, you can define the following:

- Username—Name that identifies the user. It must be unique within the device. Do not include spaces, colons, or commas in the username.
- User's full name—If the full name contains spaces, enclose it in quotation marks (" "). Do not include colons or commas.
- User identifier (UID)—Numeric identifier that is associated with the user account name. The identifier range from 100 through 64,000 and must be unique within the device. If you do not assign a UID to a username, the software assigns one when you commit the configuration, preferring the lowest available number.
- User's access privilege—You can create login classes with specific permission bits or use one of the predefined classes.
- Authentication method or methods and passwords that the user can use to access the device—You can use SSH or an MD5 password, or you can enter a plain-text password that Junos OS encrypts using MD5-style encryption before entering it in the password database. If you configure the plain-text-password option, you are prompted to enter and confirm the password.

Related Documentation

- [Understanding User Authentication Methods on page 19](#)
- [Example: Configuring a RADIUS Server for System Authentication on page 21](#)
- [Example: Configuring a TACACS+ Server for System Authentication on page 23](#)
- [Example: Configuring Authentication Order on page 26](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

Example: Configuring a RADIUS Server for System Authentication

This example shows how to configure a RADIUS server for system authentication.

- [Requirements on page 21](#)
- [Overview on page 21](#)
- [Configuration on page 21](#)
- [Verification on page 23](#)

Requirements

Before you begin:

- Perform the initial device configuration. See the Getting Started Guide for your device.
- Configure at least one RADIUS server. See RADIUS Authentication and Accounting Servers Configuration Overview.

Overview

In this example, you add a new RADIUS server with an IP address of 172.16.98.1 and specify the shared secret password of the RADIUS server as Radiussecret1. The secret is stored as an encrypted value in the configuration database. Finally, you specify the source address to be included in the RADIUS server requests by the device. In most cases you can use the loopback address of the device, which in this example is 10.0.0.1.

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 radius-server address 172.16.98.1
set system radius-server 172.16.98.1 secret Radiussecret1
set system radius-server 172.16.98.1 source-address 10.0.0.1
```

GUI Step-by-Step Procedure

To configure a RADIUS server for system authentication:

1. In the J-Web user interface, select **Configure>System Properties>User Management**.
2. Click **Edit**. The Edit User Management dialog box appears.
3. Select the **Authentication Method and Order** tab.
4. In the RADIUS section, click **Add**. The Add Radius Server dialog box appears.
5. In the IP Address box, type the server's 32-bit IP address.
6. In the Password and Confirm Password boxes, type the secret password for the server and verify your entry.
7. In the Server Port box, type the appropriate port.
8. In the Source Address box, type the source IP address of the server.

9. In the Retry Attempts box, specify the number of times that the server should try to verify the user's credentials.
10. In the Time Out box, specify the amount of time (in seconds) the device should wait for a response from the server.
11. Click **OK** to check your configuration and save it as a candidate configuration.
12. 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](#) in the *Junos OS CLI User Guide*.

To configure a RADIUS server for system authentication:

1. Add a new RADIUS server and set its IP address.

```
[edit system]
user@host# set radius-server address 172.16.98.1
```
2. Specify the shared secret (password) of the RADIUS server.

```
[edit system]
user@host# set radius-server 172.16.98.1 secret Radiussecret1
```
3. Specify the device's loopback address source address.

```
[edit system]
user@host# set radius-server 172.16.98.1 source-address 10.0.0.1
```

Results From configuration mode, confirm your configuration by entering the **show system radius-server** 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 radius-server
radius-server 172.16.98.1 {
  secret Radiussecret1;
  source-address 10.0.0.1;
}
```

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



NOTE: To completely set up RADIUS authentication, you must create user template accounts and specify a system authentication order. Do one of the following tasks:

- Configure a system authentication order. See [“Example: Configuring Authentication Order” on page 26](#).
 - Configure a user. See [“Example: Configuring New Users” on page 31](#).
 - Configure local user template accounts. See [“Example: Creating Template Accounts” on page 40](#).
-

Verification

Confirm that the configuration is working properly.

- [Verifying the RADIUS Server System Authentication Configuration on page 23](#)

Verifying the RADIUS Server System Authentication Configuration

Purpose Verify that the RADIUS server has been configured for system authentication.

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

Related Documentation

- [Understanding User Authentication Methods on page 19](#)
- [Understanding User Accounts on page 20](#)
- [Example: Configuring a TACACS+ Server for System Authentication on page 23](#)
- [Understanding Login Classes on page 28](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

Example: Configuring a TACACS+ Server for System Authentication

This example shows how to configure a TACACS+ server for system authentication.

- [Requirements on page 23](#)
- [Overview on page 23](#)
- [Configuration on page 23](#)
- [Verification on page 25](#)

Requirements

Before you begin:

- Perform the initial device configuration. See the Getting Started Guide for your device.
- Configure at least one TACACS+ server. See Configuring TACACS+ Authentication.

Overview

In this example, you set the IP address to 172.16.98.24 and the shared secret password of the TACACS+ server to Tacacssecret1. The secret password is stored as an encrypted value in the configuration database. You then set the loopback source address as 10.0.0.1

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 tacplus-server address 172.16.98.24
set system tacplus-server 172.16.98.24 secret Tacacssecret1
set system tacplus-server 172.16.98.24 source-address 10.0.0.1
```

GUI Step-by-Step Procedure

To configure a TACACS+ server for system authentication:

1. In the J-Web user interface, select **Configure>System Properties>User Management**.
2. Click **Edit**. The Edit User Management dialog box appears.
3. Select the **Authentication Method and Order** tab.
4. In the TACACS section, click **Add**. The Add TACACS Server dialog box appears.
5. In the IP Address box, type the server's 32-bit IP address.
6. In the Password and Confirm Password boxes, type the secret password for the server and verify your entry.
7. In the Server Port box, type the appropriate port.
8. In the Source Address box, type the source IP address of the server.
9. In the Retry Attempts box, specify the number of times that the server should try to verify the user's credentials.
10. In the Time Out box, specify the amount of time (in seconds) the device should wait for a response from the server.
11. Click **OK** to check your configuration and save it as a candidate configuration.
12. 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 in the [Junos OS CLI User Guide](#).

To configure a TACACS+ server for system authentication:

1. Add a new TACACS+ server and set its IP address.

```
[edit system]
user@host# set tacplus-server address 172.16.98.24
```
2. Specify the shared secret (password) of the TACACS+ server.

```
[edit system]
user@host# set tacplus-server 172.16.98.24 secret Tacacssecret1
```
3. Specify the device's loopback address as the source address.

```
[edit system]
user@host# set tacplus-server 172.16.98.24 source-address 10.0.0.1
```

Results From configuration mode, confirm your configuration by entering the **show system tacplus-server** 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 tacplus-server
tacplus-server 172.16.98.24 {
  secret Tacacssecret1;
  source-address 10.0.0.1;
}
```

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



NOTE: To completely set up TACACS+ authentication, you must create user template accounts and specify a system authentication order. Do one of the following tasks:

- Configure a system authentication order. See [“Example: Configuring Authentication Order” on page 26](#).
- Configure a user. See [“Example: Configuring New Users” on page 31](#).
- Configure local user template accounts. See [“Example: Creating Template Accounts” on page 40](#).

Verification

Confirm that the configuration is working properly.

- [Verifying the TACACS+ Server System Authentication Configuration on page 25](#)

Verifying the TACACS+ Server System Authentication Configuration

Purpose Verify that the TACACS+ server has been configured for system authentication.

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

Related Documentation

- [Understanding User Authentication Methods on page 19](#)
- [Understanding User Accounts on page 20](#)
- [Example: Configuring a RADIUS Server for System Authentication on page 21](#)
- [Understanding Login Classes on page 28](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

Example: Configuring Authentication Order

This example shows how to configure authentication order.

- [Requirements on page 26](#)
- [Overview on page 26](#)
- [Configuration on page 26](#)
- [Verification on page 27](#)

Requirements

Before you begin, perform the initial device configuration. See the Getting Started Guide for your device.

Overview

You can configure the authentication methods that the device uses to verify that a user can gain access. For each login attempt, the device tries the authentication methods in order, starting with the first one, until the password matches. If you do not configure system authentication, users are verified based on their configured local passwords.

This example configures the device to attempt user authentication with the local password first, then with the RADIUS server, and finally with the TACACS+ server.

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.

```
insert system authentication-order radius after password
insert system authentication-order tacplus after radius
```

GUI Step-by-Step Procedure

To configure authentication order:

1. In the J-Web user interface, select **Configure>System Properties>User Management**.
2. Click **Edit**. The Edit User Management dialog box appears.
3. Select the **Authentication Method and Order** tab.
4. Under Available Methods, select the authentication method the device should use to authenticate users, and use the arrow button to move the item to the Selected Methods list. Available methods include:
 - RADIUS
 - TACACS+
 - Local Password

If you want to use multiple methods to authenticate users, repeat this step to add the additional methods to the Selected Methods list.

5. Under Selected Methods, use the Up Arrow and Down Arrow to specify the order in which the device should execute the authentication methods.
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* in the [Junos OS CLI User Guide](#).

To configure authentication order:

1. Add RADIUS authentication to the authentication order.

```
[edit]
user@host# insert system authentication-order radius after password
```
2. Add TACACS+ authentication to the authentication order.

```
[edit]
user@host# insert system authentication-order tacplus after radius
```

Results From configuration mode, confirm your configuration by entering the **show system authentication-order** 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 authentication-order
authentication-order [password, radius, tacplus];
```

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



NOTE: To completely set up RADIUS or TACACS+ authentication, you must configure at least one RADIUS or TACACS+ server and create user template accounts. Do one of the following tasks:

- Configure a RADIUS server. See [“Example: Configuring a RADIUS Server for System Authentication”](#) on page 21.
- Configure a TACACS+ server. See [“Example: Configuring a TACACS+ Server for System Authentication”](#) on page 23.
- Configure a user. See [“Example: Configuring New Users”](#) on page 31.
- Configure template accounts. See [“Example: Creating Template Accounts”](#) on page 40.

Verification

Confirm that the configuration is working properly.

- [Verifying the Authentication Order Configuration](#) on page 28

Verifying the Authentication Order Configuration

Purpose Verify that the authentication order has been configured.

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

- Related Documentation**
- [Understanding User Authentication Methods on page 19](#)
 - [Understanding User Accounts on page 20](#)
 - [Understanding Login Classes on page 28](#)
 - [Junos OS Security Configuration Guide](#)
 - [Junos OS System Basics Configuration Guide](#)
 - [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

Login Classes

This section contains the following topics:

- [Understanding Login Classes on page 28](#)
- [Example: Configuring New Users on page 31](#)

Understanding Login Classes

All users who log into the device must be in a login class. You can define any number of login classes. You then apply one login class to an individual user account. With login classes, you define the following:

- Access privileges users have when they are logged into the device.
- Commands and statements that users can and cannot specify.
- How long a login session can be idle before it times out and the user is logged off.

[Table 4 on page 28](#) contains a few predefined login classes. The predefined login classes cannot be modified.

Table 4: Predefined Login Classes

Login Class	Permission Bits Set
operator	clear, network, reset, trace, view
read-only	view
super-user and superuser	all
unauthorized	None

This section contains the following topics:

- [Permission Bits on page 29](#)
- [Denying or Allowing Individual Commands on page 31](#)

Permission Bits

Each top-level command-line interface (CLI) command and each configuration statement has an access privilege level associated with it. Users can execute only those commands and configure and view only those statements for which they have access privileges. The access privileges for each login class are defined by one or more permission bits (see [Table 5 on page 29](#)).

Two forms for the permissions control the individual parts of the configuration:

- "Plain" form—Provides read-only capability for that permission type. An example is **interface**.
- Form that ends in **-control**—Provides read and write capability for that permission type. An example is **interface-control**.

Table 5: Permission Bits for Login Classes

Permission Bit	Access
admin	Can view user account information in configuration mode and with the show configuration command.
admin-control	Can view user accounts and configure them (at the [edit system login] hierarchy level).
access	Can view the access configuration in configuration mode and with the show configuration operational mode command.
access-control	Can view and configure access information (at the [edit access] hierarchy level).
all	Has all permissions.
clear	Can clear (delete) information learned from the network that is stored in various network databases (using the clear commands).
configure	Can enter configuration mode (using the configure command) and commit configurations (using the commit command).
control	Can perform all control-level operations (all operations configured with the -control permission bits).
field	Reserved for field (debugging) support.
firewall	Can view the firewall filter configuration in configuration mode.
firewall-control	Can view and configure firewall filter information (at the [edit firewall] hierarchy level).
floppy	Can read from and write to the removable media.

Table 5: Permission Bits for Login Classes (*continued*)

Permission Bit	Access
interface	Can view the interface configuration in configuration mode and with the show configuration operational mode command.
interface-control	Can view chassis, class of service, groups, forwarding options, and interfaces configuration information. Can configure chassis, class of service, groups, forwarding options, and interfaces (at the [edit] hierarchy).
maintenance	Can perform system maintenance, including starting a local shell on the device and becoming the superuser in the shell (by issuing the su root command), and can halt and reboot the device (using the request system commands).
network	Can access the network by entering the ping , ssh , telnet , and traceroute commands.
reset	Can restart software processes using the restart command and can configure whether software processes are enabled or disabled (at the [edit system processes] hierarchy level).
rollback	Can use the rollback command to return to a previously committed configuration other than the most recently committed one.
routing	Can view general routing, routing protocol, and routing policy configuration information in configuration and operational modes.
routing-control	Can view general routing, routing protocol, and routing policy configuration information and configure general routing (at the [edit routing-options] hierarchy level), routing protocols (at the [edit protocols] hierarchy level), and routing policy (at the [edit policy-options] hierarchy level).
secret	Can view passwords and other authentication keys in the configuration.
secret-control	Can view passwords and other authentication keys in the configuration and can modify them in configuration mode.
security	Can view security configuration in configuration mode and with the show configuration operational mode command.
security-control	Can view and configure security information (at the [edit security] hierarchy level).
shell	Can start a local shell on the device by entering the start shell command.
snmp	Can view SNMP configuration information in configuration and operational modes.
snmp-control	Can view SNMP configuration information and configure SNMP (at the [edit snmp] hierarchy level).
system	Can view system-level information in configuration and operational modes.
system-control	Can view system-level configuration information and configure it (at the [edit system] hierarchy level).

Table 5: Permission Bits for Login Classes (*continued*)

Permission Bit	Access
trace	Can view trace file settings in configuration and operational modes.
trace-control	Can view trace file settings and configure trace file properties.
view	Can use various commands to display current system-wide, routing table, and protocol-specific values and statistics.

Denying or Allowing Individual Commands

By default, all top-level CLI commands have associated access privilege levels. Users can execute only those commands and view only those statements for which they have access privileges. For each login class, you can explicitly deny or allow the use of operational and configuration mode commands that are otherwise permitted or not allowed by a permission bit.

Related Documentation

- [Understanding User Authentication Methods on page 19](#)
- [Understanding User Accounts on page 20](#)
- [Understanding Template Accounts on page 39](#)
- [Example: Configuring New Users on page 31](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

Example: Configuring New Users

This example shows how to configure new users.

- [Requirements on page 31](#)
- [Overview on page 31](#)
- [Configuration on page 32](#)
- [Verification on page 34](#)

Requirements

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

Overview

You can add new users to the device's local database. For each account, you define a login name and password for the user and specify a login class for access privileges. The login password must meet the following criteria:

- The password must be at least six characters long.

- You can include most character classes in a password (alphabetic, numeric, and special characters), but not control characters.
- The password must contain at least one change of case or character class.

In this example, you create a login class named `operator-and-boot` and allow it to reboot the device. You can define any number of login classes. You then allow the `operator-and-boot` login class to use commands defined in the `clear`, `network`, `reset`, `trace`, and `view` permission bits.

Then you create user accounts. User accounts provide enable you to access the device. (You can access the device without accounts if you configured RADIUS or TACACS+ servers.) You set the username as `cmartin` and the login class as `superuser`. Finally, you define the encrypted password for the user.

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 login class operator-and-boot allow-commands "request system reboot"
set class system login operator-and-boot permissions [clear network reset trace view]
set system login user cmartin class superuser authentication encrypted-password
$1$14c5.$sBopasdFFdssdfFFdsdfs0
```

GUI Step-by-Step Procedure

To configure new users:

1. In the J-Web user interface, select **Configure>System Properties>User Management**.
2. Click **Edit**. The Edit User Management dialog box appears.
3. Select the **Users** tab.
4. Click **Add** to add a new user. The Add User dialog box appears.
5. In the User name box, type a unique name for the user.

Do not include spaces, colons, or commas in the username.
6. In the User ID box, type a unique ID for the user.
7. In the Full Name box, type the user's full name.

If the full name contains spaces, enclose it in quotation marks. Do not include colons or commas.
8. In the Password and Confirm Password boxes, enter a login password for the user and verify your entry.
9. From the Login Class list, select the user's access privilege:
 - **operator**
 - **read-only**
 - **unauthorized**

This list also includes any user-defined login classes.

10. Click **OK** in the Add User dialog box and Edit User Management dialog box.
11. Click **OK** to check your configuration and save it as a candidate configuration.
12. 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 in the [Junos OS CLI User Guide](#).

To configure new users:

1. Set the name of the login class and allow the use of the reboot command.

```
[edit system login]
user@host# set class operator-and-boot allow-commands "request system reboot"
```
2. Set the permission bits for the login class.

```
[edit system login]
user@host# set class operator-and-boot permissions [clear network reset trace view]
```
3. Set the username, login class, and encrypted password for the user.

```
[edit system login]
user@host# set user cmartin class superuser authentication encrypted-password $1$14c5.$sBopasdFFdssdfFFdsdfs0
```

Results From configuration mode, confirm your configuration by entering the **show system login** 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 login
  class operator-and-boot {
    permissions [ clear network reset trace view ];
    allow-commands "request system reboot";
  }
  user cmartin {
    class superuser;
    authentication {
      encrypted-password "$1$14c5.$sBopasdFFdssdfFFdsdfs0";
    }
  }
}
```

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



NOTE: To completely set up RADIUS or TACACS+ authentication, you must configure at least one RADIUS or TACACS+ server and specify a user template account. Do one of the following tasks:

- Configure a RADIUS server. See [“Example: Configuring a RADIUS Server for System Authentication” on page 21](#).
- Configure a TACACS+ server. See [“Example: Configuring a TACACS+ Server for System Authentication” on page 23](#).
- Configure a user. See [“Example: Configuring New Users” on page 31](#).
- Configure template accounts. See [“Example: Creating Template Accounts” on page 40](#).

Verification

Confirm that the configuration is working properly.

- [Verifying the New Users Configuration on page 34](#)

Verifying the New Users Configuration

Purpose Verify that the new users have been configured.

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

- Related Documentation**
- [Understanding User Authentication Methods on page 19](#)
 - [Understanding User Accounts on page 20](#)
 - [Understanding Template Accounts on page 39](#)
 - [Understanding Login Classes on page 28](#)
 - [Junos OS Security Configuration Guide](#)
 - [Junos OS System Basics Configuration Guide](#)
 - [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

User Authentication

- [Handling Authorization Failure on page 35](#)
- [Example: Configuring System Retry Options on page 36](#)

Example: Configuring System Retry Options

This example shows how to configure system retry options to protect the device from malicious users.

- [Requirements on page 36](#)
- [Overview on page 36](#)
- [Configuration on page 38](#)
- [Verification on page 39](#)

Requirements

Before you begin, you should understand [“Handling Authorization Failure” on page 35](#).

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

Overview

Malicious users sometimes try to log in to a secure device by guessing an authorized user account's password. Locking out a user account after a number of failed authentication attempts helps protect the device from malicious users.

Device lockout allows you to configure the number of failed attempts before the user account is locked out of the device and configure the amount of time before the user can attempt to log in to the device again. You can configure the amount of time in-between failed login attempts of a user account and can manually lock and unlock user accounts.

**NOTE:**

This example includes the following settings:

- **backoff-factor** — Sets the length of delay in seconds after each failed login attempt. When a user incorrectly logs in to the device, the user must wait the configured amount of time before attempting to log in to the device again. The length of delay increases by this value for each subsequent login attempt after the value specified in the **backoff-threshold** statement. The default value for this statement is five seconds, with a range of five to ten seconds.
- **backoff-threshold** — Sets the threshold for the number of failed login attempts on the device before the user experiences a delay when attempting to reenter a password. When a user incorrectly logs in to the device and hits the threshold of failed login attempts, the user experiences a delay that is set in the **backoff-factor** statement before attempting to log in to the device again. The default value for this statement is two, with a range of one through three.
- **lockout-period** — Sets the amount of time in minutes before the user can attempt to log in to the device after being locked out due to the number of failed login attempts specified in the **tries-before-disconnect** statement. When a user fails to correctly login after the number of allowed attempts specified by the **tries-before-disconnect** statement, the user must wait the configured amount of minutes before attempting to log in to the device again. The lockout-period must be greater than zero. The range at which you can configure the lockout-period is one through 43,200 minutes.
- **tries-before-disconnect** — Sets the maximum number of times the user is allowed to enter a password to attempt to log in to the device through SSH or Telnet. When the user reaches the maximum number of failed login attempts, the user is locked out of the device. The user must wait the configured amount of minutes in the **lockout-period** statement before attempting to log back in to the device. The **tries-before-disconnect** statement must be set when the **lockout-period** statement is set; otherwise, the **lockout-period** statement is meaningless. The default number of attempts is ten, with a range of one through ten attempts.

Once a user is locked out of the device, if you are the security administrator, you can manually remove the user from this state using the `clear system login lockout <username>` command. You can also use the `show system login lockout` command to view which users are currently locked out, when the lockout period began for each user, and when the lockout period ends for each user.

If the security administrator is locked out of the device, he can log in to the device from the console port, which ignores any user locks. This provides a way for the administrator to remove the user lock on their own user account.

In this example the user waits for the **backoff-threshold** multiplied by the **backoff-factor** interval, in seconds, to get the login prompt. In this example, the user must wait 5 seconds after the first failed login attempt and 10 seconds after the second failed login attempt to get the login prompt. The user gets disconnected after 15 seconds after the third failed attempt because the **tries-before-disconnect** option is configured as 3.

The user cannot attempt another login until 120 minutes has elapsed, unless a security administrator manually clears the lock sooner.

Configuration

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

```
[edit]
set system login retry-options backoff-factor 5
set system login retry-options backoff-threshold 1
set system login retry-options lockout-period 120
set system login retry-options tries-before-disconnect 3
```

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 system retry-options:

1. Configure the backoff factor.

```
[edit ]
user@host# set system login retry-options backoff-factor 5
```

2. Configure the backoff threshold.

```
[edit]
user@host# set system login retry-options backoff-threshold 1
```

3. Configure the amount of time the device gets locked after failed attempts.

```
[edit]
user@host# set system login retry-options lockout-period 5
```

4. Configure the number of unsuccessful attempts during which, the device can remain unlocked.

```
[edit]
user@host# set system login retry-options tries-before-disconnect 3
```

Results From configuration mode, confirm your configuration by entering the **show system login retry-options** 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 login retry-options
backoff-factor 5;
backoff-threshold 1;
lockout-period 5;
tries-before-disconnect 3;
```


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

Verification

Displaying the Locked User Logins

Purpose	Verify that the login lockout configuration is enabled
Action	Attempt 3 unsuccessful logins for a particular username. The device gets locked for the user and then login to the device with a different user name. From operational mode, enter the show system login lockout command.
Meaning	When you perform 3 unsuccessful login attempts with a particular username, the device is locked for that user for 5 minutes as configured in the example. You can verify that the user is, locked by logging in to the device with a different username and entering the show system login lockout command.
Related Documentation	<ul style="list-style-type: none"> • Handling Authorization Failure on page 35 • Junos OS CLI Reference

Template Accounts

This section contains the following topics:

- [Understanding Template Accounts on page 39](#)
- [Example: Creating Template Accounts on page 40](#)

Understanding Template Accounts

You use local user template accounts when you need different types of templates. Each template can define a different set of permissions appropriate for the group of users who use that template. These templates are defined locally on the device and referenced by the TACACS+ and RADIUS authentication servers.

When you configure local user templates and a user logs in, Junos OS issues a request to the authentication server to authenticate the user's login name. If a user is authenticated, the server returns the local username to the device, which then determines whether a local username is specified for that login name (**local-username** for TACACS+, **Juniper-Local-User** for RADIUS). If so, the device selects the appropriate local user template locally configured on the device. If a local user template does not exist for the authenticated user, the device defaults to the **remote** template.

Related Documentation	<ul style="list-style-type: none"> • Understanding User Authentication Methods on page 19 • Understanding User Accounts on page 20 • Understanding Login Classes on page 28 • Example: Creating Template Accounts on page 40
------------------------------	--

- [Junos OS Security Configuration Guide](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

Example: Creating Template Accounts

This example shows how to create template accounts.

- [Requirements on page 40](#)
- [Overview on page 40](#)
- [Configuration on page 40](#)
- [Verification on page 42](#)

Requirements

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

Overview

You can create template accounts that are shared by a set of users when you are using RADIUS or TACACS+ authentication. When a user is authenticated by a template account, the CLI username is the login name, and the privileges, file ownership, and effective user ID are inherited from the template account.

By default, Junos OS uses the **remote** template account when:

- The authenticated user does not exist locally on the device.
- The authenticated user's record in the RADIUS or TACACS+ server specifies local user, or the specified local user does not exist locally on the device.

In this example, you create a remote template account and set the username to remote and the login class for the user as operator. You create a remote template that is applied to users authenticated by RADIUS or TACACS+ that do not belong to a local template account.

You then create a local template account and set the username as admin and the login class as superuser. You use local template accounts when you need different types of templates. Each template can define a different set of permissions appropriate for the group of users who use that template.

Configuration

- [Creating a Remote Template Account on page 40](#)
- [Creating a Local Template Account on page 41](#)

Creating a Remote Template Account

CLI Quick Configuration To quickly configure this section of the example, copy the following command, paste it into a text file, remove any line breaks, change any details necessary to match your

network configuration, and then copy and paste the command into the CLI at the **[edit]** hierarchy level.

```
set system login user remote class operator
```

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 in the *Junos OS CLI User Guide*.

To create a remote template account:

1. Set the username and the login class for the user.

```
[edit system login]
user@host# set user remote class operator
```

Results From configuration mode, confirm your configuration by entering the **show system login** 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 login
user remote {
  class operator;
}
```

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

Creating a Local Template Account

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

```
set system login user admin class superuser
```

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 in the *Junos OS CLI User Guide*.

To create a local template account:

1. Set the username and the login class for the user.

```
[edit system login]
user@host# set user admin class superuser
```

Results From configuration mode, confirm your configuration by entering the **show system login** 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 login
```

```
user admin {  
  class super-user;  
}
```

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



NOTE: To completely set up RADIUS or TACACS+ authentication, you must configure at least one RADIUS or TACACS+ server and specify a system authentication order. Do one of the following tasks:

- Configure a RADIUS server. See [“Example: Configuring a RADIUS Server for System Authentication” on page 21](#).
- Configure a TACACS+ server. See [“Example: Configuring a TACACS+ Server for System Authentication” on page 23](#).
- Configure system authentication order. See [“Example: Configuring Authentication Order” on page 26](#).

Verification

Confirm that the configuration is working properly.

- [Verifying the Template Accounts Creation on page 42](#)

Verifying the Template Accounts Creation

Purpose Verify that the template accounts have been created.

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

Related Documentation

- [Understanding User Authentication Methods on page 19](#)
- [Understanding User Accounts on page 20](#)
- [Understanding Login Classes on page 28](#)
- [Understanding Template Accounts on page 39](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

CHAPTER 4

Telnet and SSH Device Control

- [Securing the Console Port Configuration Overview on page 43](#)
- [Accessing Remote Devices with the CLI on page 44](#)
- [Reverse Telnet on page 48](#)

Securing the Console Port Configuration Overview

You can use the console port on the device to connect to the device through an RJ-45 serial cable. From the console port, you can use the CLI to configure the device. By default, the console port is enabled. To secure the console port, you can configure the device to take the following actions:

- Log out of the console session when you unplug the serial cable connected to the console port.
- Disable root login connections to the console.
- Disable the console port. We recommend disabling the console port to prevent unauthorized access to the device, especially when the device is used as customer premises equipment (CPE).

To secure the console port:

1. Do one of the following:

- Disable the console port. Enter

```
[edit system ports console]  
user@host# set disable
```

- Disable root login connections to the console. Enter

```
[edit system ports console]  
user@host# set insecure
```

- Log out the console session when the serial cable connected to the console port is unplugged. Enter

```
[edit system ports console]  
user@host# set log-out-on-disconnect
```

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

Related Documentation

- [The telnet Command on page 44](#)
- [The ssh Command on page 45](#)
- [Configuring Password Retry Limits for Telnet and SSH Access on page 46](#)
- [Reverse Telnet Overview on page 48](#)
- [Configuring Reverse Telnet and Reverse SSH on page 49](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

Accessing Remote Devices with the CLI

This section contains the following topics:

- [The telnet Command on page 44](#)
- [The ssh Command on page 45](#)
- [Configuring Password Retry Limits for Telnet and SSH Access on page 46](#)

The telnet Command

You can use the CLI **telnet** command to open a Telnet session to a remote device:

```
user@host> telnet host <8bit> <bypass-routing> <inet> <interface interface-name>
<no-resolve> <port port> <routing-instance routing-instance-name> <source address>
```



NOTE: On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, the maximum number of concurrent Telnet sessions is as follows:

SRX100	SRX210	SRX220	SRX240	SRX650
3	3	3	5	5

To exit the Telnet session and return to the Telnet command prompt, press Ctrl-].

To exit the Telnet session and return to the CLI command prompt, enter **quit**.

[Table 6 on page 44](#) describes the **telnet** command options.

Table 6: CLI telnet Command Options

Option	Description
8bit	Use an 8-bit data path.
bypass-routing	Bypass the routing tables and open a Telnet session only to hosts on directly attached interfaces. If the host is not on a directly attached interface, an error message is returned.
host	Open a Telnet session to the specified hostname or IP address.

Table 6: CLI telnet Command Options (*continued*)

Option	Description
inet	Force the Telnet session to an IPv4 destination.
interface <i>source-interface</i>	Open a Telnet session to a host on the specified interface. If you do not include this option, all interfaces are used.
no-resolve	Suppress the display of symbolic names.
port <i>port</i>	Specify the port number or service name on the host.
routing-instance <i>routing-instance-name</i>	Use the specified routing instance for the Telnet session.
source <i>address</i>	Use the specified source address for the Telnet session.

Related Documentation

- [The ssh Command on page 45](#)
- [Configuring Password Retry Limits for Telnet and SSH Access on page 46](#)
- [Reverse Telnet Overview on page 48](#)
- [Configuring Reverse Telnet and Reverse SSH on page 49](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS System Basics and Services Command Reference](#)

The ssh Command

You can use the CLI **ssh** command to use the secure shell (SSH) program to open a connection to a remote device:

```
user@host> ssh host <bypass-routing> <inet> <interface interface-name>
<routing-instance routing-instance-name> <source address> <v1> <v2>
```



NOTE: On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, the maximum number of concurrent SSH sessions is as follows:

SRX100	SRX210	SRX220	SRX240	SRX650
3	3	3	5	5

Table 7 on page 46 describes the **ssh** command options.

Table 7: CLI ssh Command Options

Option	Description
bypass-routing	Bypass the routing tables and open an SSH connection only to hosts on directly attached interfaces. If the host is not on a directly attached interface, an error message is returned.
host	Open an SSH connection to the specified hostname or IP address.
inet	Force the SSH connection to an IPv4 destination.
interface <i>source-interface</i>	Open an SSH connection to a host on the specified interface. If you do not include this option, all interfaces are used.
routing-instance <i>routing-instance-name</i>	Use the specified routing instance for the SSH connection.
source address	Use the specified source address for the SSH connection.
v1	Force SSH to use version 1 for the connection.
v2	Force SSH to use version 2 for the connection.

Related Documentation

- [The telnet Command on page 44](#)
- [Configuring Password Retry Limits for Telnet and SSH Access on page 46](#)
- [Reverse Telnet Overview on page 48](#)
- [Configuring Reverse Telnet and Reverse SSH on page 49](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

Configuring Password Retry Limits for Telnet and SSH Access

To prevent brute force and dictionary attacks, the device performs the following actions for Telnet or SSH sessions by default:

- Disconnects a session after a maximum of 10 consecutive password retries.
- After the second password retry, introduces a delay in multiples of 5 seconds between subsequent password retries.

For example, the device introduces a delay of 5 seconds between the third and fourth password retry, a delay of 10 seconds between the fourth and fifth password retry, and so on.

- Enforces a minimum session time of 20 seconds during which a session cannot be disconnected. Configuring the minimum session time prevents malicious users from disconnecting sessions before the password retry delay goes into effect, and attempting brute force and dictionary attacks with multiple logins.

You can configure the password retry limits for Telnet and SSH access. In this example, you configure the device to take the following actions for Telnet and SSH sessions:

- Allow a maximum of four consecutive password retries before disconnecting a session.
- Introduce a delay in multiples of 5 seconds between password retries that occur after the second password retry.
- Enforce a minimum session time of 40 seconds during which a session cannot be disconnected.

To configure password retry limits for Telnet and SSH access:

1. Set the maximum number of consecutive password retries before a Telnet or SSH or telnet session is disconnected. The default number is **10**, but you can set a number from 1 through **10**.

```
[edit system login retry-options]
user@host# set tries-before-disconnect 4
```

2. Set the threshold number of password retries after which a delay is introduced between two consecutive password retries. The default number is **2**, but you can specify a value from 1 through **3**.

```
[edit system login retry-options]
user@host# set backoff-threshold 2
```

3. Set the delay (in seconds) between consecutive password retries after the threshold number of password retries. The default delay is in multiples of **5** seconds, but you can specify a value from **5** through **10** seconds.

```
[edit system login retry-options]
user@host# set backoff-factor 5
```

4. Set the minimum length of time (in seconds) during which a Telnet or SSH session cannot be disconnected. The default is **20** seconds, but you can specify an interval from **20** through **60** seconds.

```
[edit system login retry-options]
user@host# set minimum-time 40
```

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

Related Documentation

- [The telnet Command on page 44](#)
- [The ssh Command on page 45](#)
- [Reverse Telnet Overview on page 48](#)
- [Configuring Reverse Telnet and Reverse SSH on page 49](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

Reverse Telnet

This section contains the following topics:

- [Reverse Telnet Overview on page 48](#)
- [Configuring Reverse Telnet and Reverse SSH on page 49](#)

Reverse Telnet Overview

Reverse telnet allows you to configure a device to listen on a specific port for Telnet and SSH services. When you connect to that port, the device provides an interface to the auxiliary port on the device. You use a rollover cable to connect the auxiliary port from the device on which reverse telnet is enabled to the console port of the device you want to manage.



NOTE: Reverse telnet is supported only on J Series devices.

To use reverse telnet, you must have the following devices:

- A device with an auxiliary port running the appropriate version of Junos OS.
- A device with a console port for remote management if network connectivity fails and you want to use console access.

This section contains the following topics:

- [Reverse Telnet Options on page 48](#)
- [Reverse Telnet Restrictions on page 48](#)

Reverse Telnet Options

When you enable reverse telnet, you can control the port that is used, and you can optionally turn on reverse ssh to encrypt the reverse telnet communication between the device and the client. By default, reverse telnet uses port 2900 and reverse ssh uses port 2901.



NOTE: Enabling reverse ssh requires an additional command. By default, when you enable reverse telnet, the connection is not encrypted.

Reverse Telnet Restrictions

Keep the following restrictions in mind when you attempt to use reverse telnet or reverse ssh:

- Multiple connections to the serial port are not allowed. If there is an existing connection to the serial port, any other connections are denied.

- If the auxiliary port is enabled (through the **system services port auxiliary** configuration statement), you cannot use reverse telnet or reverse ssh because another service is already using the auxiliary port.

**Related
Documentation**

- [The telnet Command on page 44](#)
- [The ssh Command on page 45](#)
- [Configuring Password Retry Limits for Telnet and SSH Access on page 46](#)
- [Configuring Reverse Telnet and Reverse SSH on page 49](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

Configuring Reverse Telnet and Reverse SSH

To configure reverse telnet and reverse ssh:

1. Enable reverse telnet.

```
[edit]
user@host# set system services reverse telnet
```

2. Specify the port to be used for reverse telnet. If you do not specify a port, 2900 is the default port that is used.

```
[edit]
user@host# set system services reverse telnet port 5000
```

3. Enable reverse ssh to encrypt the connection between the device and the client.

```
[edit]
user@host# set system services reverse ssh
```

4. Specify the port for reverse ssh. If you do not specify a port, 2901 is the default port that is used.

```
[edit]
user@host# set system services reverse ssh port 6000
```

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

**Related
Documentation**

- [The telnet Command on page 44](#)
- [The ssh Command on page 45](#)
- [Configuring Password Retry Limits for Telnet and SSH Access on page 46](#)
- [Reverse Telnet Overview on page 48](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

CHAPTER 5

USB Modems for Remote Management Setup

- [USB Modem Interface Overview on page 51](#)
- [USB Modem Configuration Overview on page 54](#)
- [Example: Configuring a USB Modem Interface on page 56](#)
- [Example: Configuring a Dialer Interface on page 59](#)
- [Example: Configuring a Dialer Interface for USB Modem Dial-In on page 62](#)
- [Remote Device Connection on page 64](#)
- [USB Modem Administration on page 66](#)

USB Modem Interface Overview

Juniper Networks devices support the use of USB modems for remote management. You can use Telnet or SSH to connect to the device from a remote location through two modems over a telephone network. The USB modem is connected to the USB port on the device, and a second modem is connected to a remote management device such as a PC or laptop computer.

You can configure your device to fail over to a USB modem connection when the primary Internet connection experiences interruption.

A USB modem connects to a device through modem interfaces that you configure. The device applies its own modem AT commands to initialize the attached modem. Modem setup requires that you connect and configure the USB modem at the device and the modem at the user end of the network.

You use either the J-Web configuration editor or CLI configuration editor to configure the USB modem and its supporting dialer interfaces.



NOTE: Low-latency traffic such as VoIP traffic is not supported over USB modem connections.



NOTE: We recommend using a US Robotics USB 56k V.92 Modem, model number USR Model 5637.

USB Modem Interfaces

You configure two types of interfaces for USB modem connectivity:

- A physical interface which uses the naming convention **umdn0**. The device creates this interface when a USB modem is connected to the USB port.
- A logical interface called the dialer interface. You use the dialer interface, **dln**, to configure dialing properties for USB modem connections. The dialer interface can be configured using Point-to-Point Protocol (PPP) encapsulation. You can also configure the dialer interface to support authentication protocols—PPP Challenge Handshake (CHAP) or Password Authentication Protocol (PAP). You can configure multiple dialer interfaces for different functions on the device. After configuring the dialer interface, you must configure a backup method such as a dialer backup, a dialer filter, or a dialer watch.

The USB modem provides a dial-in remote management interface, and supports dialer interface features by sharing the same dial pool as a dialer interface. The dial pool allows the logical dialer interface and the physical interface to be bound together dynamically on a per-call basis. You can configure the USB modem to operate either as a dial-in console for management or as a dial-in WAN backup interface. Dialer pool priority has a range from 1 to 255, with 1 designating the lowest priority interfaces and 255 designating the highest priority interfaces.

Dialer Interface Rules

The following rules apply when you configure dialer interfaces for USB modem connections:

- The dialer interface must be configured to use PPP encapsulation. You cannot configure Cisco High-Level Data Link Control (HDLC) or Multilink PPP (MLPPP) encapsulation on dialer interfaces.
- The dialer interface cannot be configured as a constituent link in a multilink bundle.
- The dialer interface can perform backup, dialer filter, and dialer watch functions, but these operations are mutually exclusive. You can configure a single dialer interface to operate in only one of the following ways:
 - As a backup interface—for one primary interface
 - As a dialer filter
 - As a dialer watch interface

The backup dialer interfaces are activated only when the primary interface fails. USB modem backup connectivity is supported on all interfaces except `lsq-0/0/0`.

The dial-on-demand routing backup method allows a USB modem connection to be activated only when network traffic configured as an “interesting packet” arrives on the network. Once the network traffic is sent, an inactivity timer is triggered and the connection is closed. You define an interesting packet using the dialer filter feature of the device. To configure dial-on-demand routing backup using a dialer filter, you first configure the dialer filter and then apply the filter to the dialer interface.

Dialer watch is a backup method that integrates backup dialing with routing capabilities and provides reliable connectivity without relying on a dialer filter to trigger outgoing USB modem connections. With dialer watch, the device monitors the existence of a specified route. If the route disappears, the dialer interface initiates the USB modem connection as a backup connection.

How the Device Initializes USB Modems

When you connect the USB modem to the USB port on the device, the device applies the modem AT commands configured in the **init-command-string** command to the initialization commands on the modem.

If you do not configure modem AT commands for the **init-command-string** command, the device applies the following default sequence of initialization commands to the modem: **AT S7=45 S0=0 V1 X4 &C1 E0 Q0 &Q8 %C0**. [Table 8 on page 53](#) describes the commands. For more information about these commands, see the documentation for your modem.

Table 8: Default Modem Initialization Commands

Modem Command	Description
AT	Attention. Informs the modem that a command follows.
S7=45	Instructs the modem to wait 45 seconds for a telecommunications service provider (carrier) signal before terminating the call.
S0=0	Disables the auto answer feature, whereby the modem automatically answers calls.
V1	Displays result codes as words.
&C1	Disables reset of the modem when it loses the carrier signal.
E0	Disables the display on the local terminal of commands issued to the modem from the local terminal.
Q0	Enables the display of result codes.
&Q8	Enables Microcom Networking Protocol (MNP) error control mode.
%C0	Disables data compression.

When the device applies the modem AT commands in the **init-command-string** command or the default sequence of initialization commands to the modem, it compares them to

the initialization commands already configured on the modem and makes the following changes:

- If the commands are the same, the device overrides existing modem values that do not match. For example, if the initialization commands on the modem include **S0=0** and the device's **init-command-string** command includes **S0=2**, the device applies **S0=2**.
- If the initialization commands on the modem do not include a command in the device's **init-command-string** command, the device adds it. For example, if the **init-command-string** command includes the command **L2**, but the modem commands do not include it, the device adds **L2** to the initialization commands configured on the modem.

**Related
Documentation**

- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [USB Modem Configuration Overview on page 54](#)
- [Example: Configuring a USB Modem Interface on page 56](#)
- [Example: Configuring a Dialer Interface for USB Modem Dial-In on page 62](#)

USB Modem Configuration Overview

Before you begin:

1. Install device hardware. For more information, see the Getting Started Guide for your device.
2. Establish basic connectivity. For more information, see the Getting Started Guide for your device.
3. Order a US Robotics USB 56k V.92 Modem, model number USR Model 5637 from US Robotics (<http://www.usr.com/>).
4. Order a public switched telephone network (PSTN) line from your telecommunications service provider. Contact your service provider for more information.
5. Connect the USB modem to the device's USB port.



NOTE: J Series devices have two USB ports. However, you can connect only one USB modem to the USB ports on these devices. If you connect USB modems to both ports, the device detects only the first modem connected.



NOTE: When you connect the USB modem to the USB port on the device, the USB modem is initialized with the modem initialization string configured for the USB modem interface on the device.

- a. Plug the modem into the USB port.

- b. Connect the modem to your telephone network.

Suppose you have a branch office router and a head office router each with a USB modem interface and a dialer interface. This example shows you how to establish a backup connection between the branch office and head office routers. See [Table 9 on page 55](#) for a summarized description of the procedure.

Table 9: Configuring Branch Office and Head Office Routers for USB Modem Backup Connectivity

Router Location	Configuration Requirement	Procedure
Branch Office	Configure the logical dialer interface on the branch office router for USB modem dial backup.	To configure the logical dialer interface, see “Example: Configuring a USB Modem Interface” on page 56 .
	Configure the dialer interface dl0 on the branch office router using one of the following backup methods: <ul style="list-style-type: none"> Configure the dialer interface dl0 as the backup interface on the branch office router's primary T1 interface t1-1/0/0. Configure a dialer filter on the branch office router's dialer interface. Configure a dialer watch on the branch office router's dialer interface. 	Configure the dialer interface using one of the following backup methods: <ul style="list-style-type: none"> To configure dl0 as a backup for t1-1/0/0 see Example: Configuring Dialer Interfaces and Backup Methods for USB Modem Dial Backup. To configure a dialer filter on dl0, see Example: Configuring Dialer Interfaces and Backup Methods for USB Modem Dial Backup. To configure a dialer watch on dl0, see Example: Configuring Dialer Interfaces and Backup Methods for USB Modem Dial Backup.
Head Office	Configure dial-in on the dialer interface dl0 on the head office router.	To configure dial-in on the head office router, see “Example: Configuring a Dialer Interface for USB Modem Dial-In” on page 62 .

If the dialer interface is configured to accept only calls from a specific caller ID, the device matches the incoming call's caller ID against the caller IDs configured on its dialer interfaces. If an exact match is not found and the incoming call's caller ID has more digits than the configured caller IDs, the device performs a right-to-left match of the incoming call's caller ID with the configured caller IDs and accepts the incoming call if a match is found. For example, if the incoming call's caller ID is 4085321091 and the caller ID configured on a dialer interface is 5321091, the incoming call is accepted. Each dialer interface accepts calls from only callers whose caller IDs are configured on it.

See [Table 10 on page 56](#) for a list of available incoming map options.

Table 10: Incoming Map Options

Option	Description
accept-all	<p>Dialer interface accepts all incoming calls.</p> <p>You can configure the accept-all option for only one of the dialer interfaces associated with a USB modem physical interface. The dialer interface with the accept-all option configured is used only if the incoming call's caller ID does not match the caller IDs configured on other dialer interfaces.</p>
caller	<p>Dialer interface accepts calls from a specific caller ID. You can configure a maximum of 15 caller IDs per dialer interface.</p> <p>The same caller ID must not be configured on different dialer interfaces. However, you can configure caller IDs with more or fewer digits on different dialer interfaces. For example, you can configure the caller IDs 14085551515, 4085551515, and 5551515 on different dialer interfaces.</p>

You configure dialer interfaces to support PAP. PAP allows a simple method for a peer to establish its identity using a two-way handshake during initial link establishment. After the link is established, an ID and password pair are repeatedly sent by the peer to the authenticator until authentication is acknowledged or the connection is terminated.

Related Documentation

- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [USB Modem Interface Overview on page 51](#)
- [Example: Configuring a USB Modem Interface on page 56](#)

Example: Configuring a USB Modem Interface

This example shows how to configure a USB modem interface for dial backup.

- [Requirements on page 56](#)
- [Overview on page 56](#)
- [Configuration on page 57](#)
- [Verification on page 58](#)

Requirements

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

Overview

In this example, you create an interface called as umd0 for USB modem connectivity and set the dialer pool priority to 25. You also configure a modem initialization string to autoanswer after a specified number of rings. The default modem initialization string is **AT S7=45 S0=0 V1 X4 &C1 E0 Q0 &Q8 %C0**. The modem command **S0=0** disables the modem from autoanswering the calls. Finally, you set the modem to act as a dial-in WAN backup interface.

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 interfaces umd0 dialer-options pool usb-modem-dialer-pool priority 25
set modem-options init-command-string "ATSO=2 \n" dialin routable
```

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 in the *Junos OS CLI User Guide*](#).

To configure a USB modem interface for dial backup:

1. Create an interface.

```
[edit]
user@host# edit interfaces umd0
```

2. Set the dialer options and priority.

```
[edit interfaces umd0]
user@host# set dialer-options pool usb-modem-dialer-pool priority 25
```

3. Specify the modem options.

```
[edit interfaces umd0]
user@host# set modem-options init-command-string "ATSO=2 \n"
```

4. Set the modem to act as a dial-in WAN backup interface.

```
[edit interfaces umd0]
user@host# set modem-options dialin routable
```

Results From configuration mode, confirm your configuration by entering the **show interface umd0** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show interface umd0
modem-options {
  init-command-string "ATSO=2 \n";
  dialin routable;
}
dialer-options {
  pool usb-modem-dialer-pool priority 25;
}
```

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

Verification

To confirm that the configuration is working properly, perform this task:

- [Verifying the Configuration on page 58](#)

Verifying the Configuration

Purpose Verify a USB modem interface for dial backup.

Action From configuration mode, enter the **show interfaces umd0 extensive** command. The output shows a summary of interface information and displays the modem status.

```
Physical interface:  umd0, Enabled, Physical link is Up
Interface index:    64, SNMP ifIndex: 33, Generation: 1
  Type: Async-Serial, Link-level type: PPP-Subordinate, MTU: 1504,
Clocking: Unspecified, Speed: MODEM
Device flags      : Present Running
Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
Link flags       : None
Hold-times       : Up 0 ms, Down 0 ms
Last flapped     : Never
Statistics last cleared: Never
Traffic statistics:
  Input bytes  :                21672
  Output bytes :                22558
  Input packets:                1782
  Output packets:               1832
Input errors:
  Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed discards:
0,
Resource errors: 0
Output errors:
  Carrier transitions: 63, Errors: 0, Drops: 0, MTU errors: 0, Resource errors:
0
MODEM status:
  Modem type           : LT V.92 1.0 MT5634ZBA-USB-V92 Data/Fax Modem

(Dual Config) Version 2.27m
  Initialization command string : ATSO=2
  Initialization status         : Ok
  Call status                   : Connected to 4085551515
  Call duration                 : 13429 seconds
  Call direction                : Dialin
  Baud rate                     : 33600 bps
  Most recent error code        : NO CARRIER

Logical interface umd0.0 (Index 2) (SNMP ifIndex 34) (Generation 1)
  Flags: Point-To-Point SNMP-Traps Encapsulation: PPP-Subordinate
```

**Related
Documentation**

- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [USB Modem Configuration Overview on page 54](#)
- [USB Modem Interface Overview on page 51](#)
- [Example: Configuring a Dialer Interface for USB Modem Dial-In on page 62](#)

Example: Configuring a Dialer Interface

This example shows how to configure a logical dialer interface for the device.

- [Requirements on page 59](#)
- [Overview on page 59](#)
- [Configuration on page 60](#)
- [Verification on page 61](#)

Requirements

Before you begin:

- Install device hardware and establish basic connectivity. See the Getting Started Guide for your device.
- Order a US Robotics USB 56k V.92 Modem, model number USR Model 5637, from US Robotics (<http://www.usr.com/>).
- Order a dial-up modem for the PC or laptop computer at the remote location from where you want to connect to the device.
- Order a PSTN line from your telecommunications service provider. Contact your service provider.

Overview

In this example, you configure a logical dialer interface called `dl0` to establish USB connectivity. You can configure multiple dialer interfaces for different functions on the device. You add a description to differentiate among different dialer interfaces. For example, this modem is called `USB-modem-remote-management`. Configure PPP encapsulation and set the logical unit as 0. You then specify the name of the dialer pool as `usb-modem-dialer-pool` and set the source and destination IP addresses as `172.20.10.2`, and `172.20.10.1`, respectively.



NOTE: You cannot configure Cisco High-Level Data Link Control (HDLC) or Multilink PPP (MLPPP) encapsulation on dialer interfaces used in USB modem connections.



NOTE: If you configure multiple dialer interfaces, ensure that the same IP subnet address is not configured on different dialer interfaces. Configuring the same IP subnet address on multiple dialer interfaces can result in inconsistency in the route and packet loss. The device might route packets through another dialer interface with the IP subnet address instead of through the dialer interface to which the USB modem call is mapped.

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 interfaces dl0 description USB-modem-remote-management encapsulation ppp
set interfaces dl0 unit 0 dialer-options pool usb-modem-dialer-pool
set interfaces dl0 unit 0 family inet address 172.20.10.2 destination 172.20.10.1
```

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 in the [Junos OS CLI User Guide](#).

To configure a logical dialer interface for the device:

1. Create an interface.

```
[edit]
user@host# set interfaces dl0
```

2. Add a description and configure PPP encapsulation.

```
[edit interfaces dl0]
user@host# set description USB-modem-remote-management
user@host# set encapsulation ppp
```

3. Create the logical unit.



NOTE: The logical unit number must be 0.

```
[edit interfaces dl0]
user@host# set unit 0
```

4. Configure the name of the dialer pool to use for USB modem connectivity.

```
[edit interfaces dl0 unit 0]
user@host# set dialer-options pool usb-modem-dialer-pool
```

5. Configure source and destination IP addresses for the dialer interface.

```
[edit interfaces dl0 unit 0]
user@host# set family inet address 172.20.10.2 destination 172.20.10.1
```

Results From configuration mode, confirm your configuration by entering the **show interfaces dl0** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show interfaces dl0
description USB-modem-remote-management;
encapsulation ppp;
unit 0 {
```

```

family inet {
    address 172.20.10.2/32 {
        destination 172.20.10.1;
    }
}
dialer-options {
    pool usb-modem-dialer-pool;
}
}

```

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

Verification

Confirm that the configuration is working properly.

- [Verifying a Dialer Interface on page 61](#)

Verifying a Dialer Interface

Purpose Verify that the dialer interface has been configured.

Action From configuration mode, enter the **show interfaces d10 extensive** command. The output shows a summary of dialer interface information.

```

Physical interface: d10, Enabled, Physical link is Up
  Interface index: 128, SNMP ifIndex: 24, Generation: 129
  Type: 27, Link-level type: PPP, MTU: 1504, Clocking: Unspecified, Speed:
Unspecified
  Device flags      : Present Running
  Interface flags: SNMP-Traps
  Link type        : Full-Duplex
  Link flags       : Keepalives
  Physical info    : Unspecified
  Hold-times       : Up 0 ms, Down 0 ms
  Current address: Unspecified, Hardware address: Unspecified
  Alternate link address: Unspecified
  Last flapped     : Never
  Statistics last cleared: Never
  Traffic statistics:
    Input bytes   :           13859           0 bps
    Output bytes  :              0           0 bps
    Input packets :             317           0 pps
    Output packets:              0           0 pps
  Input errors:
    Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed discards:
0,
  Resource errors: 0
    Output errors:
      Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0, Resource errors:
0

Logical interface d10.0 (Index 70) (SNMP ifIndex 75) (Generation 146)
  Description: USB-modem-remote-management
  Flags: Point-To-Point SNMP-Traps 0x4000 LinkAddress 23-0 Encapsulation: PPP
  Dialer:
    State: Active, Dial pool: usb-modem-dialer-pool
    Dial strings: 220

```

```
Subordinate interfaces: umd0 (Index 64)
Activation delay: 0, Deactivation delay: 0
Initial route check delay: 120
Redial delay: 3
Callback wait period: 5
Load threshold: 0, Load interval: 60
Bandwidth: 115200
Traffic statistics:
  Input bytes :          24839
  Output bytes :         17792
  Input packets:          489
  Output packets:         340
Local statistics:
  Input bytes :          10980
  Output bytes :         17792
  Input packets:          172
  Output packets:         340
Transit statistics:
  Input bytes :          13859          0 bps
  Output bytes :           0          0 bps
  Input packets:          317          0 pps
  Output packets:           0          0 pps
LCP state: Opened
NCP state: inet: Opened, inet6: Not-configured, iso: Not-configured,
mpls: Not-configured
CHAP state: Success
  Protocol inet, MTU: 1500, Generation: 136, Route table: 0
  Flags: None
  Addresses, Flags: Is-Preferred Is-Primary
  Destination: 172.20.10.1, Local: 172.20.10.2, Broadcast: Unspecified,
Generation: 134
```

**Related
Documentation**

- [USB Modem Interface Overview on page 51](#)
- [USB Modem Configuration Overview on page 54](#)
- [Example: Configuring a USB Modem Interface on page 56](#)
- [Example: Configuring a Dialer Interface for USB Modem Dial-In on page 62](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS Interfaces Command Reference](#)

Example: Configuring a Dialer Interface for USB Modem Dial-In

This example shows how to configure a dialer interface for USB modem dial-in.

- [Requirements on page 63](#)
- [Overview on page 63](#)
- [Configuration on page 63](#)
- [Verification on page 64](#)

Requirements

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

Overview

To enable connections to the USB modem from a remote location, you must configure the dialer interfaces set up for USB modem use to accept incoming calls. You can configure a dialer interface to accept all incoming calls or accept only calls from one or more caller IDs.

If the dialer interface is configured to accept only calls from a specific caller ID, the system matches the incoming call's caller ID against the caller IDs configured on its dialer interfaces. If an exact match is not found and the incoming call's caller ID has more digits than the configured caller IDs, the system performs a right-to-left match of the incoming call's caller ID with the configured caller IDs and accepts the incoming call if a match is found. For example, if the incoming call's caller ID is 4085550115 and the caller ID configured on a dialer interface is 5550115, the incoming call is accepted. Each dialer interface accepts calls from only callers whose caller IDs are configured on it.

You can configure the following incoming map options for the dialer interface:

- **accept-all**—Dialer interface accepts all incoming calls.

You can configure the **accept-all** option for only one of the dialer interfaces associated with a USB modem physical interface. The device uses the dialer interface with the **accept-all** option configured only if the incoming call's caller ID does not match the caller IDs configured on other dialer interfaces.

- **caller**—Dialer interface accepts calls from a specific caller ID—for example, **4085550115**. You can configure a maximum of 15 caller IDs per dialer interface.

The same caller ID must not be configured on different dialer interfaces. However, you can configure caller IDs with more or fewer digits on different dialer interfaces. For example, you can configure the caller IDs 14085550115, 4085550115, and 5550115 on different dialer interfaces.

In this example, you configure the incoming map option as caller 4085550115 for dialer interface d10.

Configuration

CLI Quick Configuration

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

```
set interfaces d10 unit 0 dialer-options incoming-map caller 4085550115
```

Step-by-Step Procedure

To configure a dialer interface for USB modem dial-in:

1. Select a dialer interface.

[edit]

```
user@host# edit interfaces dlo
```

2. Configure the incoming map options.

```
[edit]
```

```
user@host# edit unit 0 dialer-options incoming-map caller 4085551515
```

3. If you are done configuring the device, commit the configuration.

```
[edit]
```

```
user@host# commit
```

Verification

To verify the configuration is working properly, enter the **show interface dlo** command.

Related Documentation

- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [USB Modem Configuration Overview on page 54](#)
- [Example: Configuring a USB Modem Interface on page 56](#)

Remote Device Connection



NOTE: These instructions describe connecting to the device from a remote PC or laptop computer running Microsoft Windows XP. If your remote PC or laptop computer does not run Microsoft Windows XP, see the documentation for your operating system and enter equivalent commands.

This section contains the following topics:

- [Configuring a Dial-Up Modem Connection Remotely on page 64](#)
- [Connecting to the Device Remotely on page 65](#)

Configuring a Dial-Up Modem Connection Remotely

To remotely connect to the USB modem connected to the USB port on the device, you must configure a dial-up modem connection on the PC or laptop computer at your remote location. Configure the dial-up modem connection properties to disable IP header compression.

To configure a dial-up modem connection remotely:

1. At your remote location, connect a modem to a management device such as a PC or laptop computer.
2. Connect the modem to your telephone network.
3. On the PC or laptop computer, select **Start>Settings>Control Panel>Network Connections**. The Network Connections page appears.
4. Click **Create a new connection**. The New Connection Wizard appears.

5. Click **Next**. The New Connection Wizard: Network Connection Type page appears.
6. Select **Connect to the network at my workplace**, and then click **Next**.
The New Connection Wizard: Network Connection page appears.
7. Select **Dial-up connection**, and then click **Next**. The New Connection Wizard: Connection Name page appears.
8. In the Company Name box, type the dial-up connection name, for example **USB-modem-connect**. Then, click **Next**. The New Connection Wizard: Phone Number to Dial page appears.
9. In the Phone number box, type the telephone number of the PSTN line connected to the USB modem at the device end.
10. Click **Next** twice, and then click **Finish**. The Connect USB-modem-connect page appears.
11. If CHAP is configured on the dialer interface used for the USB modem interface at the device end, type the username and password configured in the CHAP configuration in the User name and Password boxes.
12. Click **Properties**. The USB-modem-connect Properties page appears.
13. In the Networking tab, select **Internet Protocol (TCP/IP)**, and then click **Properties**. The Internet Protocol (TCP/IP) Properties page appears.
14. Click **Advanced**. The Advanced TCP/IP Settings page appears.
15. Clear the **Use IP header compression** check box.

Related Documentation

- [USB Modem Interface Overview on page 51](#)
- [USB Modem Configuration Overview on page 54](#)
- [Connecting to the Device Remotely on page 65](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS Interfaces Configuration Guide for Security Devices](#)

Connecting to the Device Remotely

To remotely connect to the device through a USB modem connected to the USB port on the device:

1. On the PC or laptop computer at your remote location, select **Start>Settings>Control Panel>Network Connections**. The Network Connections page appears.
2. Double-click the **USB-modem-connect** dial-up connection. The Connect USB-modem-connect page appears.
3. Click **Dial** to connect to the Juniper Networks device.

When the connection is complete, you can use Telnet or SSH to connect to the device.

Related Documentation

- [USB Modem Interface Overview on page 51](#)
- [USB Modem Configuration Overview on page 54](#)
- [Configuring a Dial-Up Modem Connection Remotely on page 64](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS Interfaces Configuration Guide for Security Devices](#)

USB Modem Administration

This section contains the following topics:

- [Modifying USB Modem Initialization Commands on page 66](#)
- [Resetting USB Modems on page 67](#)

Modifying USB Modem Initialization Commands



.....
NOTE: These instructions use Hayes-compatible modem commands to configure the modem. If your modem is not Hayes-compatible, see the documentation for your modem and enter equivalent modem commands.
.....

You can use the CLI configuration editor to override the value of an initialization command configured on the USB modem or configure additional commands for initializing USB modems.



.....
NOTE: If you modify modem initialization commands when a call is in progress, the new initialization sequence is applied on the modem only when the call ends.
.....

You can configure the following modem AT commands to initialize the USB modem:

- The command **S0=2** configures the modem to automatically answer calls on the second ring.
- The command **L2** configures medium speaker volume on the modem.

You can insert spaces between commands.

When you configure modem commands in the CLI configuration editor, you must follow these conventions:

- Use the newline character `\n` to indicate the end of a command sequence.

- Enclose the command string in double quotation marks.

You can override the value of the **S0=0** command in the initialization sequence configured on the modem and add the **L2** command.

To modify the initialization commands on a USB modem:

1. Configure the modem AT commands to initialize the USB modem.

```
[edit interfaces umd0]
user@host# set modem-options init-command-string "AT S0=2 L2 \n"
```

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

Related Documentation

- [USB Modem Interface Overview on page 51](#)
- [USB Modem Configuration Overview on page 54](#)
- [Resetting USB Modems on page 67](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS Interfaces Configuration Guide for Security Devices](#)
- [Junos OS Interfaces Fundamentals Configuration Guide](#)

Resetting USB Modems

If the USB modem does not respond, you can reset the modem.



CAUTION: If you reset the modem when a call is in progress, the call is terminated.

To reset the USB modem, in operational mode, enter the following command:

```
user@host> request interface modem reset umd0
```

Related Documentation

- [USB Modem Interface Overview on page 51](#)
- [USB Modem Configuration Overview on page 54](#)
- [Modifying USB Modem Initialization Commands on page 66](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS Interfaces Configuration Guide for Security Devices](#)
- [Junos OS Interfaces Command Reference](#)

CHAPTER 6

DHCP for IP Address Device Configuration

- [DHCP Server, Client, and Relay Agent Overview on page 69](#)
- [DHCP Configuration Overview on page 70](#)
- [DHCP Operations on page 71](#)
- [DHCP Settings and Restrictions Overview on page 88](#)

DHCP Server, Client, and Relay Agent Overview

A Dynamic Host Configuration Protocol (DHCP) server can automatically allocate IP addresses and also deliver configuration settings to client hosts on a subnet. DHCP lets network administrators centrally manage a pool of IP addresses among hosts and automate the assignment of IP addresses in a network. An IP address can be leased to a host for a limited period of time, allowing the DHCP server to share a limited number of IP addresses among a group of hosts that do not need permanent IP addresses.

The Juniper Networks device acts as the DHCP server, providing IP addresses and settings to hosts, such as PCs, that are connected to device interfaces. The DHCP server is compatible with the DHCP servers of other vendors on the network.

The device can also operate as a DHCP client and DHCP relay agent.

DHCP is based on BOOTP, a bootstrap protocol that allows a client to discover its own IP address, the IP address of a server host, and the name of a bootstrap file. DHCP servers can handle requests from BOOTP clients, but provide additional capabilities beyond BOOTP, such as the automatic allocation of reusable IP addresses and additional configuration options.



NOTE: Although a Juniper Networks device can act as a DHCP server, a DHCP client, or DHCP relay agent at the same time, you cannot configure more than one DHCP role on a single interface.

DHCP provides two primary functions:

- Allocate temporary or permanent IP addresses to clients.
- Store, manage, and provide client configuration parameters.

Related Documentation

- [DHCP Configuration Overview on page 70](#)
- [Understanding DHCP Server Operation on page 71](#)
- [Understanding DHCP Client Operation on page 78](#)
- [Understanding DHCP Relay Agent Operation on page 83](#)
- [DHCP Settings and Restrictions Overview on page 88](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

DHCP Configuration Overview

A typical DHCP server configuration provides the following configuration settings for a particular subnet on a device interface:

- An IP address pool, with one address excluded from the pool.
- Default and maximum lease times.
- Domain search suffixes. These suffixes specify the domain search list used by a client when resolving hostnames with DNS.
- A DNS name server.
- Device solicitation address option (option 32). The IP address excluded from the IP address pool is reserved for this option.

In addition, the DHCP server might assign a static address to at least one client on the subnet. [Table 11 on page 70](#) provides the settings and values for the sample DHCP server configuration.

Table 11: Sample DHCP Configuration Settings

Setting	Sample Value
DHCP Subnet Configuration	
Address pool subnet address	192.168.2.0/24
High address in the pool range	192.168.2.254
Low address in the pool range	192.168.2.2
Address pool default lease time, in seconds	1,209,600 (14 days)
Address pool maximum lease time, in seconds	2,419,200 (28 days)
Domain search suffixes	mycompany.net mylab.net
Address to exclude from the pool	192.168.2.33

Table 11: Sample DHCP Configuration Settings (*continued*)

Setting	Sample Value
DNS server address	192.168.10.2
Identifier code for router solicitation address option	32
Type choice for router solicitation address option	Ip address
IP address for router solicitation address option	192.168.2.33
DHCP MAC Address Configuration	
Static binding MAC address	01:03:05:07:09:0B
Fixed address	192.168.2.50

Related Documentation

- [DHCP Server, Client, and Relay Agent Overview on page 69](#)
- [Understanding DHCP Server Operation on page 71](#)
- [Understanding DHCP Client Operation on page 78](#)
- [Understanding DHCP Relay Agent Operation on page 83](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [RFC 3397, Dynamic Host Configuration Protocol \(DHCP\) Domain Search Option](#),

DHCP Operations

This section contains the following topics:

- [Understanding DHCP Server Operation on page 71](#)
- [Example: Configuring the Device as a DHCP Server on page 72](#)
- [Understanding DHCP Client Operation on page 78](#)
- [Example: Configuring the Device as a DHCP Client on page 79](#)
- [Understanding DHCP Relay Agent Operation on page 83](#)
- [Example: Configuring the Device as a BOOTP or DHCP Relay Agent on page 83](#)

Understanding DHCP Server Operation

As a DHCP server, a Juniper Networks device can provide temporary IP addresses from an IP address pool to all clients on a specified subnet, a process known as *dynamic binding*. Juniper Networks devices can also perform static binding, assigning permanent IP addresses to specific clients based on their media access control (MAC) addresses. Static bindings take precedence over dynamic bindings.

This section contains the following topics:

- [DHCP Options on page 72](#)
- [Compatibility with Autoinstallation on page 72](#)

[DHCP Options](#)

In addition to its primary DHCP server functions, you can also configure the device to send configuration settings like the following to clients through DHCP:

- IP address of the DHCP server (Juniper Networks device)
- List of Domain Name System (DNS) and NetBIOS servers
- List of gateway routers
- IP address of the boot server and the filename of the boot file to use
- DHCP options defined in RFC 2132, *DHCP Options and BOOTP Vendor Extensions*

[Compatibility with Autoinstallation](#)

The functions of a Juniper Networks device acting as a DHCP server are compatible with the autoinstallation feature. The DHCP server automatically checks any autoinstallation settings for conflicts and gives the autoinstallation settings priority over corresponding DHCP settings. For example, an IP address set by autoinstallation takes precedence over an IP address set by the DHCP server.

Related Documentation

- [DHCP Server, Client, and Relay Agent Overview on page 69](#)
- [Example: Configuring the Device as a DHCP Server on page 72](#)
- [Understanding DHCP Client Operation on page 78](#)
- [Understanding DHCP Relay Agent Operation on page 83](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS Policy Framework Configuration Guide](#)

Example: Configuring the Device as a DHCP Server

This example shows how to configure the device as a DHCP server.

- [Requirements on page 73](#)
- [Overview on page 73](#)
- [Configuration on page 73](#)
- [Verification on page 76](#)

Requirements

Before you begin:

- Determine the IP address pools and the lease durations to use for each subnet. See [Example: Viewing DHCP Address Pools](#).
- Obtain the MAC addresses of the clients that require permanent IP addresses. Determine the IP addresses to use for these clients. See the [Junos OS Security Configuration Guide](#).
- List the IP addresses that are available for the servers and devices on your network; for example, DNS, NetBIOS servers, boot servers, and gateway devices. See the [Junos OS Security Configuration Guide](#).
- Determine the DHCP options required by the subnets and clients in your network. See [Creating User-Defined DHCP Options Not Included in the Default Junos Implementation of the DHCP Server](#).

Overview

In this example, you configure the device as a DHCP server. You specify the IP address pool as 192.168.2.0/24 and from a low range of 192.168.2.2 to a high range of 192.168.2.254. You set the default-lease-time to 1,209,600 and the maximum-lease-time to 2,419,200. You then set the domain search suffixes as mycompany.net and mylab.net. These suffixes specify the domain search list used by a client when resolving hostnames with DNS.

Then you specify the DNS server IP address as 192.168.10.2. You set the IP address for the device solicitation address option (option 32) as 192.168.2.33. The IP address excluded from the IP address pool is reserved for this option. Finally, you assign a fixed IP address as 192.168.2.50 with the MAC address of the client, 01:03:05:07:09:0B.

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 services dhcp pool 192.168.2.0/24 address-range low 192.168.2.2
high 192.168.2.254
set system services dhcp pool 192.168.2.0/24 default-lease-time 1209600
maximum-lease-time 2419200
set system services dhcp pool 192.168.2.0/24 domain-search mycompany.net
set system services dhcp pool 192.168.2.0/24 domain-search mylab.net
set system services dhcp pool 192.168.2.0/24 name-server 192.168.10.2
set system services dhcp pool 192.168.2.0/24 option 32 ip-address 192.168.2.33
set system services dhcp static-binding 01:03:05:07:09:0B fixed-address 192.168.2.50
```

GUI Step-by-Step Procedure

To configure the device as a DHCP server:

1. In the J-Web interface, select **Configure>Services>DHCP>Boot DHCP Relay**.
2. Next to System, click **Configure**.

3. Next to Services, make sure the check box is selected, and click **Configure**.
4. Next to Dhcp, click **Configure**.
5. Define the IP address pool. Next to Pool, click **Add new entry**.
6. In the Subnet address box, type **192.168.2.0/24**.
7. Next to Address range, select the check box.
8. In the High box, type **192.168.2.254**.
9. In the Low box, type **192.168.2.2**.
10. Click **OK**.
11. Define the default and maximum lease times, in seconds. From the Default lease time list, select **Enter Specific Value**.
12. In the Length box, type **1209600**.
13. From the Maximum lease time list, select **Enter Specific Value**.
14. Next to Maximum lease time, type **2419200**.
15. Define the domain search suffixes to be used by the clients. Next to Domain search, click **Add new entry**.
16. In the Suffix box, type **mycompany.net**.
17. Click **OK**.
18. Next to Domain search, click **Add new entry**.
19. In the Suffix box, type **mylab.net**.
20. Click **OK**.
21. Define a DNS server. Next to Name server, click **Add new entry**.
22. In the Address box, type **192.168.10.2**.
23. Click **OK**.
24. Define DHCP option 32, the device solicitation address option. Next to Option, click **Add new entry**.
25. In the Option identifier code box, type **32**.
26. From the Option type choice list, select **Ip address**.
27. In the Ip address box, type **192.168.2.33**.
28. Click **OK** twice.
29. Assign a static IP address to a MAC address. Next to Static binding, click **Add new entry**.
30. In the Mac address box, type **01:03:05:07:09:0B**.
31. Next to Fixed address, click **Add new entry**.
32. In the Address box, type **192.168.2.50**.

33. Click **OK** until you return to the Configuration page.
34. Click **OK** to check your configuration and save it as a candidate configuration.
35. 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* in the [Junos OS CLI User Guide](#).

To configure the device as a DHCP server:

1. Configure the DHCP server.

```
[edit]
user@host# edit system services dhcp
```
2. Specify the IP address pool range.

```
[edit system services dhcp]
user@host# set pool 192.168.2.0/24 address-range low 192.168.2.2 high 192.168.2.254
```
3. Define the default and maximum lease times, in seconds.

```
[edit system services dhcp]
user@host# set pool 192.168.2.0/24 default-lease-time 1209600
maximum-lease-time 2419200
```
4. Define the domain search suffixes to be used by the clients.

```
[edit system services dhcp]
user@host# set pool 192.168.2.0/24 domain-search mycompany.net
user@host# set pool 192.168.2.0/24 domain-search mylab.net
```
5. Specify the DNS server IP address.

```
[edit system services dhcp]
user@host# set pool 192.168.2.0/24 name-server 192.168.10.2
```
6. Set the device solicitation IP address.

```
[edit system services dhcp]
user@host# set pool 192.168.2.0/24 option 32 ip-address 192.168.2.33
```
7. Assign a fixed IP address with the MAC address of the client.

```
[edit system services dhcp]
user@host# set static-binding 01:03:05:07:09:0B fixed-address 192.168.2.50
```

Results From configuration mode, confirm your configuration by entering the **show system services dhcp** 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 services dhcp
pool 192.168.2.0/24 {
  address-range low 192.168.2.2 high 192.168.2.254;
  maximum-lease-time 2419200;
  default-lease-time 1209600;
  name-server {
```

```
    192.168.10.2;
  }
  domain-search {
    mycompany.net;
    mylab.net;
  }
  option 32 ip-address 192.168.2.33;
  }
  static-binding 01:03:05:07:09:0B {
    fixed-address {
      192.168.2.50;
    }
  }
}
```

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

Verification

Confirm that the configuration is working properly.

- [Verifying Global DHCP Information on page 76](#)
- [Verifying the DHCP Binding Database on page 76](#)
- [Verifying DHCP Server Operation on page 77](#)

Verifying Global DHCP Information

Purpose Verify that the global DHCP Information has been configured for the device.

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

```
Global settings:
  BOOTP lease length      infinite
  DHCP lease times:
    Default lease time    1 day
    Minimum lease time    1 minute
    Maximum lease time    infinite

DHCP options:
  Name: domain-name, Value: englab.juniper.net
  Name: name-server, Value: [ 192.168.5.68, 172.17.28.101, 172.17.28.100 ]
```

Verifying the DHCP Binding Database

Purpose Verify that the DHCP binding database reflects the DHCP server configuration.

Action From operational mode, enter these commands:

- **show system services dhcp binding** command to display all active bindings in the database.
- **show system services dhcp binding address detail** command (where *address* is the IP address of the client) to display more information about a client.
- **show system services dhcp conflict** command to show any potential conflicts with the bindings.

These commands produce following sample output:

```

user@host> show system services dhcp binding

IP Address   Hardware Address   Type           Lease expires at
30.1.1.20    00:12:1e:a9:7b:81  dynamic       2007-05-11 11:14:43 PDT

user@host> show system services dhcp binding 3.3.3.2 detail

IP address           3.3.3.2
Hardware address      00:a0:12:00:13:02
Pool                  3.3.3.0/24
Interface fe-0/0/0, relayed by 3.3.3.200

Lease information:
Type                 DHCP
Obtained at          2004-05-02 13:01:42 PDT
Expires at           2004-05-03 13:01:42 PDT
State                 active

DHCP options:
Name: name-server, Value: { 6.6.6.6, 6.6.6.7 }
Name: domain-name, Value: mydomain.tld
Code: 32, Type: ip-address, Value: 3.3.3.33

user@host> show system services dhcp conflict

Detection time Detection method Address
2004-08-03 19:04:00 PDT ARP 3.3.3.5
2004-08-04 04:23:12 PDT Ping 4.4.4.8
2004-08-05 21:06:44 PDT Client 3.3.3.10

```

Verifying DHCP Server Operation

Purpose Verify that the DHCP server operation has been configured.

Action From operational mode, enter these commands:

- **ping** command to verify that a client responds to ping packets containing the destination IP address assigned by the device.
- **ipconfig /all** command to display the IP configuration on the client. For example, on a PC running Microsoft Windows, enter **ipconfig /all** at the command prompt to display the PC's IP configuration.

```

user@host> ping 192.168.2.2

PING 192.168.2.2 (192.168.2.2): 56 data bytes
64 bytes from 192.168.2.2: icmp_seq=0 ttl=255 time=8.856 ms
64 bytes from 192.168.2.2: icmp_seq=1 ttl=255 time=11.543 ms
64 bytes from 192.168.2.2: icmp_seq=2 ttl=255 time=10.315 ms
...

C:\Documents and Settings\user> ipconfig /all

Windows 2000 IP Configuration

Host Name . . . . . : my-pc
Primary DNS Suffix . . . . . : mycompany.net
Node Type . . . . . : Hybrid

```

```
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : mycompany.net mylab.net
```

Ethernet adapter Local Area Connection 2:

```
Connection-specific DNS Suffix . : mycompany.net mylab.net
Description . . . . . : 10/100 LAN Fast Ethernet Card
Physical Address. . . . . : 02-04-06-08-0A-0C
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 192.168.2.2
Subnet Mask . . . . . : 255.255.254.0
Default Gateway . . . . . : 192.168.10.3
DHCP Server . . . . . : 192.168.2.1
DNS Servers . . . . . : 192.168.10.2
Primary WINS Server . . . . . : 192.168.10.4
Secondary WINS Server . . . . . : 192.168.10.5
Lease Obtained. . . . . : Monday, January 24, 2005 8:48:59 AM
Lease Expires . . . . . : Monday, February 7, 2005 8:48:59 AM
```

**Related
Documentation**

- [DHCP Server, Client, and Relay Agent Overview on page 69](#)
- [Understanding DHCP Server Operation on page 71](#)
- [Understanding DHCP Relay Agent Operation on page 83](#)
- [DHCP Settings and Restrictions Overview on page 88](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS System Basics and Services Command Reference](#)

Understanding DHCP Client Operation

A Juniper Networks device can act as a DHCP client, receiving its TCP/IP settings and the IP address for any physical interface in any security zone from an external DHCP server. The device can also act as a DHCP server, providing TCP/IP settings and IP addresses to clients in any zone. When the device operates as a DHCP client and a DHCP server simultaneously, it can transfer the TCP/IP settings learned through its DHCP client module to its default DHCP server module. For the device to operate as a DHCP client, you configure a logical interface on the device to obtain an IP address from the DHCP server in the network. You set the vendor class ID, lease time, DHCP server address, retransmission attempts, and retry interval. You can renew DHCP client releases.

**Related
Documentation**

- [DHCP Server, Client, and Relay Agent Overview on page 69](#)
- [Example: Configuring the Device as a DHCP Client on page 79](#)
- [Understanding DHCP Relay Agent Operation on page 83](#)
- [DHCP Settings and Restrictions Overview on page 88](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

- [Junos OS Policy Framework Configuration Guide](#)

Example: Configuring the Device as a DHCP Client

This example shows how to configure the device as a DHCP client.

- [Requirements on page 79](#)
- [Overview on page 79](#)
- [Configuration on page 79](#)
- [Verification on page 81](#)

Requirements

Before you begin:

- Determine the IP address pools and the lease durations to use for each subnet. See [Example: Viewing DHCP Address Pools](#).
- Obtain the MAC addresses of the clients that require permanent IP addresses. Determine the IP addresses to use for these clients. See the [Junos OS Security Configuration Guide](#).
- List the IP addresses that are available for the servers and devices on your network; for example, DNS, NetBIOS servers, boot servers, and gateway devices. See the [Junos OS Security Configuration Guide](#).
- Determine the DHCP options required by the subnets and clients in your network. See [Creating User-Defined DHCP Options Not Included in the Default Junos Implementation of the DHCP Server](#).

Overview

In this example, you configure the device as a DHCP client. You specify the interface as ge-0/0/1, set the logical unit as 0, and create a DHCP inet family. You then specify the DHCP client identifier as 00:0a:12:00:12:12 in hexadecimal. You use hexadecimal if the client identifier is a MAC address. You set the DHCP lease time as 86,400 seconds. The range is from 60 through 2,147,483,647 seconds.

Then you set the number of retransmission attempts to 6. The range is from 0 through 6, and the default is 4. You set the retransmission interval to 5 seconds. The range is from 4 through 64, and the default is 4 seconds. Finally, you set the IPv4 address of the preferred DHCP server to 10.1.1.1 and the vendor class ID to ether.

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 interfaces ge-0/0/1 unit 0 family inet dhcp
set interfaces ge-0/0/1 unit 0 family inet dhcp client-identifier 00:0a:12:00:12:12
set interfaces ge-0/0/1 unit 0 family inet dhcp lease-time 86400
```

```
set interfaces ge-0/0/1 unit 0 family inet dhcp retransmission-attempt 6
set interfaces ge-0/0/1 unit 0 family inet dhcp retransmission-interval 5
set interfaces ge-0/0/1 unit 0 family inet dhcp server-address 10.1.1.1
set interfaces ge-0/0/1 unit 0 family inet dhcp vendor-id ether
```

**GUI Step-by-Step
Procedure**

To configure the device as a DHCP client:

1. In the J-Web user interface, select **Configure>Services>DHCP>Boot DHCP Relay**.
2. Under Interfaces, click **ge-0/0/1**.
3. Under Unit, next to the unit number, click **Edit**.
4. Under Family, select the **Inet** check box and click **Edit**.
5. Next to Dhcp, click **Yes** and click **Configure**.
6. Configure the DHCP client identifier as either an ASCII or hexadecimal value. Next to Client identifier, click **Configure**.
7. From the Client identifier choice list, select **hexadecimal**.
8. In the Hexadecimal box, type the client identifier—**00:0a:12:00:12:12**.
9. Click **OK**.
10. Set the DHCP lease time in seconds. From the Lease time list, select **Enter Specific Value**.
11. In the Length box, type **86400**.
12. Set the retransmission number of attempts. In the Retransmission attempt box, type **6**.
13. Set the retransmission interval in seconds. In the Retransmission interval box, type **5**.
14. Set the IPv4 address of the preferred DHCP server. In the Server address box, type **10.1.1.1**.
15. Set the vendor class ID. In the Vendor id box, type **ether**.
16. Click **OK**.
17. Click **OK** to check your configuration and save it as a candidate configuration.
18. 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* in the [Junos OS CLI User Guide](#).

To configure the device as a DHCP client:

1. Specify the DHCP client interface.

```
[edit]
user@host# edit interfaces ge-0/0/1 unit 0 family inet dhcp
```
2. Configure the DHCP client identifier as a hexadecimal value.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp]
```

```
user@host# set client-identifier 00:0a:12:00:12:12
```

3. Set the DHCP lease time.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp]
user@host# set lease-time 86400
```

4. Set the number of attempts allowed to retransmit a DHCP packet.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp]
user@host# set retransmission-attempt 6
```

5. Set the interval (in seconds) allowed between retransmission attempts. The range is 4 through 64. The default is 4 seconds.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp]
user@host# set retransmission-interval 5
```

6. Set the IPv4 address of the preferred DHCP server.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp]
user@host# set server-address 10.1.1.1
```

7. Set the vendor class ID for the DHCP client.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp]
user@host# set vendor-id ether
```

Results From configuration mode, confirm your configuration by entering the **show interfaces ge-0/0/1 unit 0 family inet** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show interfaces ge-0/0/1 unit 0 family inet
dhcp {
  client-identifier hexadecimal 00:0a:12:00:12:12;
  lease-time 86400;
  retransmission-attempt 6;
  retransmission-interval 5;
  server-address 10.1.1.1;
  update-server;
  vendor-id ether;
}
```

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

Verification

Confirm that the configuration is working properly.

- [Verifying the DHCP Client on page 81](#)

Verifying the DHCP Client

Purpose Verify that the DHCP client information has been configured.

Action From operational mode, enter these commands:

- **show system services dhcp client** command to display DHCP client information.

- **show system services dhcp client *interface-name*** command to display more information about a specific interface.
- **show system services dhcp client statistics** command to show client statistics.

These commands produce the following sample output:

```
user@host> show system services dhcp client

Logical Interface Name  ge-0/0/1.0
Hardware address       00:0a:12:00:12:12
Client Status          bound
Vendor Identifier       ether
Server Address          10.1.1.1
Address obtained        10.1.1.89
update server           enables
Lease Obtained at      2006-08-24 18:13:04 PST
Lease Expires at       2006-08-25 18:13:04 PST

DHCP Options:
Name: name-server, Value: [ 10.209.194.131, 2.2.2.2, 3.3.3.3 ]
Name: server-identifier, Value: 10.1.1.1
Name: router, Value: [ 10.1.1.80 ]
Name: domain-name, Value: netscreen-50
```

```
user@host> show system services dhcp client ge-0/0/1.0

Logical Interface Name  ge-0/0/1.0
Hardware address       00:12:1e:a9:7b:81
Client Status          bound
Address obtained        30.1.1.20
update server           enables
Lease Obtained at      2007-05-10 18:16:04 PST
Lease Expires at       2007-05-11 18:16:04 PST

DHCP Options:
Name: name-server, Value: [ 30.1.1.2 ]
Code: 1, Type: ip-address, Value: 255.255.255.0
Name: name-server, Value: [ 77.77.77.77, 55.55.55.55 ]
Name: domain-name, Value: englab.juniper.net
```

```
user@host> show system services dhcp client statistics

Packets dropped:
Total          0
Messages Received:
DHCP OFFER      0
DHCP ACK        8
DHCP NAK        0

Messages Sent:
DHCP DECLINE    0
DHCP DISCOVER   0
DHCP REQUEST    1
DHCP INFORM     0
DHCP RELEASE    0
DHCP RENEW      7
DHCP REBIND     0
```

- Related Documentation**
- [DHCP Server, Client, and Relay Agent Overview on page 69](#)
 - [Understanding DHCP Server Operation on page 71](#)
 - [Understanding DHCP Client Operation on page 78](#)
 - [DHCP Settings and Restrictions Overview on page 88](#)
 - [Junos OS Security Configuration Guide](#)
 - [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
 - [Junos OS System Basics and Services Command Reference](#)

Understanding DHCP Relay Agent Operation

A Juniper Networks device operating as a DHCP relay agent forwards incoming requests from BOOTP and DHCP clients to a specified BOOTP or DHCP server. Client requests can pass through virtual private network (VPN) tunnels.

You cannot configure a single device interface to operate as both a DHCP client and a DHCP relay.



NOTE: The DHCP requests received on an interface are associated to a DHCP pool that is in the same subnet as the primary IP address/subnet on an interface. If an interface is associated with multiple IP addresses/subnets, the device uses the lowest numerically assigned IP address as the primary IP address/subnet for the interface. To change the IP address/subnet that is listed as the primary address on an interface, use the `set interfaces < interface name > unit 0 family inet xxx.xxx.xxx.xxx/yy primary` command and commit the change.

- Related Documentation**
- [DHCP Server, Client, and Relay Agent Overview on page 69](#)
 - [Understanding DHCP Server Operation on page 71](#)
 - [Example: Configuring the Device as a BOOTP or DHCP Relay Agent on page 83](#)
 - [DHCP Settings and Restrictions Overview on page 88](#)
 - [Junos OS Security Configuration Guide](#)
 - [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
 - [Junos OS Policy Framework Configuration Guide](#)

Example: Configuring the Device as a BOOTP or DHCP Relay Agent

This example shows how to configure the device as a BOOTP or DHCP relay agent.

- [Requirements on page 84](#)
- [Overview on page 84](#)

- [Configuration on page 84](#)
- [Verification on page 87](#)

Requirements

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

Overview

In this example, you enable the DHCP relay agent to relay BOOTP or DHCP messages to a BOOTP server. You enable VPN encryption to allow client requests to pass through the VPN tunnel. You specify the IP time-to-live value to be set in responses to the client as 20. The range is from 1 through 255. You then set the maximum number of hops allowed per packet to 10. The range is from 4 through 16.

Then you specify the minimum number of seconds before requests are forwarded as 300. The range is from 0 through 30,000 seconds. You set the description of the server (the value is a string), and you specify a valid server name or address to the server to forward (the value is an IPv4 address). You define the routing instance, whose value is a nonreserved text string of 128 or fewer characters. You then specify the incoming BOOTP or DHCP request forwarding interface as ge-0/0/0. You enable the broadcast option if the Layer 2 interface is unknown.

You then specify the IP time-to-live value to be set in responses to the client as 30. The range is from 1 through 255. You set the description of the server as text and the DHCP option as 82. You set the maximum number of hops allowed per packet to 20 and specify the minimum number of seconds as 400 before requests are forwarded. You enable the no listen option. Finally, you enable VPN encryption to allow client requests to pass through the VPN tunnel.

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 forwarding-options helpers bootp relay agent-option
set forwarding-options helpers bootp vpn
set forwarding-options helpers bootp client-response-ttl 20
set forwarding-options helpers bootp maximum-hop-count 10
set forwarding-options helpers bootp minimum-wait-time 300
set forwarding-options helpers bootp description text
set forwarding-options helpers bootp server 2.2.2.2
set forwarding-options helpers bootp server 2.2.2.2 routing instance rt-i-1
set forwarding-options helpers bootp interface ge-0/0/0
set forwarding-options helpers bootp interface ge-0/0/0 broadcast
set forwarding-options helpers bootp interface ge-0/0/0 client-response-ttl 30
set forwarding-options helpers bootp interface ge-0/0/0 description text
set forwarding-options helpers bootp interface ge-0/0/0 dhcp-option82
set forwarding-options helpers bootp interface ge-0/0/0 maximum-hop-count 20
set forwarding-options helpers bootp interface ge-0/0/0 minimum-wait-time 400
```

```
set forwarding-options helpers bootp interface ge-0/0/0 no-listen
set forwarding-options helpers bootp interface ge-0/0/0 vpn
```

GUI Step-by-Step Procedure

To configure the device as a BOOTP/DHCP relay agent:

1. In the J-Web user interface, select **Configure>Services>DHCP>Boot DHCP Relay**.
2. Select the DHCP relay agent check box to enable the BOOTP/DHCP relay agent.
3. Select the VPN encryption check box.
4. In the Client response TTL box, type **20**.
5. In the Maximum hop count box, type **10**.
6. In the Minimum wait time box, type **300**.
7. In the Description box, type the description of the server.
8. Add a new server. Next to Server, click **Add new Entry**.
9. Next to the Name box, type **2.2.2.2**.
10. Define the routing instance. Next to Routing instance, click **Add new entry**.
11. In the Name box, type **rt-i-1** and click **OK**. A routing instance is optional.
12. Add a new interface. Next to Interface, click **Add new entry**.
13. In the Interface name box, type the interface name. For example, type **ge-0/0/0**.
14. In the Client response TTL box, type **30**.
15. In the Description box, type the description of the server.
16. Select the **Dhcp option 82** check box.
17. In the Maximum hop count box, type **20**.
18. In the Minimum wait time box, type **400**.
19. Select the **No listen** check box.
20. Select the **VPN encryption** check box.
21. Click **OK** until you return to the Configuration page.
22. Click **OK** to check your configuration and save it as a candidate configuration.
23. 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 in the *Junos OS CLI User Guide*](#).

To configure the device as a BOOTP or DHCP relay agent:

1. Set the DHCP relay agent.

```
[edit]
user@host# edit forwarding-options helpers bootp
user@host# set relay agent-option
```

2. Enable VPN encryption to allow client requests to pass through VPN tunnel.

```
[edit forwarding-options helpers bootp]  
user@host# set vpn
```

3. Set the IP time-to-live value. .

```
[edit forwarding-options helpers bootp]  
user@host# set client-response-ttl 20
```

4. Set the maximum number of hops allowed per packet.

```
[edit forwarding-options helpers bootp]  
user@host# set maximum-hop-count 10
```

5. Set the minimum wait time in seconds.

```
[edit forwarding-options helpers bootp]  
user@host# set minimum-wait-time 300
```

6. Specify the description of the server.

```
[edit forwarding-options helpers bootp]  
user@host# set description text
```

7. Add a new server.

```
[edit forwarding-options helpers bootp]  
user@host# set server 2.2.2.2
```

8. Define the routing instance.

```
[edit forwarding-options helpers bootp]  
user@host# set server 2.2.2.2 routing-instance rt-i-1
```

9. Define the incoming BootP request forwarding interface.

```
[edit forwarding-options helpers bootp]  
user@host# set interface ge-0/0/0
```

10. Enable broadcast option.

```
[edit forwarding-options helpers bootp interface ge-0/0/0]  
user@host# set broadcast
```

11. Define the IP time-to-live value.

```
[edit forwarding-options helpers bootp interface ge-0/0/0]  
user@host# set client-response-ttl 30
```

12. Specify the description of the server.

```
[edit forwarding-options helpers bootp interface ge-0/0/0]  
user@host# set description text
```

13. Set the DHCP option 82.

```
[edit forwarding-options helpers bootp interface ge-0/0/0]  
user@host# set dhcp-option82
```

14. Specify the maximum number of hops allowed per packet.

```
[edit forwarding-options helpers bootp interface ge-0/0/0]  
user@host# set forwarding-options helpers bootp interface ge-0/0/0  
maximum-hop-count 20
```


15. Set the minimum wait time.

```
[edit forwarding-options helpers bootp interface ge-0/0/0]
user@host# set minimum-wait-time 400
```
16. Set the no listen option.

```
[edit forwarding-options helpers bootp interface ge-0/0/0]
user@host# set no-listen
```
17. Enable VPN encryption to allow client requests to pass through the VPN tunnel.

```
[edit forwarding-options helpers bootp interface ge-0/0/0]
user@host# set vpn
```

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

```
[edit]
user@host# show forwarding-options
helpers {
  bootp {
    relay-agent-option;
    description text;
    server 2.2.2.2 routing-instance rt-i-1;
    maximum-hop-count 10;
    minimum-wait-time 300;
    client-response-ttl 20;
    vpn;
    interface {
      ge-0/0/0 {
        no-listen;
        broadcast;
        description text;
        maximum-hop-count 20;
        minimum-wait-time 400;
        client-response-ttl 30;
        vpn;
        dhcp-option82;
      }
    }
  }
}
```

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

Verification

Confirm that the configuration is working properly.

- [Verifying DHCP Relay Statistics on page 87](#)

Verifying DHCP Relay Statistics

Purpose Verify that the DHCP Relay statistics have been configured.

Action From operational mode, enter the **show system services dhcp relay-statistics** command.

```
user@host> show system services dhcp relay-statistics

Received Packets:    4 Forwarded Packets    4 Dropped Packets
      4      Due to missing interface in relay database: 4      Due to missing
matching routing instance: 0      Due to an error during packet read: 0      Due
to an error during packet send: 0      Due to invalid server address: 0      Due
to missing valid local address: 0      Due to missing route to server/client: 0
```

**Related
Documentation**

- [DHCP Server, Client, and Relay Agent Overview on page 69](#)
- [Understanding DHCP Relay Agent Operation on page 83](#)
- [DHCP Settings and Restrictions Overview on page 88](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS System Basics and Services Command Reference](#)
- [Junos OS Policy Framework Configuration Guide](#)

DHCP Settings and Restrictions Overview

This section contains the following topics:

- [Propagation of TCP/IP Settings for DHCP on page 88](#)
- [DHCP Conflict Detection and Resolution on page 88](#)
- [DHCP Interface Restrictions on page 89](#)

Propagation of TCP/IP Settings for DHCP

The Juniper Networks device can operate simultaneously as a client of the DHCP server in the untrust zone and a DHCP server to the clients in the trust zone. The device takes the TCP/IP settings that it receives as a DHCP client and forwards them as a DHCP server to the clients in the trust zone. The device interface in the untrust zone operates as the DHCP client, receiving IP addresses dynamically from an Internet service provider (ISP) on the external network.

During the DHCP protocol exchange, the device receives TCP/IP settings from the external network on its DHCP client interface. Settings include the address of the ISP's DHCP name server and other server addresses. These settings are propagated to the DHCP server pools configured on the device to fulfill host requests for IP addresses on the device's internal network.

DHCP Conflict Detection and Resolution

A client that receives an IP address from the device operating as a DHCP server performs a series of Address Resolution Protocol (ARP) tests to verify that the address is available and no conflicts exist. If the client detects an address conflict, it informs the DHCP server about the conflict and can request another IP address from the DHCP server.

The device maintains a log of all client-detected conflicts and removes addresses with conflicts from the DHCP address pool. To display the conflicts list, you use the **show system services dhcp conflict** command. The addresses in the conflicts list remain excluded until you use the **clear system services dhcp conflict** command to manually clear the list.

DHCP Interface Restrictions

The device supports DHCP client requests received on any Ethernet interface. DHCP requests received from a relay agent are supported on all interface types.

DHCP is not supported on interfaces that are part of a virtual private network (VPN).

Related Documentation

- [DHCP Server, Client, and Relay Agent Overview on page 69](#)
- [Understanding DHCP Server Operation on page 71](#)
- [Understanding DHCP Client Operation on page 78](#)
- [Understanding DHCP Relay Agent Operation on page 83](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

CHAPTER 7

DHCPv6 Local Server Configuration

- [DHCPv6 Server Overview on page 91](#)
- [Example: Configuring DHCPv6 Server Options on page 92](#)
- [Example: Configuring an Address-Assignment Pool on page 95](#)
- [Configuring Address-Assignment Pool and Address Features on page 98](#)
- [Creating a Security Policy for DHCPv6 on page 100](#)

DHCPv6 Server Overview

A Dynamic Host Configuration Protocol version 6 (DHCPv6) server can automatically allocate IP addresses to IP version 6 (IPv6) clients and deliver configuration settings to client hosts on a subnet or to requesting devices that need an IPv6 prefix. A DHCPv6 server lets network administrators centrally manage a pool of IP addresses among hosts and automate the assignment of IP addresses in a network.



NOTE: SRX Series and J Series devices do not support DHCP client authentication. In a DHCPv6 deployment, security policies control access through the device for any DHCP client that has received an address and other attributes from the DHCPv6 server.

Some features include:

- Configuration for a specific interface or a group of interfaces
- Stateless address autoconfiguration (SLAAC)
- Prefix delegation, including access-internal route installation
- DHCPv6 server groups

The DHCPv6 server configuration usually consists of DHCPv6 options for clients, an IPv6 prefix, an address pool that contains IPv6 address ranges and options, and a security policy to allow DHCPv6 traffic. In a typical setup the provider Juniper Networks device is configured as an IPv6 prefix delegation server that assigns addresses to the customer edge device. The customer's edge router then provides addresses to internal devices.

To configure DHCPv6 local server on a device, you include the DHCPv6 statement at the **[edit system services dhcp-local-server]** hierarchy level. You then create an address assignment pool for DHCPv6 that is configured in the **[edit access address-assignment pool]** hierarchy level using the **family inet6** statement.

You can also include the **dhcpv6** statement at the **[edit routing-instances routing-instance-name system services dhcp-local-server]** hierarchy.



NOTE: Existing DHCPv4 configurations in the **[edit system services dhcp]** hierarchy are not affected when you upgrade to Junos OS Release 10.4 from an earlier version or enable DHCPv6 server.

Related Documentation

- [Example: Configuring DHCPv6 Server Options on page 92](#)
- [Example: Configuring an Address-Assignment Pool on page 95](#)
- [Configuring a Named Address Range for Dynamic Address Assignment on page 98](#)
- [Creating a Security Policy for DHCPv6 on page 100](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS CLI Reference](#)

Example: Configuring DHCPv6 Server Options

This example shows how to configure DHCPv6 server options.

- [Requirements on page 92](#)
- [Overview on page 93](#)
- [Configuration on page 93](#)
- [Verification on page 94](#)

Requirements

Before you begin:

- Determine the IPv6 address pool range. See [Configuring the DHCPv6 Local Address Pools](#).
- Determine the IPv6 prefix. See the [Junos OS Security Configuration Guide](#).
- Determine the grace period, maximum lease time, or any custom options that should be applied to clients. See the [Junos OS Security Configuration Guide](#).
- List the IP addresses that are available for the devices on your network; for example, DNS and SIP servers.

Overview

In this example, you set a default client limit as 100 for all DHCPv6 groups. You then create a group called my-group that contains at least one interface. In this case, the interface is ge-0/0/3.0. You set a range of interfaces using the upto command and set a custom client limit as 200 for group my-group that overrides the default limit. Finally, you configure interface ge-0/0/3.0 with IPv6 address 3000::1/64 and set router advertisement for interface ge-0/0/3.0.



NOTE: A DHCPv6 group must contain at least one interface.

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 services dhcp-local-server dhcpv6 overrides interface-client-limit 100
set system services dhcp-local-server dhcpv6 group my-group interface ge-0/0/3.0
set system services dhcp-local-server dhcpv6 group my-group interface ge-0/0/3.0 upto
  ge-0/0/6.0
set system services dhcp-local-server dhcpv6 group my-group overrides
  interface-client-limit 200
set interfaces ge-0/0/3 unit 0 family inet6 address 3000::1/64
set protocols router-advertisement interface ge-0/0/3.0 prefix 3000::/64
```

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* in the *Junos OS CLI User Guide*.

To configure DHCPv6 server options:

1. Configure a DHCP local server.

```
[edit]
user@host# edit system services dhcp-local-server dhcpv6
```
2. Set a default limit for all DHCPv6 groups.

```
[edit system services dhcp-local-server dhcpv6]
user@host# set overrides interface-client-limit 100
```
3. Specify a group name and interface.

```
[edit system services dhcp-local-server dhcpv6]
user@host# set group my-group interface ge-0/0/3.0
```
4. Set a range of interfaces.

```
[edit system services dhcp-local-server dhcpv6]
user@host# set group my-group interface ge-0/0/3.0 upto ge-0/0/6.0
```
5. Set a custom client limit for the group.

```
[edit system services dhcp-local-server dhcpv6]
user@host# set group my-group overrides interface-client-limit 200
```

6. Configure an interface with an IPv6 address.

```
[edit interfaces]
user@host# set ge-0/0/3 unit 0 family inet6 address 3000::1/64
```

7. Set router advertisement for the interface.

```
[edit protocols]
user@host# set router-advertisement interface ge-0/0/3.0 prefix 3000::/64
```

Results From configuration mode, confirm your configuration by entering the **show system services dhcp-local-server**, **show interfaces ge-0/0/3**, and **show protocols** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system services dhcp-local-server
dhcpv6 {
  overrides {
    interface-client-limit 100;
  }
  group my-group {
    overrides {
      interface-client-limit 200;
    }
    interface ge-0/0/3.0 {
      upto ge-0/0/6.0;
    }
  }
}
[edit]
user@host# show interfaces ge-0/0/3
unit 0 {
  family inet6 {
    address 3000::1/64;
  }
}
[edit]
user@host# show protocols
router-advertisement {
  interface ge-0/0/3.0 {
    prefix 3000::1/64;
  }
}
```

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

Verification

Confirm that the configuration is working properly.

- [Verifying DHCPv6 Local Server Configuration on page 95](#)

Verifying DHCPv6 Local Server Configuration

Purpose	Verify that the client address bindings and statistics for the DHCPv6 local server have been configured
Action	<p>From operational mode, enter these commands:</p> <ul style="list-style-type: none">• show dhcpv6 server binding command to display the address bindings in the client table on the DHCPv6 local server.• show dhcpv6 server statistics command to display the DHCPv6 local server statistics.• clear dhcpv6 server bindings all command to clear all DHCPv6 local server bindings. You can clear all bindings or clear a specific interface, or routing instance.• clear dhcpv6 server statistics command to clear all DHCPv6 local server statistics.
Related Documentation	<ul style="list-style-type: none">• DHCPv6 Server Overview on page 91• Example: Configuring an Address-Assignment Pool on page 95• Configuring a Named Address Range for Dynamic Address Assignment on page 98• Creating a Security Policy for DHCPv6 on page 100• Junos OS Security Configuration Guide• Junos OS Feature Support Reference for SRX Series and J Series Devices• Junos OS System Basics and Services Command Reference

Example: Configuring an Address-Assignment Pool

This example shows how to configure an address-assignment pool.

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

Requirements

Before you begin:

- Specify the name of the address-assignment pool and configure addresses for the pool. See [Configuring the DHCPv6 Local Address Pools](#).
- Set DHCPv6 attributes for the address-assignment pool. See the [Junos OS Security Configuration Guide](#).

Overview

In this example, you configure an address-pool called my-pool and specify the IPv6 family as inet6. You configure the IPv6 prefix as 3000:0000::/10, the range name as range1, and the IPv6 range for DHCPv6 clients from a low of 3000:0000::/32 to a high of 3000:1000::/32. You can define the range based on the lower and upper boundaries of the prefixes in the range or based on the length of the prefixes in the range. Finally, you specify the DHCPv6 attribute for the DNS server as 3001::1, the grace period as 3600, and the maximum lease time as 120.

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 access address-assignment pool my-pool family inet6 prefix 3000:0000::/10
set access address-assignment pool my-pool family inet6 range range1 low
  3000:0000::/32 high 3000:1000::/32
set access address-assignment pool my-pool family inet6 dhcp-attributes dns-server
  3001::1
set access address-assignment pool my-pool family inet6 dhcp-attributes grace-period
  3600
set access address-assignment pool my-pool family inet6 dhcp-attributes
  maximum-lease-time 120
```

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* in the *Junos OS CLI User Guide*.

To configure an IPv6 address-assignment pool:

1. Configure an address-pool and specify the IPv6 family.

```
[edit access]
user@host# edit address-assignment pool my-pool family inet6
```
2. Configure the IPv6 prefix, the range name, and IPv6 range for DHCPv6 clients.

```
[edit access address-assignment pool my-pool family inet6]
user@host# set prefix 3000:0000::/10
user@host# set range range1 low 3000:0000::/32 high 3000:1000::/32
```
3. Configure the DHCPv6 attribute for the DNS server for the address pool.

```
[edit access address-assignment pool my-pool family inet6]
user@host# set dhcp-attributes dns-server 3001::1
```
4. Configure the DHCPv6 attribute for the grace period.

```
[edit access address-assignment pool my-pool family inet6]
user@host# set dhcp-attributes grace-period 3600
```
5. Configure the DHCPv6 attribute for the maximum lease time.

```
[edit access address-assignment pool my-pool family inet6]
```

```
user@host# set dhcp-attributes maximum-lease-time 120
```

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

```
[edit]
user@host# show access address-assignment
pool my-pool {
  family inet6 {
    prefix 3000:0000::/10;
    range range1 {
      low 3000:0000::/32;
      high 3000:1000::/32;
    }
    dhcp-attributes {
      maximum-lease-time 120;
      grace-period 3600;
      dns-server {
        3001::1;
      }
    }
  }
}
```

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

Verification

Confirm that the configuration is working properly.

- [Verifying Configuration on page 97](#)

Verifying Configuration

Purpose Verify that the address-assignment pool has been configured.

Action From operational mode, enter the **show access address-assignment** command.

- Related Documentation**
- [DHCPv6 Server Overview on page 91](#)
 - [Example: Configuring DHCPv6 Server Options on page 92](#)
 - [Configuring a Named Address Range for Dynamic Address Assignment on page 98](#)
 - [Creating a Security Policy for DHCPv6 on page 100](#)
 - [Junos OS Security Configuration Guide](#)
 - [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
 - [Junos OS System Basics and Services Command Reference](#)

Configuring Address-Assignment Pool and Address Features

This section contains the following topics:

- [Configuring a Named Address Range for Dynamic Address Assignment on page 98](#)
- [Configuring Address-Assignment Pool Linking on page 98](#)
- [Configuring DHCP Client-Specific Attributes on page 99](#)
- [Configuring an Address-Assignment Pool for Router Advertisement on page 99](#)

Configuring a Named Address Range for Dynamic Address Assignment

You can optionally configure multiple named ranges, or subsets of addresses, within an address-assignment pool. During dynamic address assignment, a client can be assigned an address from a specific named range. To create a named range, you specify a name for the range and define the address range and DHCPv6 attributes.

To configure a named address range for dynamic address assignment:

1. Specify the name of the address-assignment pool and the IPv6 family.

```
[edit access]
user@host# edit address-assignment pool my-pool2 family inet6
```

2. Configure the IPv6 prefix and then define the range name and IPv6 range for DHCPv6 clients. You can define the range based on the lower and upper boundaries of the prefixes in the range, or based on the length of the prefixes in the range.

```
[edit access address-assignment pool my-pool2 family inet6]
user@host# set prefix 3000:5000::/10
user@host# set range range2 low 3000:2000::/32 high 3000:3000::/32
```

3. Configure DHCPv6 attributes for the address pool.

```
[edit access address-assignment pool my-pool2 family inet6]
user@host# set dhcp-attributes dns-server 2001:db8:18:: grace-period 3600
maximum-lease-time 120
```

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

Configuring Address-Assignment Pool Linking

Address-assignment pool linking enables you to specify a secondary address pool for the device to use when the primary address-assignment pool is fully allocated. When the primary pool has no available addresses remaining, the device automatically switches over to the linked secondary pool and begins allocating addresses from that pool. The device uses a secondary pool only when the primary address-assignment pool is fully allocated.

You can create a chain of multiple linked pools. For example, you can link pool A to pool B, and link pool B to pool C. When pool A has no available addresses, the device switches to pool B for addresses. When pool B is exhausted, the device switches to pool C. There is no limit to the number of linked pools in a chain. However, you cannot create multiple

links to or from the same pool—a pool can be linked to only one secondary pool, and a secondary pool can be linked from only one primary pool.

To link a primary address-assignment pool named `pool1` to a secondary pool named `pool2`:

```
[edit access address-assignment]
user@host# set pool pool1 link pool2
```

Configuring DHCP Client-Specific Attributes

You use the address-assignment pool feature to include application-specific attributes when clients obtain an address. A client application, such as DHCPv6, uses the attributes to determine how addresses are assigned and to provide optional application-specific characteristics to the client. For example, the DHCPv6 application might specify that a client that matches certain prerequisite information is dynamically assigned an address from a particular named range. Based on which named range is used, DHCPv6 specifies additional DHCPv6 attributes such as the DNS server or the maximum lease time for clients.

You use the **dhcp-attributes** statement to configure DHCPv6 client-specific attributes for address-assignment pools at the **[edit access address-assignment pool *pool-name* family inet6] hierarchy**.

Table 12 on page 99 describes the DHCPv6 client attributes for configuring IPv6 address-assignment pools.

Table 12: DHCPv6 Attributes

Attribute	Description	DHCPv6 Option
dns-server	IPv6 address of DNS server to which clients can send DNS queries	23
grace-period	Grace period offered with the lease	—
maximum-lease-time	Maximum lease time allowed by the DHCPv6 server	—
option	User-defined options	—
sip-server-address	IPv6 address of SIP outbound proxy server	22
sip-server-domain-name	Domain name of the SIP outbound proxy server	21

Configuring an Address-Assignment Pool for Router Advertisement

You can create an address-assignment pool that is explicitly used for router advertisement address assignment. You populate the address-assignment pool using the standard procedure, but you additionally specify that the pool is used for router advertisement.

To configure an address-assignment pool that is used for router advertisement:

1. Create the IPv6 address-assignment pool.
2. Specify that the address-assignment pool is used for router advertisement.

```
[edit access address-assignment]  
user@host# set neighbor-discovery-router-advertisement router1
```
3. If you are done configuring the device, enter **commit** from configuration mode.

**Related
Documentation**

- [DHCPv6 Server Overview on page 91](#)
- [Example: Configuring DHCPv6 Server Options on page 92](#)
- [Example: Configuring an Address-Assignment Pool on page 95](#)
- [Creating a Security Policy for DHCPv6 on page 100](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS System Basics and Services Command Reference](#)

Creating a Security Policy for DHCPv6

For the DHCPv6 server to allow DHCPv6 requests, you must create a security policy to enable DHCPv6 traffic. In this example, the zone my-zone allows DHCPv6 traffic from the zone untrust, and the ge-0/0/3.0 interface is configured with the IPv6 address 3000:1.

To create a security zone policy to allow DHCPv6:

1. Create the zone and add an interface to that zone.

```
[edit security zones]  
user@host# edit security-zone my-zone interfaces ge-0/0/3.0
```
2. Configure host inbound traffic system services to allow DHCPv6.

```
[edit security zones security-zone my-zone interfaces ge-0/0/3.0]  
user@host# set host-inbound-traffic system-services dhcpv6
```
3. If you are done configuring the device, enter **commit** from configuration mode.

**Related
Documentation**

- [DHCPv6 Server Overview on page 91](#)
- [Example: Configuring DHCPv6 Server Options on page 92](#)
- [Example: Configuring an Address-Assignment Pool on page 95](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS System Basics and Services Command Reference](#)

CHAPTER 8

Autoinstallation Configuration

- [Autoinstallation Overview on page 101](#)
- [Example: Configuring Autoinstallation on page 104](#)

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:

- [Supported Autoinstallation Interfaces and Protocols on page 101](#)
- [Typical Autoinstallation Process on a New Device on page 102](#)

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 13 on page 102](#) lists the protocols that the device can use on these interfaces for IP address acquisition.

Table 13: 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**

- [Example: Configuring Autoinstallation on page 104](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

Example: Configuring Autoinstallation

This example shows how to configure a device for autoinstallation.

- [Requirements on page 104](#)
- [Overview on page 104](#)
- [Configuration on page 105](#)
- [Verification on page 106](#)

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” on page 72](#).
- Create one of the following configuration files, and store it on a TFTP server in the network (see Configuration Files):
 - 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.

```
edit system
set autoinstallation configuration-servers ftp://user:password@sftpconfig.sp.com
set 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 in the [Junos OS CLI User Guide](#).

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
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 on page 106](#)

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

- [Autoinstallation Overview on page 101](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS System Basics and Services Command Reference](#)

CHAPTER 9

Licenses

- [Junos OS License Overview on page 107](#)
- [License Key Generation on page 109](#)
- [Managing License Keys on page 115](#)

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 107](#)
- [License Key Components on page 108](#)
- [License Management Fields Summary on page 108](#)

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 **li29183743** is the license ID, and the trailing block of data is the license data:

```
li29183743 4ky27y acasck 82fsj6 jzsn4q ix8i8d adj7kr
            8uq38t ix8i8d jzsn4q ix8i8d 4ky27y acasck
            82fsj6 ii8i7e adj7kr 8uq38t ks2923 a9382e
```

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 14 on page 108](#).

Table 14: 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 14: 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

- [Generating a License Key on page 109](#)
- [Updating License Keys on page 116](#)
- [Saving License Keys on page 116](#)
- [Downloading License Keys on page 116](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

License Key Generation

This section contains the following topics:

- [Generating a License Key on page 109](#)
- [Example: Adding a New License Key on page 110](#)
- [Example: Deleting a License Key on page 113](#)

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

- [Example: Adding a New License Key on page 110](#)
- [Example: Deleting a License Key on page 113](#)
- [Updating License Keys on page 116](#)
- [Downloading License Keys on page 116](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

Example: Adding a New License Key

This example shows how to add a new license key.

- [Requirements on page 110](#)
- [Overview on page 110](#)
- [Configuration on page 110](#)
- [Verification on page 112](#)

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 112](#)
- [Verifying License Usage on page 112](#)
- [Verifying Installed License Keys on page 113](#)

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
```

```
G03000002223 aeaqea qkjhd ambrha 3tkqkc ayareb zicik6
              nv6jck btlxao 2trfyq 65cdou r5tbbb xdarpq
              qq53lu qcx4vm ydakcs t3yyh2 v5mq
```

```
G03000002224 aeaqea qkjhd ambrha 3tkqkc ayargb zicik6
              nv6jck btlxao 2trfyq 65cdou r5tbof l4uon5
              7rokz7 wgdocl r4q32p 2wu4zf zrxax
```

```
G03000002225 aeaqea qkjhd ambrha 3tkqkc ayarab zicik6
              nv6jck btlxao 2trfyq 65cdou r5tbiu jr6ui2
              1mqgqj ouzq5a aiokdn 4tr4u2 wmcq
```

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 License Overview on page 107](#)
- [Generating a License Key on page 109](#)
- [Example: Deleting a License Key on page 113](#)
- [Updating License Keys on page 116](#)
- [Downloading License Keys on page 116](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

Example: Deleting a License Key

This example shows how to delete a license key.

- [Requirements on page 113](#)
- [Overview on page 114](#)
- [Configuration on page 114](#)
- [Verification on page 115](#)

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 on page 115](#)

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

- [Generating a License Key on page 109](#)
- [Example: Adding a New License Key on page 110](#)
- [Updating License Keys on page 116](#)
- [Downloading License Keys on page 116](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

Managing License Keys

This section contains the following topics:

- [Updating License Keys on page 116](#)
- [Saving License Keys on page 116](#)
- [Displaying License Keys on page 116](#)
- [Downloading License Keys on page 116](#)

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://ael.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
```

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
```

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.

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 License Overview on page 107](#)
- [Generating a License Key on page 109](#)
- [Example: Adding a New License Key on page 110](#)
- [Example: Deleting a License Key on page 113](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

PART 2

Upgrades and Reboots

- [Junos OS Upgrades and Reboots for the SRX Series Devices on page 121](#)
- [Junos OS Upgrades and Reboots for J Series Devices on page 169](#)

CHAPTER 10

Junos OS Upgrades and Reboots for the SRX Series Devices

- [Understanding Junos OS Upgrades for SRX Series Devices on page 121](#)
- [Understanding Junos OS Upgrade and Downgrade Procedures for on SRX Series Devices on page 122](#)
- [Configuring External CompactFlash on SRX650 Devices on page 123](#)
- [Junos OS Initial Installation and Upgrade Tasks on page 124](#)
- [Junos OS Upgrades, Downgrades, and Reboots on page 128](#)
- [Installing Junos OS on page 143](#)
- [Download Manager on page 147](#)
- [Dual-Root Partitioning on page 150](#)
- [Autorecovery on page 159](#)
- [Auto BIOS Upgrade on SRX Series Devices on page 162](#)
- [Manual BIOS Upgrade on SRX Series Devices on page 164](#)

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 122](#)
 - [Preparing Your SRX Series Device for Junos OS Upgrades on page 124](#)
 - [Junos OS Upgrade Methods on the SRX Series Devices on page 128](#)
 - [Example: Installing Junos OS Upgrades on SRX Series Devices on page 130](#)
 - [Installing Junos OS Using a USB Device on SRX Series Devices on page 146](#)
 - [Junos OS System Basics Configuration Guide](#)
 - [Junos OS Feature Support Reference for SRX Series and J Series 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 121](#)
 - [Preparing Your SRX Series Device for Junos OS Upgrades on page 124](#)
 - [Junos OS Upgrade Methods on the SRX Series Devices on page 128](#)
 - [Example: Installing Junos OS Upgrades on SRX Series Devices on page 130](#)
 - [Example: Downgrading Junos OS on SRX Series Devices on page 133](#)
 - [Installing Junos OS Using a USB Device on SRX Series Devices on page 146](#)

- [Junos OS Security Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS Installation and Upgrade Guide](#)

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 121](#)
- [Preparing Your SRX Series Device for Junos OS Upgrades on page 124](#)
- [Junos OS Upgrade Methods on the SRX Series Devices on page 128](#)
- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 130](#)
- [Installing Junos OS Using a USB Device on SRX Series Devices on page 146](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

- [Junos OS Installation and Upgrade Guide](#)

Junos OS Initial Installation and Upgrade Tasks

This section contains the following topics:

- [Preparing Your SRX Series Device for Junos OS Upgrades on page 124](#)
- [Verifying Available Disk Space on SRX Series Devices on page 125](#)
- [Downloading Junos OS Upgrades for SRX Series Devices on page 125](#)
- [Preparing the USB Flash Drive to Upgrade Junos OS on page 126](#)

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 15 on page 124](#) lists the secondary storage devices available on an SRX Series devices.

Table 15: 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.

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

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.

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

- [Configuring External CompactFlash on SRX650 Devices on page 123](#)
- [Junos OS Upgrade Methods on the SRX Series Devices on page 128](#)
- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 130](#)
- [Example: Downgrading Junos OS on SRX Series Devices on page 133](#)
- [Installing Junos OS Using a USB Device on SRX Series Devices on page 146](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS Installation and Upgrade Guide](#)

Junos OS Upgrades, Downgrades, and Reboots

This section contains the following topics:

- [Junos OS Upgrade Methods on the SRX Series Devices on page 128](#)
- [Installing Junos OS Upgrades from a Remote Server on the SRX Series Devices on page 129](#)
- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 130](#)
- [Example: Downgrading Junos OS on SRX Series Devices on page 133](#)
- [Example: Configuring Boot Devices for SRX Series Devices on page 135](#)
- [Example: Rebooting SRX Series Devices on page 138](#)
- [Example: Halting SRX Series Devices on page 140](#)
- [Bringing Chassis Components Online and Offline on SRX Series Devices on page 141](#)
- [Restarting the Chassis on SRX Series Devices on page 142](#)
- [Upgrading the Boot Loader on SRX Series Devices on page 142](#)

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 129](#)
- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 130](#)
- [Example: Downgrading Junos OS on SRX Series Devices on page 133](#)
- [Installing Junos OS Using a USB Device on SRX Series Devices on page 146](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS Installation and Upgrade Guide](#)

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 125](#).
- Download the Junos OS package. See [“Downloading Junos OS Upgrades for SRX Series Devices” on page 125](#).

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 16 on page 130](#).

Table 16: 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 128](#)
- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 130](#)
- [Example: Downgrading Junos OS on SRX Series Devices on page 133](#)
- [Installing Junos OS Using a USB Device on SRX Series Devices on page 146](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS Installation and Upgrade Guide](#)

Example: Installing Junos OS Upgrades on SRX Series Devices

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

- [Requirements on page 131](#)
- [Overview on page 131](#)

- [Configuration on page 131](#)
- [Verification on page 132](#)

Requirements

Before you begin:

- Verify the available space on the internal media. See “[Verifying Available Disk Space on SRX Series Devices](#)” on page 125.
- Download the software package. See “[Downloading Junos OS Upgrades for SRX Series Devices](#)” on page 125.
- 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 reboots 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 in the [Junos OS CLI User Guide](#).

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 on page 132](#)

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 135](#)
- [Junos OS Upgrade Methods on the SRX Series Devices on page 128](#)
- [Example: Downgrading Junos OS on SRX Series Devices on page 133](#)
- [Installing Junos OS Using a USB Device on SRX Series Devices on page 146](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS Installation and Upgrade Guide](#)

Example: Downgrading Junos OS on SRX Series Devices

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

- [Requirements on page 133](#)
- [Overview on page 133](#)
- [Configuration on page 133](#)
- [Verification on page 134](#)

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* in the [Junos OS CLI User Guide](#).

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 on page 135](#)

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

- [Example: Configuring Boot Devices for SRX Series Devices on page 135](#)
- [Junos OS Upgrade Methods on the SRX Series Devices on page 128](#)
- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 130](#)
- [Example: Rebooting SRX Series Devices on page 138](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS Installation and Upgrade Guide](#)

Example: Configuring Boot Devices for SRX Series Devices

This example shows how to configure a boot device.

- [Requirements on page 135](#)
- [Overview on page 135](#)
- [Configuration on page 136](#)
- [Verification on page 137](#)

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 124](#).

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 in the [Junos OS CLI User Guide](#).

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 on page 137](#)

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 142](#)
 - [Junos OS Upgrade Methods on the SRX Series Devices on page 128](#)
 - [Example: Installing Junos OS Upgrades on SRX Series Devices on page 130](#)
 - [Example: Rebooting SRX Series Devices on page 138](#)
 - [Junos OS Security Configuration Guide](#)
 - [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
 - [Junos OS Installation and Upgrade Guide](#)

Example: Rebooting SRX Series Devices

This example shows how to reboot a device.

- [Requirements on page 138](#)
- [Overview on page 138](#)
- [Configuration on page 138](#)
- [Verification on page 139](#)

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 in the *Junos OS CLI User Guide*.

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 on page 139](#)

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 135](#)
- [Junos OS Upgrade Methods on the SRX Series Devices on page 128](#)
- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 130](#)
- [Example: Halting SRX Series Devices on page 140](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

- [Junos OS Installation and Upgrade Guide](#)

Example: Halting SRX Series Devices

This example shows how to halt a device.

- [Requirements on page 140](#)
- [Overview on page 140](#)
- [Configuration on page 140](#)
- [Verification on page 141](#)

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 in the [Junos OS CLI User Guide](#).

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 on page 141](#)

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 135](#)
- [Junos OS Upgrade Methods on the SRX Series Devices on page 128](#)
- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 130](#)
- [Bringing Chassis Components Online and Offline on SRX Series Devices on page 141](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS Installation and Upgrade Guide](#)

Bringing Chassis Components Online and Offline on SRX 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:

- **cluster**—Changes the chassis cluster status.
- **fpc**—Changes the Flexible PIC Concentrator (FPC) status.

Related Documentation

- [Example: Configuring Boot Devices for SRX Series Devices on page 135](#)
- [Junos OS Upgrade Methods on the SRX Series Devices on page 128](#)
- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 130](#)
- [Restarting the Chassis on SRX Series Devices on page 142](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS Installation and Upgrade Guide](#)

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 135](#)
- [Junos OS Upgrade Methods on the SRX Series Devices on page 128](#)
- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 130](#)
- [Upgrading the Boot Loader on SRX Series Devices on page 142](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS Installation and Upgrade Guide](#)

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 121](#)
- [Example: Configuring Boot Devices for SRX Series Devices on page 135](#)
- [Junos OS Upgrade Methods on the SRX Series Devices on page 128](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS Installation and Upgrade Guide](#)

Installing Junos OS

The following section contains the following topics:

- [Installing Junos OS Using TFTP on SRX Series Devices on page 144](#)
- [Installing Junos OS Using a USB Device on SRX Series Devices on page 146](#)
- [Installing Junos OS from the Boot Loader Using a USB Storage Device on an SRX Series Device on page 147](#)

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 17 on page 145](#).

Table 17: 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 `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.

Installing Junos OS Using a USB Device on SRX Series Devices

To install the Junos OS image on an SRX Series device:

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

If the LEDs do not turn amber, press the Power button or power-cycle the device and wait for the LEDs to steadily turn amber.

2. Press the Reset Config button on the SRX Series device and wait for the LEDs to turn green, indicating that the Junos OS upgrade image has 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 turn 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.

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.

Download Manager

This section contains the following topics:

- [Understanding Download Manager on page 147](#)

Understanding Download Manager

- [Overview on page 148](#)
- [Using Download Manager to Upgrade Junos OS on page 148](#)
- [Handling Errors on page 149](#)
- [Considerations on page 149](#)

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 18 on page 149 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 18: show system download Output Fields

Output Field	Description
Status	State of the download.
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**
- [Junos OS CLI Reference](#)
 - [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

Dual-Root Partitioning

This section contains the following topics:

- [Dual-Root Partitioning Scheme Overview on page 150](#)
- [Junos OS Release 10.0 or Later Upgrades with Dual-Root Partitioning on SRX Series Devices on page 152](#)
- [Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 153](#)
- [Junos OS Release 9.6 or Earlier Installation on SRX Series Devices with Dual-Root Partitioning on page 156](#)
- [Understanding How the Primary Junos OS Image with Dual-Root Partitioning Recovers on SRX Series Devices on page 157](#)
- [Reinstalling the Single-Root Partition Using “request system software add” Command on page 158](#)

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.

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 151](#)
- [Important Features of the Dual-Root Partitioning Scheme on page 151](#)

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 19 on page 151](#) provides information on the storage media available on SRX Series devices.

Table 19: 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 121](#)
- [Junos OS Release 10.0 or Later Upgrades with Dual-Root Partitioning on SRX Series Devices on page 152](#)
- [Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 153](#)
- [Junos OS Release 9.6 or Earlier Installation on SRX Series Devices with Dual-Root Partitioning on page 156](#)
- [Understanding How the Primary Junos OS Image with Dual-Root Partitioning Recovers on SRX Series Devices on page 157](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS Installation and Upgrade Guide](#)

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 144](#)
- 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 Device on SRX Series Devices” on page 146](#)
- 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 150](#)
- [Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 153](#)
- [Junos OS Release 9.6 or Earlier Installation on SRX Series Devices with Dual-Root Partitioning on page 156](#)

- [Understanding How the Primary Junos OS Image with Dual-Root Partitioning Recovers on SRX Series Devices on page 157](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS Installation and Upgrade Guide](#)

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 153](#)
- [Overview on page 153](#)
- [Configuration on page 154](#)
- [Verification on page 156](#)

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 in the [Junos OS CLI User Guide](#).

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 142](#).
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 156](#)

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 150](#)
- [Junos OS Release 10.0 or Later Upgrades with Dual-Root Partitioning on SRX Series Devices on page 152](#)
- [Junos OS Release 9.6 or Earlier Installation on SRX Series Devices with Dual-Root Partitioning on page 156](#)
- [Understanding How the Primary Junos OS Image with Dual-Root Partitioning Recovers on SRX Series Devices on page 157](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS Installation and Upgrade Guide](#)

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: 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 121](#)
- [Dual-Root Partitioning Scheme Overview on page 150](#)

- [Junos OS Release 10.0 or Later Upgrades with Dual-Root Partitioning on SRX Series Devices on page 152](#)
- [Understanding How the Primary Junos OS Image with Dual-Root Partitioning Recovers on SRX Series Devices on page 157](#)
- [Reinstalling the Single-Root Partition Using “request system software add” Command on page 158](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS Installation and Upgrade Guide](#)

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 121](#)
- [Dual-Root Partitioning Scheme Overview on page 150](#)
- [Junos OS Release 10.0 or Later Upgrades with Dual-Root Partitioning on SRX Series Devices on page 152](#)
- [Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 153](#)
- [Junos OS Release 9.6 or Earlier Installation on SRX Series Devices with Dual-Root Partitioning on page 156](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS Installation and Upgrade Guide](#)

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.

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 150](#)
- [Junos OS Release 9.6 or Earlier Installation on SRX Series Devices with Dual-Root Partitioning on page 156](#)
- [Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 153](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS Installation and Upgrade Guide](#)

Autorecovery

This section contains the following topics:

- [Understanding Integrity Check and Autorecovery of Configuration, Licenses, and Disk Information on page 159](#)

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

- [Overview on page 159](#)
- [How Autorecovery Works on page 160](#)
- [How to Use Autorecovery on page 160](#)
- [Data That Is Backed Up in an Autorecovery on page 160](#)
- [Troubleshooting Alarms on page 161](#)
- [Considerations on page 161](#)

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 20 on page 161 lists types of autorecovery alarms, descriptions, and required actions.

Table 20: Autorecovery Alarms

Alarm	Alarm Type	Description	Action Required
Autorecovery information needs to be saved	Minor	This alarm indicates: <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.
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

- [Junos OS CLI Reference](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

Auto BIOS Upgrade on SRX Series Devices

This section includes the following topics:

- [Understanding Auto BIOS Upgrade Methods on the SRX Series Devices on page 162](#)
- [Disabling Auto BIOS Upgrade on SRX Series Devices on page 164](#)

Understanding Auto BIOS Upgrade Methods on the SRX Series Devices

Junos OS Release 11.1 ships with BIOS version 1.9.

For the SRX100, SRX210, SRX240, and SRX650 devices, [Table 21 on page 162](#) lists the minimum compatible BIOS versions.

Table 21: SRX Series Services Gateways BIOS Versions

SRX100	SRX210	SRX240	SRX650
1.6	1.5	1.5	1.5

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 version 1.9.

The BIOS upgrades automatically in the following scenarios:

- During Junos OS upgrade through either the J-Web user interface or the CLI.

In this case, only the active BIOS is upgraded. The following sample output is from upgrading the Junos OS using the CLI:

```
root> request system software upgrade no-copy no-validate
junos-srxsme-10.2B2-export.tgz
Formatting alternate root (/dev/da0s2a)...
/dev/da0s2a: 298.0MB (610284 sectors) block size 16384, fragment size 2048

        using 4 cylinder groups of 74.50MB, 4768 blks, 9600 inodes.
super-block backups (for fsck -b #) at:
32, 152608, 305184, 457760
Saving boot file package in /var/sw/pkg/ junos-srxsme-10.2B2-export.tgz
JUNOS requires BIOS version upgrade from 0.0 to 1.7
Upgrading to BIOS 1.7 ...
Upgrading Loader...
#####
Verifying the loader image... OK
Upgrading U-Boot...
#####
Verifying the new U-Boot image... OK
WARNING: The new boot firmware will take effect when the system is
rebooted.
JUNOS 10.2B2 will become active at next reboot
Saving state for rollback ...
```

- During loader installation using TFTP or USB.

In this case, only the active BIOS is upgraded. The following sample output is from the loader installation:

```

loader> install tftp:///junos-srxsme-10.2B2-export.tgz

Downloading /junos-srxsme-10.2B2-export.tgz from 10.207.18.111 ...
Verified SHA1 checksum of /a/cf/install/junos-boot-srxsme-10.2B2-export.tgz
Verified SHA1 checksum of /a/cf/install/junos-srxsme-10.2B2-export
JUNOS requires BIOS version upgrade from 0.0 to 1.7
Upgrading to BIOS 1.7 ...
Upgrading Loader...
#####
Verifying the loader image... OK
Upgrading U-Boot...
#####
Verifying the new U-Boot image... OK
WARNING: The new boot firmware will take effect when the system is
rebooted.

```

- During system boot-up.

In this case, both the active BIOS and the backup BIOS are upgraded. The following sample output is from system boot-up:

```

JUNOS requires backup BIOS version upgrade from 0.0 to 1.7
Upgrading to BIOS 1.7 ...
Upgrading Secondary U-Boot...
#####
Verifying the new U-Boot image... OK
JUNOS requires active BIOS version upgrade from 0.0 to 1.7
Upgrading to BIOS 1.7 ...
Upgrading Loader...
#####
Verifying the loader image... OK
Upgrading U-Boot...
#####
Verifying the new U-Boot image... OK
WARNING: The new boot firmware will take effect when the system is
rebooted.
BIOS upgrade completed successfully, rebooting ...

```



NOTE: The SRX650 device has only one set of BIOS. There is no backup BIOS upgrade for the SRX650 device.

Related Documentation

- [Understanding Junos OS Upgrades for SRX Series Devices on page 121](#)
- [Disabling Auto BIOS Upgrade on SRX Series Devices on page 164](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS Installation and Upgrade Guide](#)

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 121](#)
- [Understanding Auto BIOS Upgrade Methods on the SRX Series Devices on page 162](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS Installation and Upgrade Guide](#)

Manual BIOS Upgrade on SRX Series Devices

This section includes the following topics:

- [Understanding Manual BIOS Upgrade Using the Junos CLI on page 164](#)

Understanding Manual BIOS Upgrade Using the Junos CLI

This feature is supported on SRX100, SRX110, SRX210, SRX220, SRX240, and SRX650 devices. For these SRX Series devices, the BIOS consists of a U-boot and the Junos loader. The SRX240 and SRX650 Service Gateways also include a U-shell binary as part of the BIOS. Additionally, on SRX100, SRX110, SRX210, SRX220 and SRX240 Service Gateways, 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 22 on page 165](#) provides information on BIOS components supported for different SRX Series devices.

Table 22: Manual BIOS Upgrade Components

BIOS Components		SRX100	SRX110	SRX210	SRX220	SRX240	SRX650
Active	U-boot	Yes	Yes	Yes	Yes	Yes	Yes
	Loader	Yes	Yes	Yes	Yes	Yes	Yes
	U-shell					Yes	Yes
Backup	U-boot	Yes	Yes	Yes	Yes	Yes	

Table 23 on page 165 Lists the CLI commands used for manual BIOS upgrade.

Table 23: 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.

```
root> request system software add /var/tmp/jloader-srxsme-10.2B3-signed.tgz no-copy
no-validate
```

```
Installing package '/var/tmp/jloader-srxsme-10.2B3-signed.tgz' ...
Verified jloader-srxsme-10.2B3.tgz signed by PackageProduction_10_2_0
Adding jloader-srxsme...
Available space: 427640 require: 2674
Mounted jloader-srxsme package on /dev/md5...
Saving state for rollback ...
```

```
root> show version
```

```
Model: srx240h
JUNOS Software Release [10.2B3]
JUNOS BIOS Software Suite [10.2B3]
```



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. The available version is displayed under the **Available version** column.

```
root> show system firmware
```

Part	Type	Tag	Current version	Available version	Status
Routing Engine 0	RE BIOS	0	1.5	1.7	OK
Routing Engine 0	RE BIOS Backup	1	1.5	1.7	OK
Routing Engine 0	RE FPGA	11	12.3.0		OK

3. Upgrade the BIOS image.

Active BIOS:

- Initiate the upgrade using the **request system firmware upgrade re bios** command.

```
root> request system firmware upgrade re bios
```

Part	Type	Tag	Current version	Available version	Status
Routing Engine 0	RE BIOS	0	1.5	1.7	OK
Routing Engine 0	RE BIOS Backup	1	1.5	1.7	OK
Perform indicated firmware upgrade ? [yes,no] (no) yes					

```
Firmware upgrade initiated.
```

- Monitor the upgrade status using the **show system firmware** command.

```
root> show system firmware
```

Part	Type	Tag	Current version	Available version	Status
Routing Engine 0	RE BIOS	0	1.5	1.7	PROGRAMMING
Routing Engine 0	RE BIOS Backup	1	1.5	1.7	OK
Routing Engine 0	RE FPGA	11	12.3.0		OK

```
root> show system firmware
```

Part	Type	Tag	Current version	Available version	Status
Routing Engine 0	RE BIOS	0	1.5	1.7	UPGRADED SUCCESSFULLY
Routing Engine 0	RE BIOS Backup	1	1.5	1.7	OK
Routing Engine 0	RE FPGA	11	12.3.0		OK



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.

```
root> request system firmware upgrade re bios backup
```

Part	Type	Tag	Current version	Available version	Status
Routing Engine 0	RE BIOS	0	1.5	1.7	OK
Routing Engine 0	RE BIOS Backup	1	1.5	1.7	OK

Perform indicated firmware upgrade ? [yes,no] (no) yes

```
Firmware upgrade initiated.
```

2. Monitor the upgrade status using the **show system firmware** command.

```
root> show system firmware
```

Part	Type	Tag	Current version	Available version	Status
Routing Engine 0	RE BIOS	0	1.5	1.7	OK
Routing Engine 0	RE BIOS Backup	1	1.5	1.7	PROGRAMMING
Routing Engine 0	RE FPGA	11	12.3.0		OK

```
root> show system firmware
```

Part	Type	Tag	Current version	Available version	Status
Routing Engine 0	RE BIOS	0	1.5	1.7	OK
Routing Engine 0	RE BIOS Backup	1	1.7	1.7	UPGRADED SUCCESSFULLY
Routing Engine 0	RE FPGA	11	12.3.0		OK

**Related
Documentation**

- [Understanding Junos OS Upgrades for SRX Series Devices on page 121](#)
- [Understanding Auto BIOS Upgrade Methods on the SRX Series Devices on page 162](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS Installation and Upgrade Guide](#)

Junos OS Upgrades and Reboots for J Series Devices

- [Understanding Junos OS Upgrades for J Series Devices on page 169](#)
- [Junos OS Upgrades and Downloads on page 170](#)
- [Installing Junos OS Upgrades from a Remote Server on J Series Devices on page 173](#)
- [Example: Installing Junos OS Upgrades on J Series Devices on page 175](#)
- [Example: Downgrading Junos OS on J Series Devices on page 177](#)
- [Boot Device Configuration on page 179](#)
- [Example: Rebooting J Series Devices on page 183](#)
- [Example: Halting J Series Devices on page 184](#)
- [Chassis Configuration on page 186](#)

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 170](#)
 - [Downloading Junos OS Upgrades for J Series Devices on page 173](#)
 - [Example: Installing Junos OS Upgrades on J Series Devices on page 175](#)
 - [Example: Downgrading Junos OS on J Series Devices on page 177](#)
 - [Junos OS Security Configuration Guide](#)
 - [Junos OS System Basics Configuration Guide](#)
 - [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)

Junos OS Upgrades and Downloads

This section contains the following topics:

- [Understanding Junos OS Upgrade and Downgrade Procedures for J Series Devices on page 170](#)
- [Preparing Your J Series Services Router for Junos OS Upgrades on page 172](#)
- [Downloading Junos OS Upgrades for J Series Devices on page 173](#)

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 170](#)
- [Junos OS Recovery Packages on page 171](#)

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 172](#)
- [Downloading Junos OS Upgrades for J Series Devices on page 173](#)
- [Example: Installing Junos OS Upgrades on J Series Devices on page 175](#)
- [Example: Downgrading Junos OS on J Series Devices on page 177](#)
- [Junos OS Security Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS Installation and Upgrade Guide](#)

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 24 on page 172 lists the secondary storage devices available in a J Series device for backup.

Table 24: 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 170](#)
 - [Downloading Junos OS Upgrades for J Series Devices on page 173](#)
 - [Example: Installing Junos OS Upgrades on J Series Devices on page 175](#)
 - [Example: Downgrading Junos OS on J Series Devices on page 177](#)
 - [Junos OS System Basics Configuration Guide](#)
 - [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
 - [Junos OS Installation and Upgrade Guide](#)

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 170](#)
 - [Preparing Your J Series Services Router for Junos OS Upgrades on page 172](#)
 - [Example: Installing Junos OS Upgrades on J Series Devices on page 175](#)
 - [Example: Downgrading Junos OS on J Series Devices on page 177](#)
 - [Junos OS Security Configuration Guide](#)
 - [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
 - [Junos OS Installation and Upgrade Guide](#)

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 25 on page 174](#).

Table 25: 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 172](#)
- [Installing Junos OS Upgrades from a Remote Server on J Series Devices on page 173](#)
- [Example: Rebooting J Series Devices on page 183](#)
- [Example: Halting J Series Devices on page 184](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS Installation and Upgrade Guide](#)
- [Junos OS Migration Guide](#)

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 175](#)
- [Overview on page 175](#)
- [Configuration on page 175](#)
- [Verification on page 176](#)

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 173.
- 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 in the [Junos OS CLI User Guide](#).

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 on page 176](#)

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 172](#)
- [Installing Junos OS Upgrades from a Remote Server on J Series Devices on page 173](#)
- [Example: Rebooting J Series Devices on page 183](#)

- [Example: Halting J Series Devices on page 184](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS Installation and Upgrade Guide](#)
- [Junos OS Migration Guide](#)

Example: Downgrading Junos OS on J Series Devices

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

- [Requirements on page 177](#)
- [Overview on page 177](#)
- [Configuration on page 177](#)
- [Verification on page 179](#)

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* in the *Junos OS CLI User Guide*.

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 on page 179](#)

[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 172](#)
- [Example: Installing Junos OS Upgrades on J Series Devices on page 175](#)
- [Example: Rebooting J Series Devices on page 183](#)
- [Example: Halting J Series Devices on page 184](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS Installation and Upgrade Guide](#)
- [Junos OS Migration Guide](#)

Boot Device Configuration

This section contains the following topics:

- [Example: Configuring Boot Devices for J Series Devices on page 179](#)
- [Configuring a Boot Device to Receive Junos OS Failure Memory Snapshots in J Series Devices on page 182](#)

Example: Configuring Boot Devices for J Series Devices

This example shows how to configure a boot device.

- [Requirements on page 179](#)
- [Overview on page 179](#)
- [Configuration on page 180](#)
- [Verification on page 181](#)

[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 172](#).

[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](#) in the *Junos OS CLI User Guide*.

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 on page 181](#)

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 172](#)
- [Configuring a Boot Device to Receive Junos OS Failure Memory Snapshots in J Series Devices on page 182](#)
- [Example: Rebooting J Series Devices on page 183](#)
- [Example: Halting J Series Devices on page 184](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS Installation and Upgrade Guide](#)

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 26 on page 182 describes the **set system dump-device** command options.

Table 26: 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.
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 172](#)
- [Example: Configuring Boot Devices for J Series Devices on page 179](#)
- [Example: Rebooting J Series Devices on page 183](#)
- [Example: Halting J Series Devices on page 184](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS Installation and Upgrade Guide](#)

Example: Rebooting J Series Devices

This example shows how to reboot a J Series device.

- [Requirements on page 183](#)
- [Overview on page 183](#)
- [Configuration on page 183](#)
- [Verification on page 184](#)

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 in the [Junos OS CLI User Guide](#).

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 on page 184](#)

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 172](#)
- [Example: Installing Junos OS Upgrades on J Series Devices on page 175](#)
- [Example: Downgrading Junos OS on J Series Devices on page 177](#)
- [Example: Halting J Series Devices on page 184](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS Installation and Upgrade Guide](#)

Example: Halting J Series Devices

This example shows how to halt a J Series device.

- [Requirements on page 185](#)
- [Overview on page 185](#)
- [Configuration on page 185](#)
- [Verification on page 186](#)

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 in the [Junos OS CLI User Guide](#).

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 on page 186](#)

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 169](#)
- [Preparing Your J Series Services Router for Junos OS Upgrades on page 172](#)
- [Example: Downgrading Junos OS on J Series Devices on page 177](#)
- [Example: Rebooting J Series Devices on page 183](#)
- [Junos OS System Basics Configuration Guide](#)
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Junos OS Installation and Upgrade Guide](#)

Chassis Configuration

This section contains the following topics:

- [Bringing Chassis Components Online and Offline on J Series Devices on page 186](#)
- [Restarting the Chassis on J Series Devices on page 187](#)

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
```

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
```


PART 3

Index

- [Index on page 191](#)

Index

Symbols

#, comments in configuration statements.....	xv
(), in syntax descriptions.....	xv
< >, in syntax descriptions.....	xv
[], in configuration statements.....	xv
{ }, in configuration statements.....	xv
(pipe), in syntax descriptions.....	xv

A

access privileges	
denying and allowing commands.....	31
permission bits for.....	29
predefined.....	28
specifying.....	31
accounts See template accounts; user accounts	
address-assignment pools	
client attributes.....	99
configuring overview.....	95
DHCP attributes.....	99
dhcpv6 attributes.....	99
linking.....	98
named range.....	98
router advertisement.....	99
AT commands, for modem initialization	
description.....	53
modifying.....	66
attacks	
brute force, preventing.....	46
dictionary, preventing.....	46
authentication	
local password, by default.....	26
login classes.....	28, 31
methods.....	19, 20
order of user authentication (configuration editor).....	26
RADIUS authentication (configuration editor).....	21
specifying a method.....	26
specifying access privileges.....	31

TACACS+ authentication (configuration editor).....	23
user accounts.....	20, 31
autoinstallation	
automatic configuration process.....	102
CLI configuration editor.....	104
default configuration file.....	102
establishing.....	101
host-specific configuration file.....	102
interfaces.....	101
IP address procurement process.....	102
J-Web configuration editor.....	104
overview.....	101
protocols for procuring an IP address.....	101
requirements.....	104
status.....	106
TFTP server.....	102
verifying.....	106
autoinstallation, compatibility with the DHCP server.....	72
automatic configuration See autoinstallation	

B

basic connectivity	
secure Web access.....	11
BOOTP, for autoinstallation.....	104
braces, in configuration statements.....	xv
brackets	
angle, in syntax descriptions.....	xv
square, in configuration statements.....	xv
browser interface See J-Web interface	
brute force attacks, preventing.....	46

C

certificates See SSL certificates	
chassis-control	
restart options.....	142
clear system services dhcp conflicts	
command.....	88
CLI configuration editor	
autoinstallation.....	104
controlling user access.....	31
RADIUS authentication.....	21
secure access configuration.....	16
TACACS+ authentication.....	23
client attributes	
address-assignment pools.....	99
comments, in configuration statements.....	xv

configuration		DHCPv6 server	
autoinstallation of.....	101	preparation.....	92
downgrading software (CLI).....	133	diagnosis	
downgrading software (J-Web).....	133	verifying DHCP server operation.....	77
installation on multiple devices.....	101	verifying dialer interfaces.....	61
upgrading (CLI).....	130	dial-in, USB modem	
configuring address-assignment pool		voice not supported.....	51
dhcpv6.....	95	dial-up modem connection	
console port		configuring user end.....	64
disabling.....	43	connecting user end.....	65
securing.....	43	dialer interface, for USB modem	
controlling user access.....	31	adding (configuration editor).....	59
conventions		<i>See also</i> USB modem connections	
notice icons.....	xiv	verifying.....	61
text and syntax.....	xiv	dialer interface, USB modem	
curly braces, in configuration statements.....	xv	limitations.....	51
customer support.....	xvi	naming convention.....	51
contacting JTAC.....	xvi	restrictions.....	51
D		dictionary attacks, preventing.....	46
default configuration file, for autoinstallation.....	102	disabling	
deleting		console port.....	43
licenses (CLI).....	113	root login to console port.....	43
licenses (J-Web).....	113	disconnection of console cable for console	
device		logout.....	43
autoinstallation.....	101	displaying	
multiple, deploying <i>See</i> autoinstallation		licenses (J-Web).....	116
DHCP (Dynamic Host Configuration Protocol)		dl0.....	51
autoinstallation, compatibility with.....	72	documentation	
conflict detection and resolution.....	88	comments on.....	xvi
interface restrictions.....	89	downgrading	
options.....	72	software, with J-Web.....	133
overview.....	69	software, with the CLI	133
<i>See also</i> DHCP leases; DHCP pages; DHCP		download URL.....	125
pools; DHCP server		downloading	
server function.....	69	configuration, with autoinstallation.....	102
verification.....	76	licenses (J-Web).....	116
DHCP server		software upgrades.....	125
preparation.....	70	dual-root partitioning.....	121
sample configuration.....	70	dual-root partitioning scheme.....	150
subnet and single client.....	72, 79, 83	Dynamic Host Configuration Protocol <i>See</i> DHCP	
verifying operation.....	77	E	
DHCPv6		encrypted access	
configure server options.....	92	through HTTPS.....	11
dhcpv6		through SSL.....	11
configuring address-assignment pool.....	95	Ethernet ports	
DHCPv6 local server		autoinstallation on.....	101
overview.....	91		
dhcpv6 security policy configuration.....	100		

F

feature licenses *See* licenses
font conventions.....xiv

G

group licenses.....109

H

hardware
 supported platforms.....xiv
Hayes-compatible modem commands, USB
 modem initialization.....66
host-specific configuration file, for
 autoinstallation.....102
hostname
 opening an SSH session to.....45
 resolving.....70
 telnetting to.....44
hostname.conf file, for autoinstallation.....102, 104
HTTP (Hypertext Transfer Protocol)
 enabling Web access14
 enabling Web access (configuration
 editor).....16
 on built-in management interfaces.....11
 verifying configuration.....18
HTTPS (Hypertext Transfer Protocol over SSL)
 enabling secure access.....14
 enabling secure access (configuration
 editor).....16
 J-Web configuration.....14
 recommended for secure access.....11
 verifying secure access configuration.....18
HTTPS Web access, establishing.....11
Hypertext Transfer Protocol *See* HTTP
Hypertext Transfer Protocol over SSL *See* HTTPS

I

init-command-string command.....53
Install Remote page
 field summary.....130, 153
installation
 licenses (CLI).....110
 licenses (J-Web).....110
 software upgrades (CLI).....130
 software upgrades, from a remote server.....129
 software upgrades, uploading.....130
Internet Explorer, modifying for worldwide version
 of Junos OS.....5

ipconfig command.....77
 explanation.....77

J

J Series
 licenses.....107
 managing user authentication.....19
 user interfaces *See* user interfaces
J series
 install remote page
 field summary.....174
J series device
 boot devices.....179
 storing memory snapshots.....182
 See also CompactFlash card
 bring components online/offline.....186
 chassis-control
 restart options.....187
 compactFlash.....169
 CompactFlash card
 configuring.....179
 configuring for failure snapshot
 storage.....182
 configuration
 downgrading software (CLI).....177
 upgrading (CLI).....175
 configuration, downgrading software
 (J-Web).....177
 device
 halting (J-Web).....183
 downgrading
 software, with the CLI177
 downgrading software (J-Web).....177
 downloading.....173
 halting (CLI).....184
 halting a
 with J-Web.....183
 installation
 software upgrades (CLI).....175
 software upgrades, from a remote
 server.....173
 installing by uploading.....175
 internal CompactFlash card *See* CompactFlash
 card
 rebooting
 with J-Web183
 rebooting (CLI).....183
 request system halt command.....184
 request system reboot command.....183

request system snapshot command.....	179	Internet Explorer, modifying for worldwide	
options.....	179	version.....	5
reverting to a previous configuration file		upgrading.....	121
(J-Web).....	177	worldwide version, modifying Internet Explorer	
rolling back a configuration file.....	177	for.....	5
snapshots		Junos OS CLI	
configuring for failure snapshot		access privilege levels.....	29
storage.....	182	command modes.....	4
software.....	169	denying and allowing commands.....	31
software upgrades.....	169, 173	overview.....	4
software upgrades, uploading.....	175	Junos Scope application.....	3
storage media		Junos XML management protocol	
configuring boot devices.....	179	enabling secure access.....	14
upgrades		verifying secure access configuration.....	18
installing (CLI).....	175	Junos XML protocol over SSL.....	14
installing from remote server.....	173		
upgrades requirements.....	172	L	
upgrading.....	169	license infringement	
USB		identifying any licenses needed.....	108
configuring.....	179	verifying license usage.....	112
configuring for failure snapshot		verifying licenses installed.....	112, 115
storage.....	182	license keys	
J series device boot devices		components.....	108
configuring (CLI).....	179	displaying (CLI).....	113
configuring (J-Web).....	179	status.....	108
J-Web Configuration		version.....	108
secure Web access.....	14	licenses	
J-Web configuration		adding (CLI).....	110
adding users.....	31	adding (J-Web).....	110
authentication method.....	26	deleting (CLI).....	113
J-Web configuration editor		deleting (J-Web).....	113
autoinstallation.....	104	displaying (CLI).....	112, 115
controlling user access.....	31	displaying (J-Web).....	108, 116
RADIUS authentication.....	21	displaying usage.....	112
secure access.....	16	downloading (J-Web).....	116
TACACS+ authentication.....	23	generating.....	109
J-Web interface		group.....	109
Internet Explorer, modifying for worldwide		infringement, preventing.....	108
version of Junos OS.....	5	<i>See also</i> license infringement	
managing licenses.....	108	key.....	108
overview.....	3	<i>See also</i> license keys	
page layout.....	6	managing (J-Web).....	108
sessions.....	10	overview.....	107
starting.....	5	saving (CLI).....	116
windows, multiple, unpredictable results		updating (CLI).....	116
with.....	10	verifying.....	112, 115
Junos OS			
autoinstallation.....	101		
generating licenses.....	109		

- limitations
 - DHCP, no support on VPN interfaces.....89
 - Server relay and DHCP client cannot coexist in device.....69
 - software downgrade cannot be undone.....133
 - local password
 - default authentication method for system.....26
 - method for user authentication26
 - order of user authentication (configuration editor).....26
 - overview.....19, 20
 - local template accounts.....40
 - login classes
 - defining (configuration editor).....31
 - permission bits for.....29
 - predefined permissions.....28
 - specifying.....31
 - login retry limits, setting.....46
- M**
- managing
 - software.....121
 - user authentication.....19
 - manuals
 - comments on.....xvi
 - Microsoft Windows XP commands, connecting to device from a management device.....64
 - modem connection to router USB port
 - connecting USB modem to router.....54
 - modem connection to user management device
 - See USB modem connections
 - multiple devices
 - deploying See autoinstallation
- N**
- network.conf file, default for
 - autoinstallation.....102, 104
 - notice icons.....xiv
- O**
- openssl command.....12
 - operator login class permissions.....28
- P**
- parentheses, in syntax descriptions.....xv
 - password retry limits, setting.....46
- passwords**
- for downloading software upgrades.....125
 - local password method for user authentication.....26
 - See also local password
 - retry limits.....46
 - setting login retry limits.....46
- permission bits, for login classes.....29**
- permissions**
- denying and allowing commands.....31
 - predefined.....28
- ping command**
- DHCP server operation.....77
 - DHCP server operation, explanation.....77
- ports**
- console port, securing.....43
 - DHCP interface restrictions.....89
- protocols**
- DHCP See DHCP
- R**
- RADIUS**
- authentication (configuration editor).....21
 - order of user authentication (configuration editor).....26
 - secret (configuration editor).....21
 - specifying for authentication26
- RARP, for autoinstallation.....104**
- read-only login class permissions.....28**
- registration form, for software upgrades.....124**
- remote accounts**
- accessing with SSH (CLI).....45
 - accessing with Telnet (CLI).....44
 - remote template accounts.....40
- remote connection to device**
- connecting USB modem to user management device.....64
 - See also USB modem connections
- remote connection to router**
- connecting USB modem to router.....54
- remote server, upgrading from.....129**
- remote template accounts.....40**
- request interface modem reset umd0**
- command.....67
- request system license add command.....110**
- request system license add terminal**
- command.....110
- request system license delete command.....113**
- request system license save command.....116**

request system license update command.....	116
retry limits for passwords.....	46
Reverse Address Resolution Protocol (RARP), for autoinstallation.....	104
reverse SSH.....	48
reverse Telnet.....	48
reverting to a previous configuration file (J-Web).....	133
rolling back a configuration file, to downgrade software (CLI).....	133
root login to the console, disabling.....	43
router.conf file, for autoinstallation.....	102
S	
sample configuration for secure access.....	18
for SSL certificates.....	18
samples local template account.....	40
user account.....	31
saving licenses (CLI).....	116
secret RADIUS (configuration editor).....	21
TACACS+ (configuration editor).....	23
secure access establishing.....	11
generating SSL certificates.....	12
HTTPS access	14
HTTPS access (configuration editor).....	16
HTTPS recommended.....	11
installing SSL certificates.....	14
installing SSL certificates (configuration editor).....	16
Junos XML protocol SSL access.....	14
overview.....	11
requirements.....	12
sample configuration.....	18
verifying secure access configuration.....	18
Secure Sockets Layer See SSL	
security access privileges.....	28, 31
console port security.....	43
password retry limits.....	46
user accounts.....	20, 31
user authentication.....	19
serial cable, disconnection for console logout.....	43
Serial Line Address Resolution Protocol (SLARP), for autoinstallation.....	104
serial ports autoinstallation on.....	101
Series user interfaces See user interfaces	
Services Gateway licenses.....	107
user interfaces See user interfaces	
Services Router as a DHCP server.....	69
licenses.....	107
user interfaces See user interfaces	
sessions Telnet.....	44
sessions, J-Web.....	10
show chassis routing-engine bios.....	142
show interfaces dIO extensive command.....	61
show system autoinstallation status command.....	106
show system license command.....	112, 115
explanation.....	112, 115
show system license keys command.....	113
show system license usage command.....	112
explanation.....	112
show system services dhcp binding command.....	76
show system services dhcp binding detail command.....	76
show system services dhcp client command.....	81
show system services dhcp client interface command.....	81
show system services dhcp client statistics command.....	82
show system services dhcp conflict command.....	88
show system services dhcp global command.....	76
show system services dhcp relay-statistics command.....	87
explanation.....	87
show system snapshot media.....	137, 181
SLARP, for autoinstallation.....	104
SRC application.....	3
SRX Series licenses.....	107
managing user authentication.....	19
SRX series devices software upgrades.....	121

-
- SRX Series Services Gateway.....135 See storage
 - m
 - e
 - d
 - i
 - a
 - auto bios upgrade methods.....162
 - boot devices
 - configuring (CLI).....135
 - configuring (J-Web).....135
 - Chassis Components
 - Offline.....141
 - Online.....141
 - configuring boot devices.....135
 - dual-root partitioning.....150
 - halting a with J-Web.....140
 - halting immediately (CLI)140
 - halting with the CLI.....140
 - Install Remote page
 - field summary.....135
 - installing earlier version of Junos OS
 - with dual-root.....156
 - installing software
 - with CLI.....153
 - with J-Web.....153
 - Junos OS Release 10.0
 - upgrading with dual-root.....152
 - upgrading without dual-root.....128
 - multiple devices, using snapshots to replicate configurations
 - J-Web.....135
 - rebooting (CLI).....138
 - rebooting with J-Web138
 - reboots.....138, 140
 - recover of primary image.....157
 - request system halt command.....140
 - request system reboot command.....138
 - request system snapshot command.....135
 - show system storage partitions.....156
 - Snapshot page.....135
 - snapshots.....135
 - software upgrade methods.....128
 - See also boot devices
 - SSH
 - accessing remote accounts (CLI).....45
 - setting login retry limits.....46
 - ssh command.....45
 - options.....45
 - SSL (Secure Sockets Layer)
 - enabling secure access14
 - management access.....11
 - verifying SSL configuration.....18
 - SSL 3.0 option, disabling on Internet Explorer for
 - worldwide version of Junos OS.....5
 - SSL access, establishing.....11
 - SSL certificates
 - adding.....15
 - adding (configuration editor).....16
 - generating.....12
 - sample configuration.....18
 - verifying SSL configuration.....18
 - startup
 - J-Web interface.....5
 - status
 - autoinstallation.....106
 - license key.....108
 - super-user login class permissions.....28
 - superuser login class permissions.....28
 - support, technical See technical support
 - syntax conventions.....xiv
 - system.....36
 - retry options.....36
 - system management
 - login classes.....28, 31
 - template accounts.....39, 40
 - user accounts.....20, 31
 - user authentication.....19
 - T
 - TACACS+
 - authentication (configuration editor).....23
 - order of user authentication (configuration editor).....26
 - secret (configuration editor).....23
 - specifying for authentication.....26
 - taskbar.....6
 - technical support
 - contacting JTAC.....xvi
 - Telnet
 - accessing remote accounts (CLI).....44
 - setting login retry limits.....46
 - telnet
 - reverse.....48
 - reverse SSH.....48
 - telnet command.....44
 - options.....44
 - Telnet session.....44
 - template accounts
 - description.....39
 - local accounts (configuration editor).....40
 - remote accounts (configuration editor).....40

TFTP, for autoinstallation.....	102	predefined login classes.....	28
Trivial File Transfer Protocol (TFTP), for autoinstallation.....	102	templates for.....	39, 40
		<i>See also</i> template accounts	
U		user interfaces	
umd0.....	51	Junos Scope application.....	3
unauthorized login class permissions.....	28	overview.....	3
updating		preparation.....	5
licenses (CLI).....	116	SRC application.....	3
upgrades		username	
downloading.....	125	description.....	20
installing (CLI).....	130	specifying	31
installing by uploading.....	130	users	
installing from remote server.....	129	access privileges.....	28, 31
requirements.....	124	accounts <i>See</i> user accounts	
URLs		adding.....	31
software downloads.....	125	login classes.....	28, 31
USB modem connections		predefined login classes.....	28
configuring dial-up modem at user end.....	64	template accounts <i>See</i> template accounts	
connecting dial-up modem at user end.....	65	usernames.....	20
connecting to user end.....	64	V	
dialer interface <i>See</i> dialer interface, USB		verification	
modem		active licenses.....	112, 115
interface naming conventions.....	51	autoinstallation.....	106
requirements.....	54	DHCP server operation.....	77
USB modem interface types.....	51	DHCP statistics.....	87
verifying dialer interfaces.....	61	dialer interfaces.....	61
USB modem interfaces		license usage.....	112
dialer interface <i>See</i> dialer interface, USB		licenses	112, 115
modem		secure access.....	18
USB modems		version, license key.....	108
administering.....	66	voice calls, not supported in dial-in	51
AT commands.....	53	VPNs (virtual private networks), DHCP support on interfaces.....	89
AT commands, modifying.....	66	W	
connecting at user end.....	64	Web access, secure <i>See</i> secure access	
default modem initialization commands.....	53	Web browser, modifying Internet Explorer for worldwide version of Junos OS.....	5
default modem initialization commands, modifying.....	66	windows, J-Web, unpredictable results with multiple.....	10
initialization by device.....	53		
resetting.....	67		
user accounts			
authentication order (configuration editor).....	26		
contents.....	20		
creating (configuration editor).....	31		
for local users.....	40		
for remote users.....	40		