



Junos OS

J-Web Help Reference for SRX Series Devices

Release
19.2R1



Modified: 2019-06-26

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

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

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

Junos® OS J-Web Help Reference

Release 19.2R1

Copyright © 2019 Juniper Networks, Inc. All rights reserved.

Revision History

June 2017—Junos OS 15.1X49-D100

Nov 2017—Junos OS 17.4R1

Mar 2018—Junos OS 18.1R1

Jun 2018—Junos OS 18.2R1

Sep 2018—Junos OS 18.3R1

Dec 2018—Junos OS 18.4R1

March 2019—Junos OS 19.1R1

June 2019—Junos OS 19.2R1

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/documentation.

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 <https://support.juniper.net/support/eula/>. 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	J-Web Tasks	
Chapter 1	Dashboard	3
Chapter 2	Monitor	11
Chapter 3	Configure	175
Chapter 4	Reports	505
Chapter 5	Administration	513

Table of Contents

	About This Guide	xiii
	SRX Series Documentation and Release Notes	xiii
	Objectives	xiii
	Audience	xiv
	Document Conventions	xiv
	Documentation Feedback	xvi
	Requesting Technical Support	xvii
	Self-Help Online Tools and Resources	xvii
	Creating a Service Request with JTAC	xviii
Part 1	J-Web Tasks	
Chapter 1	Dashboard	3
	Monitoring the Dashboard	3
	Monitoring Hardware Components Using the Graphical Chassis Viewer	8
Chapter 2	Monitor	11
	Interfaces	11
	Monitoring Interfaces	11
	Multi Tenancy	13
	Monitoring Logical System	13
	Monitoring Multi Tenancy Tenants	17
	Access	20
	Monitoring Address Pools	20
	Alarms	21
	Monitoring Alarms	21
	Monitoring Security Events by Policy	22
	Events	24
	Monitoring All Events	25
	Monitoring Firewall Events	29
	Monitoring Web Filtering Events	33
	Monitoring IPSec VPN Events	36
	Monitoring Content Filtering Events	39
	Monitoring Antispam Events	42
	Monitoring Antivirus Events	45
	Monitoring IPS Events	48
	Monitoring Screen Events	51
	Monitoring Security Intelligence Events	53
	Monitoring ATP Events	55
	Monitoring System	56

Applications	59
Monitoring Applications	59
Users	62
Monitoring Users	62
System View	64
Monitoring Chassis Information	64
Monitoring Cluster Status	65
Monitoring Cluster Statistics	67
NAT	69
Monitoring Source NAT Information	69
Monitoring Destination NAT Information	75
Monitoring Static NAT Information	77
Monitoring Interface NAT Port Information	78
Monitoring NAT Incoming Table Information	79
Security	80
Policy	80
Monitoring Policies	80
Checking Policies	83
Screen Counters	86
Monitoring Screen Counters	86
UTM	89
Monitoring Antivirus	89
Monitoring Web Filtering	90
Monitoring Antispam	91
Monitoring Content Filtering	92
ICAP Redirect	93
Monitoring ICAP Redirect	93
IPS	94
Monitoring Attacks	94
Monitoring IDP Status	96
Flow Session	97
Monitoring Flow Session Statistics	97
Flow Gate	100
Monitoring Flow Gate Information	100
Authentication	101
Monitoring Firewall Authentication	101
Monitoring Local Authentication	103
Monitoring UAC Authentication	103
Voice ALGs	104
Monitoring Voice ALG Summary	104
Monitoring Voice ALG H.323	105
Monitoring Voice ALG MGCP	107
Monitoring Voice ALG SCCP	110
Monitoring Voice ALG SIP	113
Application Firewall	118
Monitoring Application Firewalls	118
Application Tracking	119
Monitoring Application Statistics (Application Tracking)	119

DS-Lite	122
Monitoring DS-Lite	122
AppQoS	123
Monitoring AppQoS	123
Threat Prevention	125
Monitoring Threat Prevention—Diagnostics	125
Monitoring Threat Prevention—Statistics	126
IPsec VPN	127
Monitoring IPsec VPN—Phase I	128
Monitoring IPsec VPN—Phase II	129
Ethernet Switching	130
Monitoring Ethernet Switching	130
Monitoring Spanning Tree	132
Monitoring IGMP Snooping	133
Monitoring GVRP	134
Routing	135
Monitoring Route Information	135
Monitoring RIP Routing Information	137
Monitoring OSPF Routing Information	139
Monitoring BGP Routing Information	141
Class of Service	143
Monitoring CoS Interfaces	143
Monitoring CoS Classifiers	144
Monitoring CoS Value Aliases	145
Monitoring CoS RED Drop Profiles	146
Monitoring CoS Forwarding Classes	147
Monitoring CoS Rewrite Rules	148
Monitoring CoS Scheduler Maps	149
MPLS	151
Monitoring MPLS Interfaces	151
Monitoring MPLS LSP Information	152
Monitoring MPLS LSP Statistics	153
Monitoring RSVP Session Information	155
Monitoring MPLS RSVP Interfaces Information	156
PPPoE	157
Monitoring PPPoE	157
DHCP	161
Monitoring DHCP Client Bindings	161
Monitoring DHCP Server	161
Monitoring DHCP Relay	163
Wireless LAN	165
Monitoring Access Points	165
VLAN	168
Monitoring VLAN	168
Threats Map (Live)	169
Monitor Threats Map (Live)	169
Field Descriptions	170
Threat Types	170
Tasks You Can Perform	171

Chapter 3	Configure	175
	Device Setup	175
	Basic Settings	175
	System Identity Configuration Page Options	175
	Date and Time Configuration Page Options	177
	Management Access Configuration Page Options	179
	Security Logging Configuration Page Options	185
	SNMP Configuration Page Options	187
	Configuring Cluster (HA) Setup	190
	Set Up	200
	PPPoE	201
	VPN Wizard	202
	NAT Wizard	202
	Interfaces	203
	Viewing Interfaces Configuration Page Options	203
	Interconnecting Interface Ports Configuration Page Options	207
	VLAN Configuration Page Options	210
	Link Aggregation Configuration Page Options	213
	Users	216
	User Management Configuration Page Options	216
	Access Profiles Configuration Page Options	221
	Firewall Authentication Configuration Page Options	226
	UAC Settings Configuration Page Options	228
	Network	230
	DHCP	230
	DHCP Client Configuration Page Options	231
	DHCP Services Configuration Page Options	232
	Routing Instances Configuration Page Options	238
	Static Routing Configuration Page Options	239
	RIP Configuration Page Options	241
	OSPF Configuration Page Options	246
	BGP Configuration Page Options	252
	Policies Configuration Page Options	258
	Class of Service	264
	Value Alias Configuration Page Options	264
	Forwarding Classes Configuration Page Options	266
	Classifiers Configuration Page Options	267
	Rewrite Rules Configuration Page Options	270
	Schedulers Configuration Page Options	272
	Scheduler Maps Configuration Page Options	274
	Drop Profile Configuration Page Options	275
	Virtual Channel Groups Configuration Page Options	276
	Assign To Interface Configuration Page Options	278
	Forwarding Mode	280
	Forwarding Configuration Page Options	280

Security	282
Security Policy	282
Configuring Firewall Security Policy Rules	282
Configuring Firewall Policy Schedules	299
NAT	301
Source NAT Configuration Page Options	301
Destination NAT Configuration Page Options	306
Static NAT Configuration Page Options	309
Proxy Configuration Page Options	311
Objects	313
Zones and Screens Configuration Page Options	313
Configuring Applications	322
Zone Address Book Configuration Page Options	325
Address Book Configuration Page Options	326
Proxy Profiles Configuration Page Options	328
Security Objects	330
Address Pools Configuration Page Options	330
Application Tracking Configuration Page Options	331
AppSecure	332
Application Signature Configuration Page Options	332
Application Firewall Configuration Page Options	334
UTM	336
Default Configuration Page Options	336
Antivirus Configuration Page Options	346
Web Filtering Configuration Page Options	353
Category Update Configuration Page Options	363
Antispam Configuration Page Options	364
Content Filtering Configuration Page Options	366
Custom Objects Configuration Page Options	368
UTM Policies Configuration Page Options	371
IPS	373
Signature Update Configuration Page Options	373
Sensor Configuration Page Options	375
IDP Policies Configuration Page Options	381
skyATP or Threat Prevention	386
Threat Prevention Policies Configuration Page Options	386
IPSec VPN	386
VPN Global Settings Configuration Page Options	387
IKE (Phase I) Configuration Page Options	389
IKE (Phase II) Configuration Page Options	397
VPN Manual Key Configuration Page Options	404
Dynamic VPN Global Settings Configuration Page Options	407
User Firewall	409
Configuring Active Directory	409
Authentication Priority Configuration Page Options	413
Local Authentication Configuration Page Options	414
Identity Management Configuration Page Options	415

	SSL Profiles	419
	Configuring SSL Initiation Profile	419
	Configuring SSL Proxy	423
	ALG	429
	ALG Configuration Page Options	429
	Firewall Filters	437
	IPv4 Firewall Filters Configuration Page Options	437
	IPv6 Firewall Filters Configuration Page Options	450
	Assign to Interfaces Configuration Page Options	461
	ICAP Redirect	462
	ICAP Redirect Profile Configuration Page Options	462
	DS-Lite	465
	DS-Lite Configuration Page Options	465
	Multi Tenancy	466
	Configuring Multi Tenancy Logical Systems	466
	Configuring Multi Tenancy Resource Profiles	476
	Configuring Multi Tenancy Tenants	481
	Chassis Cluster	489
	Chassis Cluster Configuration Page Options	489
	Chassis Cluster Setup Configuration Page Options	496
	CLI Tools	497
	CLI Viewer Configuration Page Options	497
	CLI Editor Configuration Page Options	498
	Point and Click Configuration Page Options	498
Chapter 4	Reports	505
	Reports	505
Chapter 5	Administration	513
	Devices	513
	Maintaining Files	513
	Maintaining Reboot Schedule	515
	Maintaining System Snapshots	517
	Software	519
	Maintaining Software Upload Packages	519
	Maintaining Software Install Packages	519
	Maintaining Software Downgrades	520
	Config Management	521
	Maintaining Configuration Management Upload Files	521
	Maintaining Configuration Management History	522
	Maintaining the Rescue Configuration	524
	License Management	524
	Maintaining Licenses	524
	Certificate Management	527
	Managing Certificates	528
	Managing Device Certificates	532
	Importing a Certificate	533
	Exporting a Certificate	534
	Viewing the Details of a Certificate	535
	Generating a Certificate	537

Deleting a Certificate	539
Search Text in Device Certificates Table	539
Managing Trusted Certificate Authority	540
Enrolling a Certificate Authority Certificate	541
Importing a Certificate Authority Certificate	542
Adding a Certificate Authority Profile	543
Editing a Certificate Authority Profile	545
Deleting a Certificate Authority Profile	546
Search Text in Trusted Certificate Authority Table	546
Managing Certificate Authority Group	547
Importing a Trusted Certificate Authority Group	548
Adding a Certificate Authority Group	548
Editing a Certificate Authority Group	549
Deleting a Certificate Authority Group	549
Search Text in Certificate Authority Group Table	549
Ping Host	550
Troubleshooting Ping Host	550
Ping MPLS	553
Troubleshooting Ping MPLS	553
Traceroute	557
Troubleshooting Traceroute	557
Network Monitoring	560
Alarm	560
Monitoring Chassis Alarm	560
Monitoring System Alarm	563
RPM	566
Troubleshooting RPM Setup	566
Troubleshooting RPM Information	571
Packet Capture	574
Troubleshooting Packet Capture	574
CLI Terminal	578
Understanding the J-Web CLI Terminal	578
CLI Terminal Requirements	579
CLI Overview	579
SKY ATP Enrollment	580
Sky ATP Enrollment	580

About This Guide

This preface provides the following guidelines for using the *Junos OS J-Web Help Reference*:

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

SRX Series Documentation and Release Notes

For a list of related SRX Series documentation, see <https://www.juniper.net/documentation/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 <https://www.juniper.net/documentation/>.

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 <https://www.juniper.net/books>.

Objectives

The *Junos OS J-Web Help Reference* describes how to use the J-Web interface to configure, monitor, and maintain Juniper Networks routing devices. It explains how to configure secure routing, monitor network operations, and perform routine maintenance and troubleshooting.

Juniper Networks SRX Series Services Gateways and J Series Services Routers run Junos OS. You can configure and manage Junos OS through either a command-line interface (CLI) or the J-Web interface. The J-Web interface must be accessed through a Web browser. The J-Web interface works with Microsoft Internet Explorer version 10 or 11, Mozilla Firefox version 44 or later, and Google Chrome version 55 or later. Other browser versions might not provide access to J-Web, and only English-version browsers are supported.



NOTE: If you are accessing J-Web through a HTTPS protocol, the browser must be enabled with TLS version 1.2 and SSL version 3.0 or later.

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

Document Conventions

Table 1 on page xv 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.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>

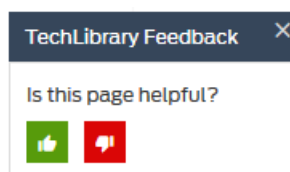
Table 2: Text and Syntax Conventions (continued)

Convention	Description	Examples
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none">To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level.The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric <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)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i>; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none">In the Logical Interfaces box, select All Interfaces.To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

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

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need 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 <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://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: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>

- Join and participate in the Juniper Networks Community Forum:
<https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net>

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

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://myjuniper.juniper.net>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

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

PART 1

J-Web Tasks

- [Dashboard on page 3](#)
- [Monitor on page 11](#)
- [Configure on page 175](#)
- [Reports on page 505](#)
- [Administration on page 513](#)

CHAPTER 1

Dashboard

- [Monitoring the Dashboard on page 3](#)
- [Monitoring Hardware Components Using the Graphical Chassis Viewer on page 8](#)

Monitoring the Dashboard

Purpose Use the monitoring functionality to view the Dashboard page. The J-Web dashboard provides a unified overview of the system and network status retrieved from SRX Series devices.

If you are using SRX300, SRX320, SRX320-poe, SRX340, SRX345, SRX550m, SRX1500, SRX4100, SRX4200, or any vSRX devices, the dashboard page is presented differently. Please see *J-Web Dashboard for SRX300, SRX320, SRX320-poe, SRX340, SRX345, SRX550m, SRX1500, SRX4100, SRX4200, or any vSRX devices*.

The Dashboard is the J-Web GUI framework on SRX Series devices, and it is based on panes. Each pane acts as a separate frame that can be viewed, dragged, minimized, maximized, or hidden. The panes include Chassis View, System Identification, Resource Utilization, Security Resources, System Alarms, File Usage, Login Sessions, Chassis Status, Storage Usage, and Threat Activity.



NOTE:

- The Threat Activity pane is not available on SRX5400, SRX5600, and SRX5800 devices.
 - For SRX Series devices configured for logical systems, the Logical System Identification and Logical System Profile panes are displayed when you log in as a user logical system administrator. These are the only logical system panes available in Dashboard Preferences.
 - Starting Junos OS Release 18.2R1-S1, J-Web supports display of SPC3 card in the dashboard and chassis viewer.
-

Action The Chassis View and several informational panes are displayed by default. To customize the page to include particular panes, click the **Open Preferences Dialog** icon at the top-right corner of the page to open Dashboard Preferences. From Dashboard Preferences,

you can also set the refresh time interval to update the data on the system properties automatically.

Meaning Table 3 on page 4 summarizes key output fields in the Dashboard page.

Starting in Junos OS 19.2R1, you can view the Web filtering, Antispam, Content filtering, Application & Users, and Threat monitoring widgets in the J-Web dashboard for root, logical systems, and tenant users.

Table 3: Dashboard Monitoring Page

Field	Description
Chassis View	<p>Provides a graphical representation of the hardware chassis.</p> <p>Displays the front or rear panel view of the device and shows which slots are occupied. When you insert or remove a card, the Chassis View reflects the change immediately.</p> <p>Changes color to indicate the port link status. For example, the ge port LED is green and steadily on when the port is up and red when the port is down.</p> <p>Displays Help tips when you hover the mouse over a port.</p>
System Identification	Provides system details such as serial number of the software, hostname, software version, BIOS version, system uptime, and system time.
System Alarms	Provides the received time, severity, description of the alarms and the action to be taken.
File Usage	Provides current space requirements for log, temporary, crash, and database files. Click Maintain to download or delete some or all of these files.
Login Sessions	Provides the user credentials, login time, idle time, and host.
Applications	Displays top 10 applications based on sessions or bandwidth.
Threats	Displays top 10 IPS sources, antispam sources, and antivirus name, sorted by count.
Security Resources	Provides the maximum, configured, and activated number of session, firewall/VPN policies, and IPsec VPNs.
Resource Utilization	Provides a graphical representation of the CPU, memory, and storage used for both the data and the control planes. The CPU control also shows the load average value for 1 minute when you mouse over CPU Control .
Firewall: Top Denies	Displays top requests denied by the firewall based on their source IP addresses, sorted by count.
Firewall Policy: Rules With No Hits	Displays firewall policies with the most rules not hit, sorted by count.
Firewall: Top Events	Displays all top 10 firewall events of the network traffic, sorted by count.
IDP: Top Events	Displays top 10 IDP events grouped by event-type, sorted by count.

Table 3: Dashboard Monitoring Page (continued)

Field	Description
Interface: Most Dropped Packets	Displays top 5 interfaces based on the CLI response; top-count will increase to 10.
Interface: Most Sessions	Displays top 10 interfaces with most sessions.
IP: Top Destinations	Displays top 10 destination-address, sorted by count or volume.
IP: Top Sources	Displays top 10 source-address of the network traffic, sorted by count or volume.
Virus: Top Blocked	Displays top 10 blocked viruses, sorted by count.
Zones: Top Bandwidth by Packets	Displays top 10 zones with maximum throughput rate in packets.
Web Filtering: Top Web Blocked	Displays top 5 Web blocked based on the CLI response.
Web Filtering: Top Source Address	Displays top 4 source address Web filter based on the CLI response.
Web Filtering: Top Destination Address	Displays top 4 destination address Web filter based on the CLI response.
Application & Users: High Risk Applications Blocked Per User	Displays top 4 high risk applications blocked per user based on the CLI response.
Application & Users: High Risk Applications Allowed Per User	Displays high risk applications allowed per user.
Content Filtering: Top Content Filters	Displays top 10 protocol, reason, and source address.
Chassis Status	Provides the component temperature and fan tray details of the system. Select View Chassis Status and then select View>Chassis for more information.
Web Filtering: Top Web Categories	Displays top 10 Web categories, security risk, productivity loss, legal-liability, and blocked.
Threat Monitoring	Displays top malware identified, threats, and infected categories.
Top Users of High Risk Applications by Volume/Count	Displays top users of high risk applications by volume.
Application & Users: Top Users	Displays top 4 users sorted by count and volume.

Table 3: Dashboard Monitoring Page (continued)

Field	Description
Application & Users: Top Categories	Displays top 4 categories of application and users sorted by count and volume.
Application & Users: Top IPs	Displays top 4 IP addresses of application and users sorted by count and volume.
Application & Users: Top High Risk Applications	Displays top 4 High Risk Applications sorted by risk, count and volume.
Application & Users: Users with the Most Critical Application Usage	Displays top 5 users with the most critical application usage volume.
Anti Spam: Top Source Address	Displays top 4 antispam group by source address and sorted by count.
Application & Users: Application Usage by Category/Type	Displays top 5 application usage by category group.
Threat Activity	Provides the most current threats received on the device.
Storage Usage	Displays used and available storage and usage information about other system components.
Signal Strength	Displays the signal strength of the device.
Logical System Identification	Provides the logical system name, the security profile assigned to the logical system, the software version, and the system time.
Logical System Profile	Displays the types of resources that are allocated to the user logical system, the number of resources used and reserved, and the maximum number of resources allowed.

**NOTE:**

- If the rescue configuration is not set, the set rescue configuration link directs you to the Maintain > Config management > Rescue page to set the rescue configuration.
- To use the Chassis View, a recent version of Adobe Flash that supports ActionScript and AJAX (Version 9) must be installed. Also note that the Chassis View is displayed by default on the Dashboard page. You can enable or disable it using options in the Dashboard Preference dialog box, but clearing cookies in Microsoft Internet Explorer also causes the Chassis View to be displayed.

J-Web Dashboard for SRX300, SRX320, SRX320-poe, SRX340, SRX345, SRX550m, SRX1500, SRX4100, SRX4200, or any vSRX devices

Use the J-Web dashboard page, to view a unified overview of the system and network status retrieved from SRX300, SRX320, SRX320-poe, SRX340, SRX345, SRX550m, SRX1500, SRX4100, SRX4200, or any vSRX devices.

To use the dashboard, select **Dashboard** at the top level menu.

By default, the dashboard Overview page displays the front view of the chassis along with System Identification, Resource Utilization, System Alarms, and Security Resource widgets.

You can refresh the display of the Overview dashboard page by clicking the refresh icon at the top right hand corner of the page.

You can toggle between the front view and rear view of the chassis by clicking **Show Rear View** or **Show Front View**. When you insert or remove a card, the Chassis View reflects the change immediately.

You can hover the mouse over a port to see its status. The ports are colored to indicate the port link status. For example, the ge port LED is green and steadily on when the port is up and red when the port is down.

Mouse over the top of each widget to minimize, refresh, and close by using the respective icons.

You can customize your dashboard as per your needs. You can add new widgets to the dashboard page.

To add a new widget to the Overview page:

1. Click the settings icon at the top right hand corner of the Overview page.

The *Dashboard Widget Preferences* popup window appears and lists the various widgets available.

2. Select the widgets that you want to be displayed in the dashboard Overview page.



NOTE: You can also select Chassis Status in the Dashboard Widget preferences window to view the chassis.

3. The **Auto Refresh Time** can be selected and the refresh rate can be set by choosing the time interval. The default auto refresh time is 10 minutes.

4. Click **OK** to view the selected widgets in the Overview page.

In certain widgets, the link *More Details>* is displayed at the lower left hand corner of the widget. If you click this link, you will be taken to that respective page in J-Web. For example, if you click *More Details>* link in the System Alarms widget, you will be taken to the Monitor > Alarms > View Alarms page in J-Web.

Release History Table

Release	Description
19.2R1	Starting in Junos OS 19.2R1, you can view the Web filtering, Antispam, Content filtering, Application & Users, and Threat monitoring widgets in the J-Web dashboard for root, logical systems, and tenant users.
18.2R1-S1	Starting Junos OS Release 18.2R1-S1, J-Web supports display of SPC3 card in the dashboard and chassis viewer.

Related Documentation

- [Monitoring Hardware Components Using the Graphical Chassis Viewer on page 8](#)

Monitoring Hardware Components Using the Graphical Chassis Viewer

Purpose Use the monitoring functionality to view the images of the chassis and access information about each component.

Action Select **Dashboard** and click **Chassis** in the upper right corner of the J-Web page.

A separate window opens with the image of the chassis and its component parts, including power supplies, individual PICs, and ports. The status of each port appears in red or green. Major or minor alarm indicators appear in red.

The chassis viewer is updated dynamically every 10 seconds.

- To view information about a component, mouse over the component in the chassis image.
- To go to the monitor or configuration page for a component, right-click the interface, and click **Monitor** or **Configure**. The monitor or configuration page opens in the main J-Web window.

If a PIC is not supported by the J-Web chassis viewer, an image of the PIC is not displayed. However, you can still right-click an interface to access its monitor or configuration page.



NOTE: The J-Web window might be behind the chassis viewer window.

- To move the image of the chassis, click the image inside the chassis viewer window.
- To zoom in or out, use the zoom option on the left side of the chassis viewer window.
- To toggle between front and rear views of the chassis, use the View Front and View Back buttons at the top of the chassis viewer window.

Meaning [Table 4 on page 9](#) summarizes the fields in the Chassis Viewer window.

Table 4: Chassis Viewer Monitoring Page

Field	Description
Chassis View	Displays the details of the routing engine, power and fan tray, and chassis components.
View Front	Displays the front view of the chassis.
View Rear	Displays the rear view of the chassis.

Related Documentation • [Monitoring the Dashboard on page 3](#)

CHAPTER 2

Monitor

- [Interfaces on page 11](#)
- [Multi Tenancy on page 13](#)
- [Access on page 20](#)
- [Alarms on page 21](#)
- [Events on page 24](#)
- [Applications on page 59](#)
- [Users on page 62](#)
- [System View on page 64](#)
- [NAT on page 69](#)
- [Security on page 80](#)
- [IPsec VPN on page 127](#)
- [Ethernet Switching on page 130](#)
- [Routing on page 135](#)
- [Class of Service on page 143](#)
- [MPLS on page 151](#)
- [PPPoE on page 157](#)
- [DHCP on page 161](#)
- [Wireless LAN on page 165](#)
- [VLAN on page 168](#)
- [Threats Map \(Live\) on page 169](#)

Interfaces

- [Monitoring Interfaces on page 11](#)

Monitoring Interfaces

Purpose View general information about all physical and logical interfaces for a device.

Action Enter the following **show** commands in the CLI to view interface status and traffic statistics.

- **show interfaces terse**



NOTE: On SRX Series devices, when configuring identical IPs on a single interface, you will not see a warning message; instead, you will see a syslog message.

- **show interfaces extensive**
- **show interfaces *interface-name***



NOTE: If you are using the J-Web user interfaces, select **Monitor>Interfaces** in the J-Web user interface. The J-Web Interfaces page displays the following details about each device interface:

- **Port**—Indicates the interface name.
- **Admin Status**—Indicates whether the interface is enabled (Up) or disabled (Down).
- **Link Status**—Indicates whether the interface is linked (Up) or not linked (Down).
- **Address**—Indicates the IP address of the interface.
- **Zone**—Indicates whether the zone is an untrust zone or a trust zone.
- **Services**—Indicates services that are enabled on the device, such as HTTP and SSH.
- **Protocols**—Indicates protocols that are enabled on the device, such as BGP and IGMP.
- **Input Rate graph**—Displays interface bandwidth utilization. Input rates are shown in bytes per second.
- **Output Rate graph**—Displays interface bandwidth utilization. Output rates are shown in bytes per second.
- **Error Counters chart**—Displays input and output error counters in the form of a bar chart.
- **Packet Counters chart**—Displays the number of broadcast, unicast, and multicast packet counters in the form of a pie chart. (Packet counter charts are supported only for interfaces that support MAC statistics.)

To change the interface display, use the following options:

- **Port for FPC**—Controls the member for which information is displayed.
- **Start/Stop button**—Starts or stops monitoring the selected interfaces.
- **Show Graph**—Displays input and output packet counters and error counters in the form of charts.

- Pop-up button—Displays the interface graphs in a separate pop-up window.
- Details—Displays extensive statistics about the selected interface, including its general status, traffic information, IP address, I/O errors, class-of-service data, and statistics.
- Refresh Interval—Indicates the duration of time after which you want the data on the page to be refreshed.
- Clear Statistics—Clears the statistics for the selected interface.

See Also • *Interfaces Feature Guide for Security Devices*

Multi Tenancy

- [Monitoring Logical System on page 13](#)
- [Monitoring Multi Tenancy Tenants on page 17](#)

Monitoring Logical System

Purpose Use the monitoring functionality to view the logical system page.

Action To monitor logical systems, select **Monitor>Logical System**.

Meaning [Table 5 on page 13](#) summarizes key output fields in the logical system page.



NOTE: All the information displayed in the format $n(m)$ means that n is the used number and m is the reserved number.

Table 5: Logical System Monitoring Page

Field	Value	Additional Information
Name	Displays the logical systems configured on the device.	—
Resource Profile	Displays the logical system profile assigned to each logical system.	—
Zone Usage	Displays the used and reserved number of zones that user logical system administrators and master logical system administrators have configured for their logical systems if the security profile is bound to the logical systems.	—

Table 5: Logical System Monitoring Page (continued)

Field	Value	Additional Information
Scheduler Usage	Displays the number of schedulers that user logical system administrators and master logical system administrators have configured for their logical systems if the security profile is bound to the logical systems.	—
Policy Count Usage	Displays the number of security policies with a count that user logical system administrators and master logical system administrators have configured for their logical systems if the security profile is bound to the logical systems.	—
Policy Without Count Usage	Displays the number of security policies without a count that user logical system administrators and master logical system administrators have configured for their logical systems if the security profile is bound to the logical systems.	—
Nat Static Rule Usage	Displays the number of NAT static rule configurations that user logical system administrators and master logical system administrators have configured for their logical systems if the security profile is bound to the logical systems.	—
Nat Source Rule Usage	Displays the NAT source rule configurations that user logical system administrators and master logical system administrators have configured for their logical systems if the security profile is bound to the logical systems.	—
Nat Source Pool Usage	Displays the NAT source pool configurations that logical system administrators and master logical system administrators have configured for their logical systems if the security profile is bound to the logical systems.	—
Nat Rule Referenced Prefix Usage	Displays the security NAT rule referenced IP prefix quota of a logical system.	—
Nat Port-OL IP Number Usage	Displays the number of NAT port overloading IP number configurations that user logical system administrators and master logical system administrators have configured for their logical systems if the security profile is bound to the logical systems.	—

Table 5: Logical System Monitoring Page (continued)

Field	Value	Additional Information
Nat Pat Portnum Usage	Displays the used quantity and the reserved quantity of ports for the logical system as part of the security profile.	–
Nat Pat Address Usage	Displays the number of NAT with port address translation (PAT) configurations that user logical system administrators and master logical system administrators have configured for their logical systems if the security profile is bound to the logical systems.	–
Nat No Pat Address Usage	Displays the number of NAT without port address translation configurations that user logical system administrators and master logical system administrators have configured for their logical systems if the security profile is bound to the logical systems.	–
Nat Interface Port-OI IP Usage	Displays the security NAT interface port overloading quota of a logical system.	–
Nat Destination Rule Usage	Displays the number of NAT destination rule configurations that user logical system administrators and master logical system administrators have configured for their logical systems if the security profile is bound to the logical systems.	–
Nat Destination Pool Usage	Displays the number of NAT destination pools that user logical system administrators and master logical system administrators have configured for their logical systems if the security profile is bound to the logical systems.	–
Nat Cone Binding Usage	Displays the number of NAT cone binding configurations that user logical system administrators and master logical system administrators have configured for their logical systems if the security profile is bound to the logical systems.	–
Flow Session Usage	Displays the number of flow sessions that user logical system administrators and master logical system administrators have configured for their logical systems if the security profile is bound to the logical systems.	–

Table 5: Logical System Monitoring Page (continued)

Field	Value	Additional Information
Flow Gate Usage	Displays the number of flow gates, also known as pinholes, that user logical system administrators and master logical system administrators have configured for their logical systems if the security profile is bound to the logical systems.	—
DsLite Softwire Initiator Usage	Displays the number of IPv6 dual-stack lite (DS-Lite) softwire initiators that can connect to the softwire concentrator configured in either a user logical system or the master logical system.	This statement is configured in the security profile that is bound to the logical system.
CPU on SPU Usage	Displays the CPU utilization and average utilization of all SPUs is shown.	The detail option shows CPU utilization on each SPU.
Auth Entry Usage	Displays the number of firewall authentication entries that user logical system administrators and master logical system administrators have configured for their logical systems if the security profile is bound to the logical systems.	—
Appfw Rule Set Usage	Displays the number of application firewall rule set configurations that a master administrator has configured for a master logical system or user logical system when the security profile is bound to the logical systems.	—
Appfw Rule Usage	Displays the number of application firewall rule configurations that a master administrator have configured for a master logical system or user logical system when the security profile is bound to the logical systems.	—
appfw-profile-count	Displays the application firewall profile quota of a logical system.	As a master administrator, you can create a security profile and specify the kinds and amounts of resources to allocate to a logical system to which the security profile is bound.
address-book-count	Displays the number of address books that user logical system administrators and master logical system administrators have configured for their logical systems if the security profile is bound to the logical systems.	—

Monitoring Multi Tenancy Tenants

Purpose Use the monitoring functionality to view the Tenants page.

- Action**
1. To monitor tenants, select **Monitor>Multi Tenancy>Tenants**.
 2. Click one:
 - **View Details**—Displays the grid view or graph view of all the resources for the tenant you have selected.
 - Search icon—Enables you to search for a tenant system in the grid.
 - Filter icon—Enables you to filter and display the list of tenants based on a column in the grid.
 - Show Hide Column icon—Enables you to show or hide a column in the grid.

Meaning Table 6 on page 17 summarizes key output fields in the tenants page.



NOTE: All the information displayed in the format $n(m)$ means that n is the used number and m is the reserved number.

Table 6: Tenants Monitoring Page

Field	Value	Additional Information
Name	Displays the tenants configured on the device.	—
Resource Profile	Displays the resource profile assigned to each tenant.	—
Zone Usage	Displays the used and reserved number of zones for the given tenant.	—
Scheduler Usage	Displays the number of schedulers that master administrators have configured for their tenants.	—
Policy Count Usage	Displays the number of security policies with a count master administrators have configured for their tenants if the security profile is bound to the tenants.	—
Policy Without Count Usage	Displays the number of security policies without a count that master administrators have configured for their tenants if the security profile is bound to the tenants.	—

Table 6: Tenants Monitoring Page (continued)

Field	Value	Additional Information
Nat Static Rule Usage	Displays the number of NAT static rule configurations that master administrators have configured for their tenants if the security profile is bound to the tenants.	—
Nat Source Rule Usage	Displays the NAT source rule configurations that master administrators have configured for their tenants if the security profile is bound to the tenants.	—
Nat Source Pool Usage	Displays the NAT source pool configurations that master administrators have configured for their tenants if the security profile is bound to the tenants.	—
Nat Rule Referenced Prefix Usage	Displays the security NAT rule referenced IP prefix quota of a tenant.	—
Nat Port-OI IP Number Usage	Displays the number of NAT port overloading IP number configurations that master administrators have configured for their tenants if the security profile is bound to the tenants.	—
Nat Pat Portnum Usage	Displays the used quantity and the reserved quantity of ports for the tenant as part of the security profile.	—
Nat Pat Address Usage	Displays the number of NAT with port address translation (PAT) configurations that master administrators have configured for their tenants if the security profile is bound to the tenants.	—
Nat No Pat Address Usage	Displays the number of NAT without port address translation configurations that master administrators have configured for their tenants if the security profile is bound to the tenants.	—
Nat Interface Port-OI IP Usage	Displays the security NAT interface port overloading quota of a tenant.	—
Nat Destination Rule Usage	Displays the number of NAT destination rule configurations that master administrators have configured for their tenants if the security profile is bound to the tenants.	—
Nat Destination Pool Usage	Displays the number of NAT destination pools that master administrators have configured for their tenants if the security profile is bound to the tenants.	—

Table 6: Tenants Monitoring Page (continued)

Field	Value	Additional Information
Nat Cone Binding Usage	Displays the number of NAT cone binding configurations that master administrators have configured for their tenants if the security profile is bound to the tenants.	—
Flow Session Usage	Displays the number of flow sessions that master administrators have configured for their tenants if the security profile is bound to the tenants.	—
Flow Gate Usage	Displays the number of flow gates, also known as pinholes, that master administrators have configured for their tenants if the security profile is bound to the tenants.	—
DSLite Softwire Initiator Usage	Displays the number of IPv6 dual-stack lite (DS-Lite) softwire initiators that can connect to the softwire concentrator configured in either a user tenant or the master tenant.	This statement is configured in the security profile that is bound to the tenant.
CPU on SPU Usage	Displays the CPU utilization and average utilization of all SPUs.	The detail option shows CPU utilization on each SPU.
Auth Entry Usage	Displays the number of firewall authentication entries that master administrators have configured for their tenants if the security profile is bound to the tenants.	—
Appfw Rule Set Usage	Displays the number of application firewall rule set configurations that a master administrator has configured for a tenant when the security profile is bound to the tenants.	—
Appfw Rule Usage	Displays the number of application firewall rule configurations that a master administrator have configured for a master tenant or user tenant when the security profile is bound to the tenants.	—
appfw-profile-count	Displays the application firewall profile quota of a tenant.	As a master administrator, you can create a security profile and specify the kinds and amounts of resources to allocate to a tenant to which the security profile is bound.
address-book-count	Displays the number of address books that master administrators have configured for their tenants if the security profile is bound to the tenants.	—

Access

- [Monitoring Address Pools on page 20](#)

Monitoring Address Pools

Purpose Use the monitoring functionality to view the Address Pools page.

Action To monitor Address Pools, select **Monitor>Access>Address Pools** in the J-Web user interface.

Meaning [Table 7 on page 20](#) summarizes key output fields in the Address Pools page.

Table 7: Address Pools Monitoring Page

Field	Values	Additional Information
Address Pool Properties		
Address Pool Name	Displays the name of the address pool.	-
Network Address	Displays the IP network address of the address pool.	-
Address Ranges	Displays the name, the lower limit, and the upper limit of the address range.	-
Primary DNS	Displays the primary-dns IP address.	-
Secondary DNS	Displays the secondary-dns IP address.	-
Primary WINS	Displays the primary-wins IP address.	-
Secondary WINS	Displays the secondary-wins IP address.	-
Address Pool Address Assignment		
IP Address	Displays the IP address of the address pool.	-
Hardware Address	Displays the hardware MAC address of the address pool.	-
Host/User	Displays the user name using the address pool.	-
Type	Displays the authentication type used by the address pool	The authentication types can be extended authentication (XAuth) or IKE Authentication.

- See Also**
- [Monitoring Interfaces on page 11](#)
 - *Threats Monitoring Report*

Alarms

- [Monitoring Alarms on page 21](#)
- [Monitoring Security Events by Policy on page 22](#)

Monitoring Alarms

Purpose Use the monitoring functionality to view the alarms page.

Action To monitor alarms, select one of the following in the J-Web user interface:

- If you are using SRX5400, SRX5600, or SRX5800 platforms, select **Monitor>Events and Alarms>View Alarms**.
- Select **Monitor>Alarms>View Alarms**.

Meaning [Table 8 on page 21](#) summarizes key output fields in the alarms page.

Table 8: Alarms Monitoring Page

Field	Value	Additional Information
Alarm Filter		
Alarm Type	Specifies the type of alarm to monitor: <ul style="list-style-type: none"> • System— System alarms include FRU detection alarms (power supplies removed, for instance). • Chassis— Chassis alarms indicate environmental alarms such as temperature. • All— Indicates to display all the types of alarms. 	—
Severity	Specifies the alarm severity that you want to monitor <ul style="list-style-type: none"> • Major— A major (red) alarm condition requires immediate action. • Minor— A minor (yellow) condition requires monitoring and maintenance. • All— Indicates to display all the severities. 	—
Description	Enter a brief synopsis of the alarms you want to monitor.	—

Table 8: Alarms Monitoring Page (continued)

Field	Value	Additional Information
Date From	Specifies the beginning of the date range that you want to monitor. Set the date using the calendar pick tool.	—
To	Specifies the end of the date range that you want to monitor. Set the date using the calendar pick tool.	—
Go	Executes the options that you specified.	—
Reset	Clears the options that you specified.	—
Alarm Details	Displays the following information about each alarm: <ul style="list-style-type: none"> • Type— Type of alarm: System, Chassis, or All. • Severity— Severity class of the alarm: Minor or Major. • Description— Description of the alarm. • Time— Time that the alarm was registered. 	—

- See Also**
- [Monitoring Active Alarms on a Device](#)
 - [Monitoring Events](#)
 - [Monitoring Security Events by Policy on page 22](#)

Monitoring Security Events by Policy

Purpose Monitor security events by policy and display logged event details with the J-Web user interface.

Action To monitor security events by policy:

1. Select one of the following in the J-Web user interface:
 - If you are using SRX5400, SRX5600, or SRX5800 platforms, select **Monitor>Events and Alarms>Security Events**.
 - Select **Monitor>Alarms>Policy Log**.

The View Policy Log pane appears. [Table 9 on page 23](#) describes the content of this pane.

Table 9: View Policy Log Fields

Field	Value
Log file name	Name of the event log files to search.
Policy name	Name of the policy of the events to be retrieved.
Source address	Source address of the traffic that triggered the event.
Destination address	Destination address of the traffic that triggered the event.
Event type	Type of event that was triggered by the traffic.
Application	Application of the traffic that triggered the event.
Source port	Source port of the traffic that triggered the event.
Destination port	Destination port of the traffic that triggered the event.
Source zone	Source zone of the traffic that triggered the event.
Destination zone	Destination zone of the traffic that triggered the event.
Source NAT rule	Source NAT rule of the traffic that triggered the event.
Destination NAT rule	Destination NAT rule of the traffic that triggered the event.
Is global policy	Specifies that the policy is a global policy.

If your device is not configured to store session log files locally, the Create log configuration button is displayed in the lower-right portion of the View Policy Log pane.

- To store session log files locally, click **Create log configuration**.

If session logs are being sent to an external log collector (stream mode has been configured for log files), a message appears indicating that event mode must be configured to view policy logs.



NOTE: Reverting to event mode will discontinue event logging to the external log collector.

- To reset the **mode** option to **event**, enter the **set security log** command.
2. Enter one or more search fields in the View Policy Log pane and click **Search** to display events matching your criteria.

For example, enter the event type **Session Close** and the policy **pol1** to display event details from all Session Close logs that contain the specified policy. To reduce search

results further, add more criteria about the particular event or group of events that you want displayed.

The Policy Events Detail pane displays information from each matching session log. [Table 10 on page 24](#) describes the contents of this pane.

Table 10: Policy Events Detail Fields

Field	Value
Timestamp	Time when the event occurred.
Policy name	Policy that triggered the event.
Record type	Type of event log providing the data.
Source IP/Port	Source address (and port, if applicable) of the event traffic.
Destination IP/Port	Destination address (and port, if applicable) of the event traffic.
Service name	Service name of the event traffic.
NAT source IP/Port	NAT source address (and port, if applicable) of the event traffic.
NAT destination IP/Port	NAT destination address (and port, if applicable) of the event traffic.

- See Also**
- [Monitoring Overview](#)
 - [Monitoring Interfaces on page 11](#)
 - [Monitoring Alarms on page 21](#)
 - [Monitoring Events](#)

Events

- [Monitoring All Events on page 25](#)
- [Monitoring Firewall Events on page 29](#)
- [Monitoring Web Filtering Events on page 33](#)
- [Monitoring IPSec VPN Events on page 36](#)
- [Monitoring Content Filtering Events on page 39](#)
- [Monitoring Antispam Events on page 42](#)
- [Monitoring Antivirus Events on page 45](#)
- [Monitoring IPS Events on page 48](#)
- [Monitoring Screen Events on page 51](#)
- [Monitoring Security Intelligence Events on page 53](#)

- [Monitoring ATP Events on page 55](#)
- [Monitoring System on page 56](#)

Monitoring All Events

Purpose The All Events page displays an overall, consolidated, high level view of your network environment. You can view all types of events that are being logged in your SRX platform. You can view abnormal events, attacks, viruses, spam attacks when log data is correlated and analyzed. This page provides you with an advanced filtering mechanism and visibility into actual events.



NOTE:

- For the events to be logged, registered, and displayed in the graph, the device should be in stream mode. You can configure stream mode in the **Configure > Device Setup > Basic Settings > Logging** page.
- Starting in Junos OS Release 19.1R1, All Events option is available for logical system users.

Action To monitor all events, select **Monitor>Events>All Events** in the J-Web user interface.

Meaning **Time Range** graph displays the trend of all events or flow for all the events that has transpired in the device.

You can specify the duration of time for which you want to view the trend for all events. The available options are **30m, 1h, 2h...** and so on, which are displayed at the top right hand side of the page. For example, if you choose **30m**, the end time is the current system time and the start time is the preceding 30 minutes from the current system time.

Click **Custom** to specify a customized time range. The Custom Time Range Selection popup window is presented. You can set the *from* and *to* date and time, and click **OK** to set the time range.

To refresh the graph on demand, click the refresh button.

You can also drag the slider in the Time Range graph from the extreme left or right of the graph and set the time range to see the trend or flow of events that has transpired in that time range.

[Table 11 on page 25](#) summarizes key output fields in the All Events page.

Table 11: Events Monitoring Page

Field	Value	Additional Information
-------	-------	------------------------

Chart View—Displays the trend analysis, displayed in the Time Range graph, in numbers.

Table 11: Events Monitoring Page (continued)

Field	Value	Additional Information
Total Events	Displays the total number of events that occurred in the specified time range.	-
Virus Instances	Displays the number of virus instances that occurred in the specified time range.	-
Attacks	Displays the number of IDP or IPS attacks that occurred in the specified time range.	-
Interface Down	Displays the total number of interfaces that are down.	-
Sessions	Displays the total number of firewall events or sessions that occurred during the time period specified in the Time Range graph.	-
Graphs Firewall Web Filtering IPSec VPNs Content Filtering Antispam Antivirus IPS	<p>The graphs display the trend analysis in swim lane chart for the time range that you specified in the Time Range graph.</p> <p>The legend in each graph shows the colors and its related interpretation.</p> <p>For example, in the Firewall graph, blue color represents all firewall events and black represents blocked firewall events. Similarly, in the IPS graph, orange, amber, and yellow represent critical, high, and medium IPS attacks respectively.</p>	Mouse over at any point in the swim lane chart to view further details at that point.
Grid View —Displays information in grids that are lazy loaded with infinite scrolling. You can narrow down your search to a particular event based on IP address, description, or attack name.		
Filters: The dropdown filters that are displayed above the grids. First dropdown filter	Options available in the first filter dropdown are: Firewall, Webfilter, ContentFilter, Antispam, Antivirus, Ipsecvpn, and IPS.	Select the event that you want to filter in the first dropdown filter.
Second dropdown filter	Options available in the second filter dropdown are: event-name, source-address, destination-address, application, user, service, policy, nested-application, source-interface, and source-zone.	Select the next criteria of the event on which you want to filter from the second dropdown filter.

Table 11: Events Monitoring Page (continued)

Field	Value	Additional Information
Text box	<p>Displays the filter parameter that you selected from the second filter dropdown.</p> <p>NOTE: In the filter statement the following limitation exists.</p> <ul style="list-style-type: none"> You can use only one operator at a time. You can use only one instance of the criteria or parameter in one filter statement. <p>For example, if you have used & operator and the parameter event-name once, I cannot use them again in the same filter statement</p> <p>CORRECT USAGE: event name = rt_flow_session_close & application=TELNET</p> <p>WRONG USAGE: event name=rt_flow_session_close & event-name = rt_flow_session_create</p> <p>WRONG USAGE: event name = rt_flow_session_close & source-address=x.x.x.x & application=TELNET</p> <p>NOTE: The filter statement is NOT case-sensitive.</p>	<p>Add the parameter for which you want to filter. For example, in the first dropdown if you selected Firewall as the event filter and in the second filter dropdown you selected event-name as the parameter, then the text box displays event-name = . If you add rt_flow_session_close to see only Firewall events then the text box displays event name = rt_flow_session_close.</p>
Go	Executes the filter statement that is displayed in the text box.	Click Go .
X	Clears the filters.	Click x .
Show Hide Column Filter icon represented by three vertical dots	Enables you to show or hide a column in the grid.	

[Table 12 on page 27](#) describes the grid elements that are displayed in the Detailed View.

Table 12: All Events - Grid Elements in Detailed View

Grid Element	Description
Threat Severity	The severity level of the threat.
Event Name	The event name of the log.
Description	The description of the log.
Attack Name	Attack name of the log: Trojan, worm, virus, and so on.

Table 12: All Events - Grid Elements in Detailed View (continued)

Grid Element	Description
UTM Category or Virus Name	The UTM category of the log.
Event Category	The event category of the log.
Source IP	The source IP address from where the event occurred.
Source Port	The source port of the event.
Destination IP	The destination IP address of the event.
Destination Port	The destination port of the event.
Application	The application name from which the events or logs are generated.
User Name	The username from whom the log is generated.
Hostname	The host name in the log.
Service Name	The name of the application service. For example, FTP, HTTP, SSH, and so on.
Protocol ID	The protocol ID in the log.
Policy Name	Policy name in the log.
SourceZone	User traffic received from the zone.
Destination Zone	The destination zone of the log.
Nested Application	The nested application in the log.
Roles	Role names associated with the event.
Reason	The reason for the log generation. For example, a connection tear down may have an associated reason such as authentication failed.
NAT Source Port	The translated source port.
NAT Destination Port	The translated destination port.
NAT Source Rule Name	The NAT source rule name.
NAT Destination Rule Name	The NAT destination rule name.
NAT Source IP	The translated (or natted) source IP address. It can contain IPv4 or IPv6 addresses.
NAT Destination IP	The translated (also called natted) destination IP address.

Table 12: All Events - Grid Elements in Detailed View (continued)

Grid Element	Description
Traffic Session ID	The traffic session ID of the log.
URL	Accessed URL name that triggered the event.
Object Name	The object name of the log.
Path Name	The path name of the log.
Logical System Name	The name of the logical system.
Rule Name	The rule name of the log.
Action	Action taken for the event: warning, allow, and block.
Time	The time when the log was received.

- See Also**
- [Monitoring Alarms on page 21](#)
 - [Monitoring Security Events by Policy on page 22](#)

Monitoring Firewall Events

Purpose Use the Firewall Events page to view information about security events based on firewall policies. Analyzing firewall logs yields useful security management information, such as attempts to breach your network and observing the inherent characteristics of your traffic in real time. Using the time-frame slider, you can quickly focus on the area of activity that you are most interested in. Once the time range is selected, all of the data presented in your view is refreshed automatically. You can also use the Custom button to set a custom time range.

Starting in Junos OS Release 19.1R1, Firewall Events option is available for logical system and tenant users.

Action To monitor firewall events select **Monitor>Events>Firewall** in the J-Web user interface.

There are two ways to view your data. You can select either the Summary View tab or the Detailed View tab.

Click **Summary View** for a brief summary of all the firewall events in your network.

The data presented in the line graph (also known as swim lanes) is refreshed automatically based on the selected time range. The line graph shows light blue lanes that represent all firewall events and dark blue lanes represent blocked firewall events.

Meaning **Time Range** graph displays the trend of all events or flow for all the events that has transpired in the device.

You can specify the duration of time for which you want to view the trend for all events. The available options are **30m**, **1h**, **2h**,..., and so on, which are displayed at the top right hand side of the page. For example, if you choose **30m**, the end time is the current system time and the start time is the preceding 30 minutes from the current system time.

Click **Custom** to specify a customized time range. The Custom Time Range Selection popup window is presented. You can set the *from* and *to* date and time, and click **OK** to set the time range.

To refresh the graph on demand, click the refresh button.

You can also drag the slider in the Time Range graph from the extreme left or right of the graph and set the time range to see the trend or flow of events that has transpired in that time range.

There are two ways to view your data. You can select either the Summary View tab or the Detailed View tab.

The **Summary View** is selected by default, and it gives a brief summary of all the firewall events in your network.

The data presented in the line graph (also known as swim lanes) is refreshed automatically based on the selected time range. The line graph shows light blue lanes that represent all events and dark blue lanes represent blocked events.

Below the swim lanes are widgets displaying critical information such as top five sources, top five destinations, and top five users.

See [Table 13 on page 30](#) for descriptions of the widgets.

Table 13: Widgets in Summary View

Widget Name	Displays
Top Sources	Top five source IP addresses of the network traffic; sorted by event count.
Top Destinations	Top five destination IP addresses of the network traffic; sorted by event count.
Top Users	Top five users of the network traffic; sorted by event count.

Click the **Detailed View** for comprehensive details of events in a grid format that includes sortable columns. It displays information in grids that are lazy loaded with infinite scrolling. You can narrow down your search to a particular event based on IP address, description, or attack name. The table includes information such as the rule that caused the event, severity for the event, event ID, traffic information, and how and when the event was detected.

Table 14: Filter Options in Detailed View

The dropdown filter that is displayed above the grids.	Options available in the filter dropdown are: Event-Name, Source-Address, Destination-Address, Application, Rule-name, Threat-Severity, and Attack-Name.	Select the criteria or parameter on which you want to construct the filter statement.
Text box	<p>Displays the filter parameter that you selected from the filter dropdown.</p> <p>NOTE: In the filter statement the following limitation exists.</p> <ul style="list-style-type: none"> You can use only one operator at a time. You can use only one instance of the criteria or parameter in one filter statement. <p>For example, if you have used & operator and the parameter event-name once, you cannot use them again in the same filter statement</p> <p>CORRECT USAGE: event name = rt_flow_session_close & application=TELNET</p> <p>WRONG USAGE:event name = rt_flow_session_close & event-name = rt_flow_session_create</p> <p>WRONG USAGE:event name = rt_flow_session_close & source-address = x.x.x.x & application = TELNET</p> <p>NOTE: The filter statement is NOT case-sensitive.</p>	Add the parameter for which you want to filter. For example, in the dropdown filter if you selected event-name as the parameter, the text box displays event-name = . If you add rt_flow_session_close to see only Firewall events then the text box displays event name = rt_flow_session_close .
Go	Executes the filter statement that is displayed in the text box.	Click Go .
X	Clears the filters.	Click x .
Show Hide Column Filter icon represented by three vertical dots	Enables you to show or hide a column in the grid.	

The [Table 15 on page 31](#) describes the grid information displayed in the Detailed View.

Table 15: Firewall Events - Grid Elements in Detailed View

Grid Element	Description
Event Name	The event name of the log.
Description	The description of the log.
Source IP	The source IP address from where the event occurred.

Table 15: Firewall Events - Grid Elements in Detailed View (continued)

Grid Element	Description
Source Port	The source port of the event.
Destination IP	The destination IP address of the event.
Destination Port	The destination port of the event.
Application	The application name from which the events or logs are generated. NOTE: Starting in Junos OS Release 19.2R1, you can see that an application displays the same value as a nested application (if the application supports nested application).
User Name	The username from whom the log is generated.
Hostname	The host name in the log.
Service Name	The name of the application service. For example, FTP, HTTP, SSH, and so on.
Protocol ID	The protocol ID in the log.
Policy Name	Policy name in the log.
SourceZone	User traffic received from the zone.
Destination Zone	The destination zone of the log.
Nested Application	The nested application in the log. NOTE: Starting in Junos OS Release 19.2R1, you can see that an application displays the same value as a nested application (if the application supports nested application).
Roles	Role names associated with the event.
NAT Source Port	The translated source port.
NAT Destination Port	The translated destination port.
NAT Source Rule Name	The NAT source rule name.
NAT Destination Rule Name	The NAT destination rule name.
NAT Source IP	The translated (or natted) source IP address. It can contain IPv4 or IPv6 addresses.
NAT Destination IP	The translated (also called natted) destination IP address.
Traffic Session ID	The traffic session ID of the log.

Table 15: Firewall Events - Grid Elements in Detailed View (continued)

Grid Element	Description
Rule Name	The rule name of the log.
Action	Action taken for the event: warning, allow, and block.
Time	The time when the log was received.

- See Also**
- [Monitoring Alarms on page 21](#)
 - [Monitoring Security Events by Policy on page 22](#)

Monitoring Web Filtering Events

Purpose Use this page to view information about security events based on Web filtering policies. Web filtering allows you to permit or block access to specific websites by URL or by URL category using cloud-based lookups, a local database, or an external Websense server. Analyzing Web filtering logs yields useful security management information such as users detected accessing restricted URLs and actions taken by the system. Using the time-frame slider, you can quickly focus on the area of activity that you are most interested in. Once the time range is selected, all of the data presented in your view is refreshed automatically. You can also use the Custom button to set a custom time range.

Starting in Junos OS Release 19.1R1, Web Filtering option is available for logical system users.

Action To monitor Web filtering events select **Monitor>Events>Web Filtering** in the J-Web user interface.

Meaning **Time Range** graph displays the trend of all events or flow for all the events that has transpired in the device.

You can specify the duration of time for which you want to view the trend for all events. The available options are **30m**, **1h**, **2h**,..., and so on, which are displayed at the top right hand side of the page. For example, if you choose 30m, the end time is the current system time and the start time is the preceding 30 minutes from the current system time.

Click **Custom** to specify a customized time range. The Custom Time Range Selection popup window is presented. You can set the *from* and *to* date and time, and click **OK** to set the time range.

To refresh the graph on demand, click the refresh button.

You can also drag the slider in the Time Range graph from the extreme left or right of the graph and set the time range to see the trend or flow of events that has transpired in that time range.

There are two ways to view your data. You can select either the Summary View tab or the Detailed View tab.

The **Summary View** is selected by default, and it gives a brief summary of all the Web filtering events in your network.

The data presented in the line graph (also known as swim lanes) is refreshed automatically based on the selected time range. The line graph shows light blue lanes that represent all Web filtering events and dark blue lanes represent blocked Web filtering events.

Below the swim lanes are widgets displaying critical information such as top URLs blocked, top matched profiles, top five sources, and top five destinations.

See [Table 16 on page 34](#) for descriptions of the widgets.

Table 16: Widgets in Summary View

Widget Name	Displays
Top URLs Blocked	Top URLs that are blocked.
Top Matched Profiles	Top matched profiles.
Top Sources	Top five source IP addresses of the network traffic; sorted by event count.
Top Destinations	Top five destination IP addresses of the network traffic; sorted by event count.

Click the **Detailed View** for comprehensive details of events in a grid format that includes sortable columns. It displays information in grids that are lazy loaded with infinite scrolling. You can narrow down your search to a particular event based on IP address, description, or event name. The table includes information such as the rule that caused the event, severity for the event, event ID, traffic information, and how and when the event was detected.

Table 17: Filter Options in Detailed View

The dropdown filter that is displayed above the grids.	Options available in the filter dropdown are: event-name, source-address, destination-address, application, user, service, policy, source-interface, source-zone.	Select the criteria or parameter on which you want to construct the filter statement.
--	---	---

Table 17: Filter Options in Detailed View (continued)

Text box	<p>Displays the filter parameter that you selected from the filter dropdown.</p> <p>NOTE: In the filter statement the following limitation exists.</p> <ul style="list-style-type: none"> You can use only one operator at a time. You can use only one instance of the criteria or parameter in one filter statement. <p>For example, if you have used & operator and the parameter Event-Name once, I cannot use them again in the same filter statement</p> <p>CORRECT USAGE: Event-Name = rt_flow_session_close & application=TELNET</p> <p>WRONG USAGE: Event-Name = rt_flow_session_close & Event-Name = rt_flow_session_create</p> <p>WRONG USAGE: Event-Name = rt_flow_session_close & source-address = x.x.x.x & application = TELNET</p> <p>NOTE: The filter statement is NOT case-sensitive.</p>	<p>Add the parameter for which you want to filter. For example, in the dropdown filter if you selected event-name as the parameter, the text box displays Event-Name =. If you add WEBFILTER_URL_BLOCKED to see only Web filtering events then the text box displays Event-Name = WEBFILTER_URL_BLOCKED.</p>
Go	Executes the filter statement that is displayed in the text box.	Click Go .
X	Clears the filters.	Click x .

The [Table 18 on page 35](#) describes the grid information displayed in the Detailed View.

Table 18: Web Filtering Events - Grid Elements in Detailed View

Grid Element	Description
Event Name	The event name of the log.
Description	The description of the log.
UTM Category or Virus Name	The UTM category or name of the virus.
Source IP	The source IP address from where the event occurred.
Source Port	The source port of the event.
Destination IP	The destination IP address of the event.
Destination Port	The destination port of the event.

Table 18: Web Filtering Events - Grid Elements in Detailed View (continued)

Grid Element	Description
Hostname	The host name in the log.
SourceZone	User traffic received from the zone.
Roles	Role names associated with the event.
Reason	The reason for the log generation. For example, a connection tear down may have an associated reason such as authentication failed.
URL	Accessed URL name that triggered the event.
Object Name	The object name of the log.
Path Name	The path name of the log.
Action	Action taken for the event: warning, allow, and block.
Profile Name	Profile name in the log.
Time	The time when the log was received.

- See Also**
- [Monitoring Alarms on page 21](#)
 - [Monitoring Security Events by Policy on page 22](#)

Monitoring IPSec VPN Events

Purpose Use this page to view information about security events based on IPSec VPN policies. This page provides a view of all IPsec VPN events.

Action To monitor events select **Monitor>Events>IPSec VPNs** in the J-Web user interface.

Meaning **Time Range** graph displays the trend of all events or flow for all the events that has transpired in the device.

You can specify the duration of time for which you want to view the trend for all events. The available options are **30m**, **1h**, **4h**,..., and so on, which are displayed at the top right hand side of the page. For example, if you choose 30m, the end time is the current system time and the start time is the preceding 30 minutes from the current system time.

Click **Custom** to specify a customized time range. The Custom Time Range Selection popup window is presented. You can set the *from* and *to* date and time, and click **OK** to set the time range.

To refresh the graph on demand, click the refresh button.

You can also drag the slider in the Time Range graph from the extreme left or right of the graph and set the time range to see the trend or flow of events that has transpired in that time range.

There are two ways to view your data. You can select either the Summary View tab or the Detailed View tab.

The **Summary View** is selected by default, and it gives a brief summary of all the IPSec VPN events in your network.

The data presented in the line graph (also known as swim lanes) is refreshed automatically based on the selected time range. The line graph shows light blue lanes that represent all IPSec VPN events and dark blue lanes represent blocked IPSec VPN events.

Click the **Detailed View** for comprehensive details of events in a grid format that includes sortable columns. It displays information in grids that are lazy loaded with infinite scrolling. You can narrow down your search to a particular event based on IP address, description, or attack name. The table includes information such as the rule that caused the event, severity for the event, event ID, traffic information, and how and when the event was detected.

Table 19: Filter Options in Detailed View

The dropdown filter that is displayed above the grids.	Options available in the filter dropdown is: Event-Name.	Select Event-Name.
--	---	--------------------

Table 19: Filter Options in Detailed View (continued)

Text box	<p>Displays the filter parameter that you selected from the filter dropdown.</p> <p>NOTE: In the filter statement the following limitation exists.</p> <ul style="list-style-type: none"> You can use only one operator at a time. You can use only one instance of the criteria or parameter in one filter statement. <p>For example, if you have used & operator and the parameter Event-Name once, I cannot use them again in the same filter statement</p> <p>CORRECT USAGE: Event-Name = rt_flow_session_close & application=TELNET</p> <p>WRONG USAGE: Event-Name = rt_flow_session_close & Event-Name = rt_flow_session_create</p> <p>WRONG USAGE: Event-Name = rt_flow_session_close & source-address = x.x.x.x & application = TELNET</p> <p>NOTE: The filter statement is NOT case-sensitive.</p>	<p>Add the parameter for which you want to filter. For example, in the dropdown filter if you selected event-name as the parameter, the text box displays Event-Name =. If you add RT_IPSEC_BAD_SPI_RT_IPSEC_RELAY, RT_IPSEC_PV_RELAY to see only IPSec VPN events then the text box displays Event-Name = RT_IPSEC_BAD_SPI_RT_IPSEC_RELAY, RT_IPSEC_PV_RELAY.</p>
Go	Executes the filter statement that is displayed in the text box.	Click Go .
X	Clears the filters.	Click x .

The [Table 20 on page 38](#) describes the grid information displayed in the Detailed View.

Table 20: IPSec VPN Events - Grid Elements in Detailed View

Grid Element	Description
Event Name	The event name of the log.
Description	The description of the log.
Destination Port	The destination port of the event.
Hostname	The host name in the log.
Rule Name	The rule name of the log.
Time	The time when the log was received.

- See Also**
- [Monitoring Alarms on page 21](#)
 - [Monitoring Security Events by Policy on page 22](#)

Monitoring Content Filtering Events

Purpose Use this page to view information about security events based on content filtering policies. The event viewer provides a view of all content filtering events and how the events are handled by content filter. This page can be used to view traffic on the network in real time or as a debugging tool to view how content filtering is operating.

Content filtering provides basic data loss prevention functionality. Content filtering screens traffic based on MIME type, file extension, protocol commands, and embedded object type. It either permits or blocks specific commands or extensions on a protocol-by-protocol basis.

Starting in Junos OS Release 19.1R1, Content Filtering option is available for logical system users.

Action To monitor events select **Monitor>Events>Content Filtering** in the J-Web user interface.

Meaning **Time Range** graph displays the trend of all events or flow for all the events that has transpired in the device.

You can specify the duration of time for which you want to view the trend for all events. The available options are **30m, 1h, 2h,...**, and so on, which are displayed at the top right hand side of the page. For example, if you choose 30m, the end time is the current system time and the start time is the preceding 30 minutes from the current system time.

Click **Custom** to specify a customized time range. The Custom Time Range Selection popup window is presented. You can set the *from* and *to* date and time, and click **OK** to set the time range.

To refresh the graph on demand, click the refresh button.

You can also drag the slider in the Time Range graph from the extreme left or right of the graph and set the time range to see the trend or flow of events that has transpired in that time range.

There are two ways to view your data. You can select either the Summary View tab or the Detailed View tab.

The **Summary View** is selected by default, and it gives a brief summary of all the Content Filtering events in your network.

The data presented in the line graph (also known as swim lanes) is refreshed automatically based on the selected time range. The line graph shows light blue lanes that represent all Content Filtering events.

Below the swim lanes are widgets displaying critical information such as top five sources, top reasons, and top blocked protocol commands.

See [Table 21 on page 40](#) for descriptions of the widgets.

Table 21: Widgets in Summary View

Widget Name	Displays
Top Sources	Top five source IP addresses of the network traffic; sorted by event count.
Top Reasons	Adds respective content for display column.
Top Blocked Protocol Commands	Adds respective content for display column.

Click the **Detailed View** for comprehensive details of events in a grid format that includes sortable columns. It displays information in grids that are lazy loaded with infinite scrolling. You can narrow down your search to a particular event based on Event-Name, Source-Address, Reason, or Profile. The table includes information such as event name, description, source IP, reason, profile, and how and when the event was detected.

Table 22: Filter Options in Detailed View

The dropdown filter that is displayed above the grids.	Options available in the filter dropdown are: event-name, source-address, destination-address, Source-Name, User, Role, Reason, Profile, Protocol, and Category for dropdown filter.	Select the criteria or parameter on which you want to construct the filter statement.
--	--	---

Table 22: Filter Options in Detailed View (continued)

Text box	<p>Displays the filter parameter that you selected from the filter dropdown.</p> <p>NOTE: In the filter statement the following limitation exists.</p> <ul style="list-style-type: none"> You can use only one operator at a time. You can use only one instance of the criteria or parameter in one filter statement. <p>For example, if you have used & operator and the parameter Event-Name once, I cannot use them again in the same filter statement</p> <p>CORRECT USAGE: Event-Name = rt_flow_session_close & application=TELNET</p> <p>WRONG USAGE: Event-Name = rt_flow_session_close & Event-Name = rt_flow_session_create</p> <p>WRONG USAGE: Event-Name = rt_flow_session_close & source-address = x.x.x.x & application = TELNET</p> <p>NOTE: The filter statement is NOT case-sensitive.</p>	<p>Add the parameter for which you want to filter. For example, in the dropdown filter if you selected event-name as the parameter, the text box displays Event-Name =. If you add CONTENT-FILTERING-BLOCKED-MT to see only Content Filtering events then the text box displays Event Name = CONTENT-FILTERING-BLOCKED-MT.</p>
Go	Executes the filter statement that is displayed in the text box.	Click Go .
X	Clears the filters.	Click x .
Show Hide Column Filter icon represented by three vertical dots	Enables you to show or hide a column in the grid.	

The [Table 23 on page 41](#) describes the grid information displayed in the Detailed View.

Table 23: Content Filtering Events - Grid Elements in Detailed View

Grid Element	Description
Event Name	The event name of the log.
Description	The description of the log.
UTM Category or Virus Name	The UTM category or name of the virus.
Event category	The event category of the log.
Source IP	The source IP address from where the event occurred.
Hostname	The host name in the log.

Table 23: Content Filtering Events - Grid Elements in Detailed View (continued)

Grid Element	Description
SourceZone	User traffic received from the zone.
Roles	Role names associated with the event.
Reason	The reason for the log generation. For example, a connection tear down may have an associated reason such as authentication failed.
URL	Accessed URL name that triggered the event.
Action	Action taken for the event: warning, allow, and block.
Profile Name	Profile name in the log.
Time	The time when the log was received.

- See Also**
- [Monitoring Alarms on page 21](#)
 - [Monitoring Security Events by Policy on page 22](#)

Monitoring Antispam Events

Purpose Use this page to view information about security events based on antispam policies. The event viewer provides a view of all antispam events and the action taken by the antispam scanner.

The antispam scanner inspects and block spam by scanning inbound and outbound SMTP e-mail traffic. The filtering can be server-based using an external spam block list server or local-based using local lists (blacklists and whitelists) for matching.

Starting in Junos OS Release 19.1R1, Antispam option is available for logical system users.

Action To monitor events select **Monitor>Events>Antispam** in the J-Web user interface.

Meaning **Time Range** graph displays the trend of all events or flow for all the events that has transpired in the device.

You can specify the duration of time for which you want to view the trend for all events. The available options are **30m**, **1h**, **2h**,..., and so on, which are displayed at the top right hand side of the page. For example, if you choose 30m, the end time is the current system time and the start time is the preceding 30 minutes from the current system time.

Click **Custom** to specify a customized time range. The Custom Time Range Selection popup window is presented. You can set the *from* and *to* date and time, and click **OK** to set the time range.

To refresh the graph on demand, click the refresh button.

You can also drag the slider in the Time Range graph from the extreme left or right of the graph and set the time range to see the trend or flow of events that has transpired in that time range.

There are two ways to view your data. You can select either the Summary View tab or the Detailed View tab.

The **Summary View** is selected by default, and it gives a brief summary of all the antis spam events in your network.

The data presented in the line graph (also known as swim lanes) is refreshed automatically based on the selected time range. The line graph shows light blue lanes that represent all antis spam events.

Below the swim lanes is a widget displaying top five sources.

See [Table 24 on page 43](#) for descriptions of the widgets.

Table 24: Widgets in Summary View

Widget Name	Displays
Top Sources	Top five source IP addresses of the network traffic; sorted by event count.

Click the **Detailed View** for comprehensive details of events in a grid format that includes sortable columns. It displays information in grids that are lazy loaded with infinite scrolling. You can narrow down your search to a particular event based on IP address, or description. The table includes information such as the rule that caused the event and how and when the event was detected.

Table 25: Filter Options in Detailed View

The dropdown filter that is displayed above the grids.	Options available in the filter dropdown are: Event-Name, Source-Address, Destination-Address, Source-Name, User, Role, Reason, Profile, Protocol, and Category.	Select the criteria or parameter on which you want to construct the filter statement.
--	---	---

Table 25: Filter Options in Detailed View (continued)

Text box	<p>Displays the filter parameter that you selected from the filter dropdown.</p> <p>NOTE: In the filter statement the following limitation exists.</p> <ul style="list-style-type: none"> You can use only one operator at a time. You can use only one instance of the criteria or parameter in one filter statement. <p>For example, if you have used & operator and the parameter event-name once, I cannot use them again in the same filter statement</p> <p>CORRECT USAGE: event name = rt_flow_session_close & application=TELNET</p> <p>WRONG USAGE:event name = rt_flow_session_close & event-name = rt_flow_session_create</p> <p>WRONG USAGE:event name = rt_flow_session_close & source-address = x.x.x.x & application = TELNET</p> <p>NOTE: The filter statement is NOT case-sensitive.</p>	<p>Add the parameter for which you want to filter. For example, in the dropdown filter if you selected event-name as the parameter, the text box displays event-name =. If you add ANTISPAM_SPAM_DETECTED_MTA to see only antispam events then the text box displays event name = ANTISPAM_SPAM_DETECTED_MTA.</p>
Go	Executes the filter statement that is displayed in the text box.	Click Go .
X	Clears the filters.	Click x .
Show Hide Column Filter icon represented by three vertical dots	Enables you to show or hide a column in the grid.	

The [Table 26 on page 44](#) describes the grid information displayed in the Detailed View.

Table 26: Antispam Events - Grid Elements in Detailed View

Grid Element	Description
Event Name	The event name of the log.
Description	The description of the log.
UTM Category or Virus Name	
Source IP	The source IP address from where the event occurred.
Hostname	The host name in the log.
SourceZone	User traffic received from the zone.

Table 26: Antispam Events - Grid Elements in Detailed View (continued)

Grid Element	Description
Roles	Role names associated with the event.
Reason	The reason for the log generation. For example, a connection tear down may have an associated reason such as authentication failed.
URL	Accessed URL name that triggered the event.
Action	Action taken for the event: warning, allow, and block.
Profile Name	Profile name in the log.
Time	The time when the log was received.

- See Also**
- [Monitoring Alarms on page 21](#)
 - [Monitoring Security Events by Policy on page 22](#)

Monitoring Antivirus Events

Purpose Use this page to view information about security events based on antivirus policies. The event viewer provides a view of all antivirus events and the action taken by the virus scanner.

The antivirus scanner inspects files transmitted over several protocols to determine if the files exchanged are malicious (for example, viruses, Trojans, rootkits, and worms).

Starting in Junos OS Release 19.1R1, Antivirus option is available for logical system users.

Action To monitor events select **Monitor>Events>Antivirus** in the J-Web user interface.

Meaning **Time Range** graph displays the trend of all events or flow for all the events that has transpired in the device.

You can specify the duration of time for which you want to view the trend for all events. The available options are **30m**, **1h**, **2h**,..., and so on, which are displayed at the top right hand side of the page. For example, if you choose 30m, the end time is the current system time and the start time is the preceding 30 minutes from the current system time.

Click **Custom** to specify a customized time range. The Custom Time Range Selection popup window is presented. You can set the *from* and *to* date and time, and click **OK** to set the time range.

To refresh the graph on demand, click the refresh button.

You can also drag the slider in the Time Range graph from the extreme left or right of the graph and set the time range to see the trend or flow of events that has transpired in that time range.

There are two ways to view your data. You can select either the Summary View tab or the Detailed View tab.

The **Summary View** is selected by default, and it gives a brief summary of all the antivirus events in your network.

The data presented in the line graph (also known as swim lanes) is refreshed automatically based on the selected time range. The line graph shows light blue lanes that represent all antivirus events.

Below the swim lanes are widgets displaying critical information such as top five sources and top five destinations.

See [Table 27 on page 46](#) for descriptions of the widgets.

Table 27: Widgets in Summary View

Widget Name	Displays
Top Sources	Top five source IP addresses of the network traffic; sorted by event count.
Top Destinations	Top five destination IP addresses of the network traffic; sorted by event count.

Click the **Detailed View** for comprehensive details of events in a grid format that includes sortable columns. It displays information in grids that are lazy loaded with infinite scrolling. You can narrow down your search to a particular event based on Event-Name, Source-Address, or Destination-Address. The table includes information such as the rule that caused the event, severity for the event, event ID, traffic information, and how and when the event was detected.

Table 28: Filter Options in Detailed View

The dropdown filter that is displayed above the grids.	Options available in the filter dropdown are: Event-Name, Source-Address, Destination-Address, Source-Name, User, Role, Reason, Profile, Protocol, and Category.	Select the criteria or parameter on which you want to construct the filter statement.
--	---	---

Table 28: Filter Options in Detailed View (continued)

Text box	<p>Displays the filter parameter that you selected from the filter dropdown.</p> <p>NOTE: In the filter statement the following limitation exists.</p> <ul style="list-style-type: none"> You can use only one operator at a time. You can use only one instance of the criteria or parameter in one filter statement. <p>For example, if you have used & operator and the parameter Event-Name once, I cannot use them again in the same filter statement</p> <p>CORRECT USAGE: Event-Name = rt_flow_session_close & application=TELNET</p> <p>WRONG USAGE: event name = rt_flow_session_close & event-name = rt_flow_session_create</p> <p>WRONG USAGE: event name = rt_flow_session_close & source-address = x.x.x.x & application = TELNET</p> <p>NOTE: The filter statement is NOT case-sensitive.</p>	<p>Add the parameter for which you want to filter. For example, in the dropdown filter if you selected event-name as the parameter, the text box displays Event-Name =. If you add AV_VIRUS_DETECTED_MT to see only antivirus events then the text box displays Event-Name = AV_VIRUS_DETECTED_MT.</p>
Go	Executes the filter statement that is displayed in the text box.	Click Go .
X	Clears the filters.	Click x .
Show Hide Column Filter icon represented by three vertical dots	Enables you to show or hide a column in the grid.	-

The [Table 29 on page 47](#) describes the grid information displayed in the Detailed View.

Table 29: antivirus Events - Grid Elements in Detailed View

Grid Element	Description
Event Name	The event name of the log.
Description	The description of the log.
UTM Category or Virus Name	The UTM category of the log.
Source IP	The source IP address from where the event occurred.
Hostname	The host name in the log.
SourceZone	User traffic received from the zone.

Table 29: antivirus Events - Grid Elements in Detailed View (continued)

Grid Element	Description
Roles	Role names associated with the event.
Reason	The reason for the log generation. For example, a connection tear down may have an associated reason such as authentication failed.
URL	Accessed URL name that triggered the event.
Action	Action taken for the event: warning, allow, and block.
Profile Name	The profile name of the log.
Time	The time when the log was received.

- See Also**
- [Monitoring Alarms on page 21](#)
 - [Monitoring Security Events by Policy on page 22](#)

Monitoring IPS Events

Purpose Use the IPS Events page to view information about security events based on IPS policies and criticality of the IDP events. Analyzing IPS logs yields useful security management information, such as abnormal events or attacks.

Starting in Junos OS Release 19.1R1, IPS Events option is available for logical system users.

Action To monitor events select **Monitor>Events>IPS** in the J-Web user interface.

Meaning **Time Range** graph displays the trend of all events or flow for all the events that has transpired in the device.

You can specify the duration of time for which you want to view the trend for all events. The available options are **30m**, **1h**, **2h**,..., and so on, which are displayed at the top right hand side of the page. For example, if you choose 30m, the end time is the current system time and the start time is the preceding 30 minutes from the current system time.

Click **Custom** to specify a customized time range. The Custom Time Range Selection popup window is presented. You can set the *from* and *to* date and time, and click **OK** to set the time range.

To refresh the graph on demand, click the refresh button.

You can also drag the slider in the Time Range graph from the extreme left or right of the graph and set the time range to see the trend or flow of events that has transpired in that time range.

There are two ways to view your data. You can select either the Summary View tab or the Detailed View tab.

The **Summary View** is selected by default, and it gives a brief summary of all the IPS events in your network.

The data presented in the line graph (also known as swim lanes) is refreshed automatically based on the selected time range. The line graph shows dark red, red, and yellow lanes that represent critical, high, and medium IDP events based on the criticality of events.

Below the swim lanes are widgets displaying critical information such as top five sources, top five destinations, top IPS attacks, and top IPS severities.

See [Table 30 on page 49](#) for descriptions of the widgets.

Table 30: Widgets in Summary View

Widget Name	Displays
Top Sources	Top five source IP addresses of the network traffic; sorted by event count.
Top Destinations	Top five destination IP addresses of the network traffic; sorted by event count.
Top IPS Attacks	Top five IPS attacks; sorted by event count.
IPS Severities	Donught chart which shows the percentage of IPS events based on their severity levels. The colors are blue, black, green, and amber representing high, info, critical, and medium IPS events respectively.

Click the **Detailed View** for comprehensive details of events in a grid format that includes sortable columns. It displays information in grids that are lazy loaded with infinite scrolling. You can narrow down your search to a particular event based on IP address or attack name. The table includes information such as the rule that caused the event, severity for the event, event ID, traffic information, and how and when the event was detected.

Table 31: Filter Options in Detailed View

The dropdown filter that is displayed above the grids.	Options available in the filter dropdown are: Event-Name, Source-Address, Destination-Address, Application, User, Service, Policy, Nested-Application, Source-Interface, and Source-Zone.	Select the criteria or parameter on which you want to construct the filter statement.
--	--	---

Table 31: Filter Options in Detailed View (continued)

Text box	<p>Displays the filter parameter that you selected from the filter dropdown.</p> <p>NOTE: In the filter statement the following limitation exists.</p> <ul style="list-style-type: none"> You can use only one operator at a time. You can use only one instance of the criteria or parameter in one filter statement. <p>For example, if you have used & operator and the parameter Event-Name once, I cannot use them again in the same filter statement</p> <p>CORRECT USAGE: Event-Name = rt_flow_session_close & application=TELNET</p> <p>WRONG USAGE: Event-Name = rt_flow_session_close & Event-Name = rt_flow_session_create</p> <p>WRONG USAGE: Event-Name = rt_flow_session_close & source-address = x.x.x.x & application = TELNET</p> <p>NOTE: The filter statement is NOT case-sensitive.</p>	<p>Add the parameter for which you want to filter. For example, in the dropdown filter if you selected event-name as the parameter, the text box displays Event-Name =. If you add IDP_ATTACK_LOG_EVENT to see only IPS events then the text box displays Event-Name = IDP_ATTACK_LOG_EVENT.</p>
Go	Executes the filter statement that is displayed in the text box.	Click Go .
X	Clears the filters.	Click x .

The [Table 32 on page 50](#) describes the grid information displayed in the Detailed View.

Table 32: IPS Events - Grid Elements in Detailed View

Grid Element	Description
Threat Severity	The severity level of the threat.
Event Name	The event name of the log.
Description	The description of the log.
Attack Name	Attack name of the log: Trojan, worm, virus, and so on.
Source IP	The source IP address from where the event occurred.
Source Port	The source port of the event.
Destination IP	The destination IP address of the event.

Table 32: IPS Events - Grid Elements in Detailed View (continued)

Grid Element	Description
Destination Port	The destination port of the event.
Application	The application name from which the events or logs are generated.
Hostname	The host name in the log.
Service Name	The name of the application service. For example, FTP, HTTP, SSH, and so on.
Protocol ID	The protocol ID in the log.
Policy Name	Policy name in the log.
SourceZone	User traffic received from the zone.
Destination Zone	The destination zone of the log.
Nested Application	The nested application in the log.
NAT Source Port	The translated source port.
NAT Destination Port	The translated destination port.
Rule Name	The rule name of the log.
Action	Action taken for the event: warning, allow, and block.
Time	The time when the log was received.

- See Also**
- [Monitoring Alarms on page 21](#)
 - [Monitoring Security Events by Policy on page 22](#)

Monitoring Screen Events

Purpose Starting in Junos OS Release 19.2R1, you can monitor the screen events.

Use screen events to view the information about security events based on screen profiles. Analyzing screen logs yields information such as attack name, action taken, source of an attack, and destination of an attack.

Action To monitor screen events, select **Monitor > Events > Screen** in the J-Web user interface.

Meaning Using the time-range slider, you can quickly focus on the time and area of activity that you are most interested in. Once the time range is selected, all of the data presented in your view is refreshed automatically. You can also use the Custom button to set a custom time range.

You can select either the Grid View tab or the Chart View tab to view your data:

- **Grid View**—View the comprehensive details of all screen events in a tabular format that includes sortable columns. You can group the events using the Group By option. For example, you can group the events based on source country. The table includes information such as the event name, source country, source address, destination country, attack name, and so on. [Table 33 on page 52](#) describes the fields on the Grid View page.
- **Chart View**—View a brief summary of all the screen events in your network. The top of the page has a swim lane graph of all the screen events. You can use the widgets at the bottom of the page to view critical information such as, top screen attackers, top screen victims, and top screen hits. [Table 34 on page 53](#) describes the widgets on the Chart View page.

Table 33: Screen—Fields on the Grid View Page

Field	Description
Timestamp	The time when the log was received.
Event Name	Name of the event in the log.
Source Country	Country from which the traffic that triggered the event originated.
Source Address	Source IP address for the traffic that triggered the event (IPv4 or IPv6).
Destination Country	Country to which the traffic that triggered the event was sent
Attack Name	Name of the attack in the log for threat event. For example, trojan, worm, virus, and so on.
Destination Address	Destination IP address for the traffic that triggered the event (IPv4 or IPv6).
Source Port	Source TCP/UDP port number of the traffic that triggered the event.
Destination Port	Destination TCP/UDP port number of the traffic that triggered the event.
Description	Brief description of the event.
Action	Action taken for the event. For example, warning, allow, and block.
Host Name	Hostname of the device where the log was generated.
Source Zone Name	Name of the source security zone of the traffic that triggered the event.
Interface Name	Name of the interface.

Table 33: Screen—Fields on the Grid View Page (continued)

Field	Description
Domain	Displays the network or subnetwork to which the device belongs.

Table 34: Screen—Widgets on the Chart View Page

Field	Description
Top Screen Attackers	Top source countries from where the event source originated; sorted by the number of source IP addresses.
Top Screen Victims	Top destination countries targeted for the attack; sorted by the number of destination IP addresses.
Top Screen Hits	Top source IP addresses of the network traffic; sorted by the number of event occurrences.

- See Also**
- [Monitoring IPS Events on page 48](#)
 - [Monitoring Security Intelligence Events on page 53](#)
 - [Monitoring ATP Events on page 55](#)

Monitoring Security Intelligence Events

Purpose Starting in Junos OS Release 19.2R1, you can monitor the security intelligence events. Use the monitoring functionality to view the Security Intelligence page.

Action To monitor security intelligence events, select **Monitor > Events > Security Intelligence**.

Meaning Using the time-range slider, you can quickly focus on the time and area of activity that you are most interested in. Once the time range is selected, all of the data presented in your view is refreshed automatically. You can also use the Custom button to set a custom time range.

You can select either the Grid View tab or the Chart View tab to view your data:

- **Grid View**—View the comprehensive details of security intelligence events in a tabular format that includes sortable columns. You can group the events using the Group By option. For example, you can group the events based on source country. The table includes information such as the event name, source address, source country, destination country, and so on. [Table 35 on page 54](#) describes the fields on the Grid View page.
- **Chart View**—View a brief summary of all the security intelligence events in your network. The top of the page has a swim lane graph of all the security intelligence events. You

can use the widgets at the bottom of the page to view critical information such as, top compromised host and top C&C Servers. [Table 36 on page 54](#) describes the widgets on the Chart View page.

Table 35: Security Intelligence—Fields on the Grid View Page

Field	Description
Timestamp	The time when the log was received.
Event Name	Event name of the log.
Source Country	Source country name from where the event originated.
Source Address	Source IP address from where the event occurred.
Destination Country	Destination country name from where the event occurred.
Destination Address	Destination IP address of the event.
Destination Port	Destination port of the event.
Source Port	Source port of the event.
Description	Description of the log.
Source Zone Name	The name of log source zone.
Host Name	The name of the host user in contact with the command and control server.
Action	The action taken on the communication (permitted or blocked).
Interface Name	Name of the interface.
Domain	Displays the network or subnetwork to which the device belongs.

Table 36: Security Intelligence—Widgets on the Chart View Page

Field	Description
Top Compromised Hosts	A list of the top compromised hosts based on their associated threat level and blocked status.
Top C&C Servers	A color-coded map displaying the location of Command and Control servers. Click a location on the map to view the number of detected sources.

- See Also**
- [Monitoring Screen Events on page 51](#)
 - [Monitoring System on page 56](#)

- [Monitoring ATP Events on page 55](#)

Monitoring ATP Events

Purpose Starting in Junos OS Release 19.2R1, you can monitor the Juniper Sky ATP events.

Use the monitoring functionality to view the ATP page.

Action To monitor Juniper Sky ATP events, select **Monitor > Events > ATP**.

Meaning Using the time-range slider, you can quickly focus on the time and area of activity that you are most interested in. Once the time range is selected, all of the data presented in your view is refreshed automatically. You can also use the Custom button to set a custom time range.

You can select either the Grid View tab or the Chart View tab to view your data:

- **Grid View**—View the comprehensive details of all Juniper Sky ATP events in a tabular format that includes sortable columns. You can group the events using the Group By option. For example, you can group the events based on source country. The table includes information such as the event name, source country, source address, destination country, malware information, and so on. [Table 37 on page 55](#) describes the fields on the Grid View page.
- **Chart View**—View a brief summary of all the Juniper Sky ATP events in your network. The top of the page has a swim lane graph of all the Juniper Sky ATP events. You can use the widgets at the bottom of the page to view critical information such as, Top malware source countries, top infected file categories, and top malwares identified. [Table 38 on page 56](#) describes the widgets on the Chart View page.

Table 37: ATP—Fields on the Grid View Page

Field	Description
Timestamp	The time when the log was received.
Event Name	Event name of the log.
Source Country	Source country name from where the event originated.
Source Address	Source IP address from where the event occurred.
Destination Country	Destination country name from where the event occurred.
Destination Address	Destination IP address of the event.
Source Port	Source port of the event.
Destination Port	Destination port of the event.

Table 37: ATP—Fields on the Grid View Page (continued)

Field	Description
Description	Description of the log.
Source Zone Name	The name of source zone of the log.
Action	Action taken for the event: warning, allow, and block.
Host Name	The hostname in the log.
Interface Name	Name of the interface.
Domain	Displays the network or subnetwork to which the device belongs.

Table 38: ATP—Widgets on the Chart View Page

Field	Description
Top Malware Source Countries	Top source countries from where the event source originated; sorted by the number of IP addresses.
Top Infected File Categories	A graph of the top infected file categories. Examples: executables, archived files, libraries. Use the arrows to filter by threat level and time frame.
Top Malwares Identified	Top malware found based on the number of times the malware is detected over a period of time.

- See Also**
- [Monitoring Security Intelligence Events on page 53](#)
 - [Monitoring Screen Events on page 51](#)
 - [Monitoring System on page 56](#)

Monitoring System

Purpose Use the monitoring functionality to view the events page.

Action To monitor events select **Monitor>Events>System** in the J-Web user interface.

Meaning [Table 39 on page 56](#) summarizes key output fields in the events page.

Table 39: System Monitoring Page

Field	Value	Additional Information
Events Filter		

Table 39: System Monitoring Page (continued)

Field	Value	Additional Information
System Log File	Specifies the name of the system log file that records errors and events.	-
Process	Specifies the system processes that generate the events to display.	-
Include archived files	Specifies to enable the option to include archived files.	Select to enable.
Date From	Specifies the beginning date range to monitor. Set the date using the calendar pick tool.	-
To	Specifies the end of the date range to monitor. Set the date using the calendar pick tool.	-
Event ID	Specifies the specific ID of the error or event to monitor.	-
Description	Enter a description for the errors or events.	-
Search	Fetches the errors and events specified in the search criteria.	-
Reset	Clears the cache of errors and events that were previously selected.	-
Generate Report	Creates an HTML report based on the specified parameters.	-
Events Detail		
Process	Displays the system process that generated the error or event.	-

Table 39: System Monitoring Page (continued)

Field	Value	Additional Information
Severity	<p>Displays the severity level that indicates how seriously the triggering event affects routing platform functions. Only messages from the facility that are rated at that level or higher are logged. Possible severities and their corresponding color code are:</p> <ul style="list-style-type: none"> • Debug/Info/Notice (Green)—Indicates conditions that are not errors but are of interest or might warrant special handling. • Warning (Yellow)—Indicates conditions that warrant monitoring. • Error (Blue)—Indicates standard error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels. • Critical (Pink)—Indicates critical conditions, such as hard drive errors. • Alert (Orange)—Indicates conditions that require immediate correction, such as a corrupted system database. • Emergency (Red)—Indicates system panic or other conditions that cause the routing platform to stop functioning. 	—
Event ID	<p>Displays the unique ID of the error or event. The prefix on each code identifies the generating software process. The rest of the code indicates the specific event or error.</p>	—
Event Description	<p>Displays a more detailed explanation of the message.</p>	—
Time	<p>Time that the error or event occurred.</p>	—

- See Also**
- [Monitoring Alarms on page 21](#)
 - [Monitoring Security Events by Policy on page 22](#)

Release History Table

Release	Description
19.2R1	Starting in Junos OS Release 19.2R1, you can see that an application displays the same value as a nested application (if the application supports nested application).
19.2R1	Starting in Junos OS Release 19.2R1, you can see that an application displays the same value as a nested application (if the application supports nested application).
19.2R1	Starting in Junos OS Release 19.2R1, you can monitor the screen events.
19.2R1	Starting in Junos OS Release 19.2R1, you can monitor the security intelligence events.
19.2R1	Starting in Junos OS Release 19.2R1, you can monitor the Juniper Sky ATP events.
19.1R1	Starting in Junos OS Release 19.1R1, All Events option is available for logical system users.
19.1R1	Starting in Junos OS Release 19.1R1, Firewall Events option is available for logical system and tenant users.
19.1R1	Starting in Junos OS Release 19.1R1, Web Filtering option is available for logical system users.
19.1R1	Starting in Junos OS Release 19.1R1, Content Filtering option is available for logical system users.
19.1R1	Starting in Junos OS Release 19.1R1, Antispam option is available for logical system users.
19.1R1	Starting in Junos OS Release 19.1R1, Antivirus option is available for logical system users.
19.1R1	Starting in Junos OS Release 19.1R1, IPS Events option is available for logical system users.

- Related Documentation**
- [Monitoring Alarms on page 21](#)
 - [Monitoring Security Events by Policy on page 22](#)

Applications

- [Monitoring Applications on page 59](#)

Monitoring Applications

- Purpose** You can use the Application Visibility page to view information on bandwidth consumption, session establishment, and the risks associated with your applications.

Analyzing your network applications yields useful security management information, such as abnormal applications that can lead to data loss, bandwidth hogging, time-consuming applications, and personal applications that can elevate business risks.

Action To monitor Applications select **Monitor>Applications** in the J-Web user interface.



NOTE: If traffic is not enabled, click Enable Logging. The **Configure>Device Setup>Basic Settings>Logging** page appears, where you can enable the traffic.

Meaning There are two ways to view your data. You can select either the Chart View tab or the Grid View tab.

Chart View

The Chart View is selected by default, and it gives a brief summary of the top 50 applications consuming maximum bandwidth in your network. The data is presented graphically as a bubble graph, heat map, or zoomable bubble graph.

You can reorder the bubble graph by bandwidth or by number of sessions from the **Show By** filter dropdown. The size of the bubble depends on the bandwidth used if you select Bandwidth in the dropdown. If you select Number of Sessions, the size of the bubble depends on the number of sessions.

The data is refreshed automatically based on the selected time range in the **Time Span** filter dropdown. The default time span is set to the last 15 minutes from the current time. If you select Custom, you need to specify the *from* and *to* date range in the Custom Time Range Selection popup window. You can also Edit the *from* and *to* date range.

You can reorder the bubble graph by groups in the **Group By** filter dropdown. The options are: Risk and Categories. If you select Risk, the bubbles are grouped by Critical, High, Unsafe, Moderate, Low, and Unknown criticality. If you select Categories, the bubbles are grouped by Gaming, Infrastructure, Messaging, Multimedia, P2P, Remote-Access, Web, and Unknown. The legends show the color associated with each group parameter.



NOTE: A *Fake application* bubble is created if a new application, whose name is not present in the signature database, is detected.

You can hover over your applications to view critical information such as total number of sessions, total number of blocks, category, bandwidth consumed, risk levels, and characteristics. You can also view the top five users accessing your application. Sessions appear as links, when you click a link, the All Events page appears.

Grid View

Click the Grid View link for comprehensive details on applications. You can view top users by volume, top applications by volume, top category by volume, top characteristics by

volume, and sessions by risk. You can also view the data in a tabular format that includes sortable columns. You can sort the applications in ascending or descending order based on application name, risk level, and so on. [Table 40 on page 61](#) describes the widgets in this view. Use these widgets to get an overall, high level view of your applications, users, and the content traversing your network.

Table 40: Applications Visibility in Grid View Widgets

Widget	Description
Top Users By Volume	Top users of the application; sorted by bandwidth consumption.
Top Apps By Volume	Top applications, such as Amazon, Facebook, and so on of the network traffic; sorted by bandwidth consumption.
Top Category By Volume	Top category, such as web, infrastructure, and so on of the application; sorted by bandwidth consumption.
Top Characteristics By Volume	Top behavioral characteristics, such as prone to misuse, bandwidth consumer, and so on of the application.
Sessions By Risk	Number of events/sessions received; grouped by risk.

[Table 41 on page 61](#) describes the fields in the table below the widgets. Users are displayed by usernames or IP addresses. When you click a link, the User Visibility page in Grid view appears with the correct filter applied. Sessions are also displayed as links and when you click a link, the All Events page appears with all security events. You can select an application or a user to perform a block operation.

Table 41: Grid View of Applications

Field	Description
Application Name	Name of the application, such as Amazon, Facebook, and so on.
Risk Level	Risk associated with the application: critical, high, unsafe, moderate, low, and unknown.
Users	Total number of users accessing the application.
Volume	Bandwidth used by the application.
Total Sessions	Total number of application sessions.
Category	Category of the application, such as web, infrastructure, and so on.
Sub-Category	Subcategory of the application. For example, social networking, news, and advertisements.

NOTE: There can be many sub-categories for a single category. For example, if the Category is Multimedia, it can have sub-categories as Video-streaming and Audio-streaming and so on.

Table 41: Grid View of Applications (continued)

Field	Description
Characteristics	<p>Characteristics of the application. For example, prone to misuse, bandwidth consumer, capable of tunneling.</p> <p>NOTE: There can be many characteristics displayed by a comma separator. For example, characteristics can be displayed as Support File Transfer, Loss of Productivity, Bandwidth.</p>

You can search the user interface by clicking the search lens icon. You can do a search in search by entering the second search string after the first search result is displayed.

You can sort the data based on the column heading. Mouse over the column heading, click the dropdown arrow, and select Sort Ascending or Sort Descending depending on how you want the data sorted.

- See Also**
- [Monitoring Alarms on page 21](#)
 - [Monitoring Security Events by Policy on page 22](#)

Users

- [Monitoring Users on page 62](#)

Monitoring Users

Purpose Use the User Visibility page to view information related to the bandwidth consumption and session establishment.

Starting in Junos OS Release 19.1R1, Users option is available for logical system and tenant users.

Action To monitor top 50 users, select **Monitor>Users** in the J-Web user interface.

Meaning There are two ways to view your data. You can select either the Chart View or Grid View.

Chart View

By default, the user's data is shown in the Chart view. It shows the top 50 users consuming maximum bandwidth in your network. The data is presented graphically as a bubble graph, heat map, or zoomable bubble graph.

You can reorder the bubble graph by bandwidth or by number of sessions from the **Show By** filter dropdown. The size of the bubble depends on the bandwidth used if you select Bandwidth in the dropdown. If you select Number of Sessions, the size of the bubble depends on the number of sessions.

The data is refreshed automatically based on the selected time range in the **Time Span** filter dropdown. If you select Custom, you need to specify the *from* and *to* date range in

the Custom Time Range Selection popup window. You can also Edit the *from* and *to* date range.

You can mouse over the bubble to view critical information for top five applications, such as total number of sessions, bandwidth consumed, and application name. You can also view the top five applications the user has accessed.

Grid View

Click Grid View to view the user's data in the tabular format. You can view top users by volume and top applications by volume. Grid view provides a detailed view of all the users. By default, data is sorted based on the bandwidth usage. [Table 42 on page 63](#) and [Table 43 on page 63](#) describe the fields on this page.

The data is refreshed automatically based on the selected time range in the **Time Span** filter dropdown. If you select Custom, you need to specify the *from* and *to* date range in the Custom Time Range Selection popup window. You can also Edit the *from* and *to* date range.

Table 42: User Visibility in Grid View Widgets

Widget	Description
Top Users By Volume	Top users of the application; sorted by bandwidth consumption.
Top Apps By Volume	Top applications, such as Amazon, Facebook, and so on of the network traffic; sorted by bandwidth consumption.

Table 43: Grid View of Users

Field	Description
User Name	Name of a user.
Volume	Bandwidth consumption of the user.
Total Sessions	Total number of user sessions.
Applications	All the applications used by a user for the time range.

You can search the user interface by clicking the search lens icon. You can do a search in search by entering the second search string after the first search result is displayed.

- See Also**
- [Monitoring Alarms on page 21](#)
 - [Monitoring Security Events by Policy on page 22](#)

System View

- [Monitoring Chassis Information on page 64](#)
- [Monitoring Cluster Status on page 65](#)
- [Monitoring Cluster Statistics on page 67](#)

Monitoring Chassis Information

Purpose View chassis properties, which include the status of hardware components on the device.

Action To view these chassis properties, select **Monitor>System View>Chassis Information** in the J-Web user interface.



CAUTION: Do not install a combination of Physical Interface Modules (PIMs) in a single chassis that exceeds the maximum power and heat capacity of the chassis. If power management is enabled, PIMs that exceed the maximum power and heat limits remain offline when the chassis is powered on. To check PIM power and heat status, use the **show chassis fpc** and **show chassis power-ratings** commands.

The Chassis Information page displays the following types of information:

- Routing Engine Details—This section of the page includes the following tabs:
 - Master—Master tab displays information about the routing engine, including the routing engine module, model number, version, part number, serial number, memory utilization, temperature, and start time. Additionally, this tab displays the CPU load averages for the last 1, 5, and 15 minutes.
 - Backup—If a backup routing engine is available, the Backup tab displays the routing engine module, model number, version, part number, serial number, memory utilization, temperature, and start time. Additionally, this tab displays the CPU load averages for the last 1, 5, and 15 minutes.



NOTE: If you need to contact customer support about the device chassis, supply them with the version and serial number displayed in the Routing Engine Details section of the page.

- Power and Fan Tray Details—This Details section of the page includes the following tabs:
 - Power—Power tab displays the names of the device's power supply units and their statuses.

- Fan—Fan tab displays the names of the device's fans and their speeds (normal or high). (The fan speeds are adjusted automatically according to the current temperature.)
- Chassis Component Details—This section of the page includes the following tabs:
 - General—General tab displays the version number, part number, serial number, and description of the selected device component.
 - Temperature—Temperature tab displays the temperature of the selected device component (if applicable).
 - Resource—Resource tab displays the state, total CPU DRAM, and start time of the selected device component (if applicable).



NOTE: On some devices, you can have an FPC state as “offline.” You might want to put an FPC offline because of an error or if the FPC is not responding. You can put the FPC offline by using the CLI command `request chassis fpc slot number offline`.

- Sub-Component—Sub-Component tab displays information about the device's sub-components (if applicable). Details include the sub-component's version, part number, serial number, and description.

To control which component details appear, select a hardware component from the **Select component** list.

Alternatively, you can view chassis details by entering the following **show** commands in the CLI configuration editor:

- `show chassis hardware`
- `show chassis routing-engine`
- `show chassis environment`
- `show chassis redundant-power-supply`
- `show redundant-power-supply status`

- See Also**
- [Monitoring Cluster Status on page 65](#)
 - [Monitoring Cluster Statistics on page 67](#)

Monitoring Cluster Status

Purpose Use the monitoring functionality to view the cluster status page.

Action To monitor cluster status select, **Monitor>System View>Cluster Status**.

Meaning Table 44 on page 66 summarizes key output fields on the cluster status page.

Table 44: Cluster Status Monitoring Page

Field	Value	Additional Information
Refresh Interval (sec)	Displays the time interval set for page refresh.	Select the time interval from the drop-down list.
Refresh	Displays the option to refresh the page.	—
Cluster Status		
Redundancy Group	Displays the redundancy group specified for the chassis cluster.	—
Failover	Displays the failover options selected. <ul style="list-style-type: none"> Counter— Displays the number of times chassis cluster failed. Action—Displays the active tool for users to fail over chassis cluster. 	—
Primary	Displays the node used for the chassis cluster.	—
Switch	Provides an option to switch between the primary and secondary nodes.	
Status	Displays the state of the redundancy group for node 0 and node 1. The possible states are: <ul style="list-style-type: none"> Primary—Redundancy group is active and passing traffic. Secondary—Redundancy group is passive and not passing traffic. Lost—Node loses contact with the other node through the control link. Most likely to occur when both nodes are in a cluster one node is rebooted, or, because of a control link failure, one node cannot exchange heartbeats with the other node. Unavailable—Node has not received a single heartbeat over the control link from the other node since the other node booted up. Most likely to occur when one node boots up before the other node or if only one node is present in the cluster. 	—
Preempt	Displays the preempt option selected to initiate a failover for node 0 and 1. The possible preempt options are: <ul style="list-style-type: none"> Yes—Mastership can be preempted based on priority. No—Mastership cannot be preempted if the priority changes. 	—

Table 44: Cluster Status Monitoring Page (continued)

Field	Value	Additional Information
Manual Failover	Displays the priority value of node 0 for manual failover. The possible manual failover options are: <ul style="list-style-type: none"> • Yes—If the mastership is set manually, it overrides the Priority and Preempt options. • No—Mastership is not set manually. 	—
Interface Monitoring		
I/F	Displays the interfaces monitored by the redundancy group and shows their respective weights.	—
Weight	Displays the weight for the interface to be monitored.	—
Status	Displays the status of the interface.	—

- See Also**
- [Monitoring Chassis Information on page 64](#)
 - [Monitoring Cluster Statistics on page 67](#)

Monitoring Cluster Statistics

Purpose Use the monitoring functionality to view the cluster statistics page.

Action To monitor cluster statistics select **Monitor>Device>Cluster Statistics**.

Meaning [Table 45 on page 67](#) summarizes key output fields in the cluster statistics page.

Table 45: Cluster Statistics Monitoring Page

Field	Value
Control Link Statistics	
Control Link Statistics	Displays the Statistics of the control link used by chassis cluster traffic. Statistics for Control link 1 are displayed when you use dual control links (SRX5000 line of devices only).
Heartbeat packets sent	Displays the Number of heartbeat messages sent on the control link.
Heartbeat packets received	Displays the number of heartbeat messages received on the control link.
Heartbeat packet errors	Displays the number of heartbeat packets received with errors on the control link.

Table 45: Cluster Statistics Monitoring Page (continued)

Field	Value
Fabric Link Statistics	
Fabric Link Statistics	Displays the statistics of the fabric link used by chassis cluster traffic. Statistics for Child Link 1 are displayed when you use dual fabric links.
Probes sent	Displays the number of probes sent on the fabric link.
Probes received	Displays the number of probes received on the fabric link.
Services Synchronized	
Service name	Displays the name of the service.
Rtos sent	Displays the number of runtime objects (RTOs) sent.
Rtos received	Displays the number of RTOs received.
Translation context	Displays the messages synchronizing Network Address Translation (NAT) translation context.
Incoming NAT	Displays the messages synchronizing incoming Network Address Translation (NAT) service.
Resource manager	Displays the messages synchronizing resource manager groups and resources.
Session create	Displays the messages synchronizing session creation.
Session close	Displays the messages synchronizing session close.
Session change	Displays the messages synchronizing session change.
Gate create	Displays the messages synchronizing creation of pinholes (temporary openings in the firewall).
Session ageout refresh request	Displays the messages synchronizing request session after age-out.
Session ageout refresh reply	Displays the messages synchronizing reply session after age-out.
IPsec VPN	Displays the messages synchronizing VPN session.
Firewall user authentication	Displays the messages synchronizing firewall user authentication session.
MGCP ALG	Displays the messages synchronizing MGCP ALG sessions.
H323 ALG	Displays the messages synchronizing H.323 ALG sessions.
SIP ALG	Displays the messages synchronizing SIP ALG sessions.

Table 45: Cluster Statistics Monitoring Page (continued)

Field	Value
SCCP ALG	Displays the messages synchronizing SCCP ALG sessions.
PPTP ALG	Displays the messages synchronizing PPTP ALG sessions.
RTSP ALG	Displays the messages synchronizing RTSP ALG sessions.
MAC address learning	Displays the messages synchronizing MAC address learning.

- See Also**
- [Monitoring Chassis Information on page 64](#)
 - [Monitoring Cluster Status on page 65](#)

NAT

- [Monitoring Source NAT Information on page 69](#)
- [Monitoring Destination NAT Information on page 75](#)
- [Monitoring Static NAT Information on page 77](#)
- [Monitoring Interface NAT Port Information on page 78](#)
- [Monitoring NAT Incoming Table Information on page 79](#)

Monitoring Source NAT Information

Purpose Display configured information about source Network Address Translation (NAT) rules, pools, persistent NAT, and paired addresses.

Action Select **Monitor>NAT>Source NAT** in the J-Web user interface, or enter the following CLI commands:

- **show security nat source summary**
- **show security nat source pool *pool-name***
- **show security nat source persistent-nat-table**
- **show security nat source paired-address**

[Table 46 on page 69](#) describes the available options for monitoring source NAT.

Table 46: Source NAT Monitoring Page

Field	Description	Action
Rules		
Rule-set Name	Name of the rule set.	Select all rule sets or a specific rule set to display from the list.

Table 46: Source NAT Monitoring Page (continued)

Field	Description	Action
Total rules	Number of rules configured.	—
ID	Rule ID number.	—
Name	Name of the rule .	—
From	Name of the routing instance/zone/interface from which the packet flows.	—
To	Name of the routing instance/zone/interface to which the packet flows.	—
Source address range	Source IP address range in the source pool.	—
Destination address range	Destination IP address range in the source pool.	—
Source ports	Source port numbers.	—
Ip protocol	IP protocol.	—
Action	Action taken for a packet that matches a rule.	—
Persistent NAT type	Persistent NAT type.	—
Inactivity timeout	Inactivity timeout interval for the persistent NAT binding.	—
Alarm threshold	Utilization alarm threshold.	—
Max session number	The maximum number of sessions.	—
Sessions (Succ/ Failed/ Current)	Successful, failed, and current sessions. <ul style="list-style-type: none"> Succ—Number of successful session installations after the NAT rule is matched. Failed—Number of unsuccessful session installations after the NAT rule is matched. Current—Number of sessions that reference the specified rule. 	—

Table 46: Source NAT Monitoring Page (continued)

Field	Description	Action
Translation Hits	Number of times a translation in the translation table is used for a source NAT rule.	—
Pools		
Pool Name	The names of the pools.	Select all pools or a specific pool to display from the list.
Total Pools	Total pools added.	—
ID	ID of the pool.	—
Name	Name of the source pool.	—
Address range	IP address range in the source pool.	—
Single/Twin ports	Number of allocated single and twin ports.	—
Port	Source port number in the pool.	—
Address assignment	Displays the type of address assignment.	—
Alarm threshold	Utilization alarm threshold.	—
Port overloading factor	Port overloading capacity.	—
Routing instance	Name of the routing instance.	—
Total addresses	Total IP address, IP address set, or address book entry.	—
Host address base	Host base address of the original source IP address range.	—
Translation hits	Number of times a translation in the translation table is used for source NAT.	—
Top 10 Translation Hits		
Graph	Displays the graph of top 10 translation hits.	—
Persistent NAT		

Table 46: Source NAT Monitoring Page (continued)

Field	Description	Action
Persistent NAT table statistics		
binding total	Displays the total number of persistent NAT bindings for the FPC.	—
binding in use	Number of persistent NAT bindings that are in use for the FPC.	—
enode total	Total number of persistent NAT enodes for the FPC.	—
enode in use	Number of persistent NAT enodes that are in use for the FPC.	—
Persistent NAT table		
Source NAT pool	Name of the pool.	Select all pools or a specific pool to display from the list.
Internal IP	Internal IP address.	Select all IP addresses or a specific IP address to display from the list.
Internal port	Displays the internal ports configured in the system.	Select the port to display from the list.
Internal protocol	Internal protocols .	Select all protocols or a specific protocol to display from the list.
Internal IP	Internal transport IP address of the outgoing session from internal to external.	—
Internal port	Internal transport port number of the outgoing session from internal to external.	—
Internal protocol	Internal protocol of the outgoing session from internal to external.	—
Reflective IP	Translated IP address of the source IP address.	—
Reflective port	Displays the translated number of the port.	—
Reflective protocol	Translated protocol.	—
Source NAT pool	Name of the source NAT pool where persistent NAT is used.	—
Type	Persistent NAT type.	—

Table 46: Source NAT Monitoring Page (continued)

Field	Description	Action
Left time/Conf time	Inactivity timeout period that remains and the configured timeout value.	—
Current session num/Max session num	Number of current sessions associated with the persistent NAT binding and the maximum number of sessions.	—
Source NAT rule	Name of the source NAT rule to which this persistent NAT binding applies.	—
External node table		
Internal IP	Internal transport IP address of the outgoing session from internal to external.	—
Internal port	Internal port number of the outgoing session from internal to external.	—
External IP	External IP address of the outgoing session from internal to external.	—
External port	External port of the outgoing session from internal to external.	—
Zone	External zone of the outgoing session from internal to external.	—
Paired Address		
Pool name	Name of the pool.	Select all pools or a specific pool to display from the list.
Specified Address	IP address.	Select all addresses, or select the internal or external IP address to display, and enter the IP address.
Pool name	Displays the selected pool or pools.	—
Internal address	Displays the internal IP address.	—
External address	Displays the external IP address.	—
Resource Usage		
Utilization for all source pools		

Table 46: Source NAT Monitoring Page (continued)

Field	Description	Action
Pool name	Name of the pool.	To view additional usage information for Port Address Translation (PAT) pools, select a pool name. The information displays under Detail Port Utilization for Specified Pool.
Pool type	Pool type: PAT or Non-PAT.	—
Port overloading factor	Port overloading capacity for PAT pools.	—
Address	Addresses in the pool.	—
Used	<p>Number of used resources in the pool.</p> <p>For Non-PAT pools, the number of used IP addresses is displayed.</p> <p>For PAT pools, the number of used ports is displayed.</p>	—
Available	<p>Number of available resources in the pool.</p> <p>For Non-PAT pools, the number of available IP addresses is displayed.</p> <p>For PAT pools, the number of available ports is displayed.</p>	—
Total	<p>Number of used and available resources in the pool.</p> <p>For Non-PAT pools, the total number of used and available IP addresses is displayed.</p> <p>For PAT pools, the total number of used and available ports is displayed.</p>	—
Usage	<p>Percent of resources used.</p> <p>For Non-PAT pools, the percent of IP addresses used is displayed.</p> <p>For PAT pools, the percent of ports, including single and twin ports, is displayed.</p>	—
Peak usage	Percent of resources used during the peak date and time.	—
Detail Port Utilization for Specified Pool		
Address Name	IP addresses in the PAT pool.	Select the IP address for which you want to display detailed usage information.
Factor-Index	Index number.	—

Table 46: Source NAT Monitoring Page (continued)

Field	Description	Action
Port-range	Displays the number of ports allocated at a time.	—
Used	Displays the number of used ports.	—
Available	Displays the number of available ports.	—
Total	Displays the number of used and available ports.	—
Usage	Displays the percentage of ports used during the peak date and time.	—

Monitoring Destination NAT Information

Purpose View the destination Network Address Translation (NAT) summary table and the details of the specified NAT destination address pool information.

Action Select **Monitor>NAT> Destination NAT** in the J-Web user interface, or enter the following CLI commands:

- **show security nat destination summary**
- **show security nat destination pool *pool-name***

Table 47 on page 75 summarizes key output fields in the destination NAT display.

Table 47: Summary of Key Destination NAT Output Fields

Field	Values	Action
Rules		
Rule-set Name	Name of the rule set.	Select all rule sets or a specific rule set to display from the list.
Total rules	Number of rules configured.	—
ID	Rule ID number.	—
Name	Name of the rule .	—
Ruleset Name	Name of the rule set.	—
From	Name of the routing instance/zone/interface from which the packet flows.	—

Table 47: Summary of Key Destination NAT Output Fields (continued)

Field	Values	Action
Source address range	Source IP address range in the source pool.	—
Destination address range	Destination IP address range in the source pool.	—
Destination port	Destination port in the destination pool.	—
IP protocol	IP protocol.	—
Action	Action taken for a packet that matches a rule.	—
Alarm threshold	Utilization alarm threshold.	—
Sessions (Succ/ Failed/ Current)	Successful, failed, and current sessions. <ul style="list-style-type: none"> Succ—Number of successful session installations after the NAT rule is matched. Failed—Number of unsuccessful session installations after the NAT rule is matched. Current—Number of sessions that reference the specified rule. 	—
Translation hits	Number of times a translation in the translation table is used for a destination NAT rule.	—
Pools		
Pool Name	The names of the pools.	Select all pools or a specific pool to display from the list.
Total Pools	Total pools added.	—
ID	ID of the pool.	—
Name	Name of the destination pool.	—
Address range	IP address range in the destination pool.	—
Port	Destination port number in the pool.	—
Routing instance	Name of the routing instance.	—

Table 47: Summary of Key Destination NAT Output Fields (continued)

Field	Values	Action
Total addresses	Total IP address, IP address set, or address book entry.	–
Translation hits	Number of times a translation in the translation table is used for destination NAT.	–
Top 10 Translation Hits		
Graph	Displays the graph of top 10 translation hits.	–

Monitoring Static NAT Information

Purpose View static NAT rule information.

Action Select **Monitor>NAT>Static NAT** in the J-Web user interface, or enter the following CLI command:

show security nat static rule

Table 48 on page 77 summarizes key output fields in the static NAT display.

Table 48: Summary of Key Static NAT Output Fields

Field	Values	Action
Rule-set Name	Name of the rule set.	Select all rule sets or a specific rule set to display from the list.
Total rules	Number of rules configured.	–
ID	Rule ID number.	–
Position	Position of the rule that indicates the order in which it applies to traffic.	–
Name	Name of the rule.	–
Ruleset Name	Name of the rule set.	–
From	Name of the routing instance/interface/zone from which the packet comes	–
Source addresses	Source IP addresses.	–
Source ports	Source port numbers.	–

Table 48: Summary of Key Static NAT Output Fields (continued)

Field	Values	Action
Destination addresses	Destination IP address and subnet mask.	—
Destination ports	Destination port numbers .	—
Host addresses	Name of the host addresses.	—
Host ports	Host port numbers.	
Netmask	Subnet IP address.	—
Host routing instance	Name of the routing instance from which the packet comes.	—
Alarm threshold	Utilization alarm threshold.	—
Sessions (Succ/ Failed/ Current)	Successful, failed, and current sessions. <ul style="list-style-type: none"> • Succ—Number of successful session installations after the NAT rule is matched. • Failed—Number of unsuccessful session installations after the NAT rule is matched. • Current—Number of sessions that reference the specified rule. 	—
Translation hits	Number of times a translation in the translation table is used for a static NAT rule.	—
Top 10 Translation Hits Graph	Displays the graph of top 10 translation hits.	—

Monitoring Interface NAT Port Information

Purpose View port usage for an interface source pool information.

- Action** To monitoring interface NAT port information, do one of the following:
- If you are using SRX5400, SRX5600, or SRX5800 platforms, select **Monitor>Firewall/NAT>Interface NAT** in the J-Web user interface or enter the CLI command **show security nat interface-nat-ports**.
 - Select **Monitor>NAT>Interface NAT Ports** in the J-Web user interface.

[Table 49 on page 79](#) summarizes key output fields in the interface NAT display.

Table 49: Summary of Key Interface NAT Output Fields

Field	Values	Additional Information
Interface NAT Summary Table		
Pool Index	Port pool index.	—
Total Ports	Total number of ports in a port pool.	—
Single Ports Allocated	Number of ports allocated one at a time that are in use.	—
Single Ports Available	Number of ports allocated one at a time that are free for use.	—
Twin Ports Allocated	Number of ports allocated two at a time that are in use.	—
Twin Ports Available	Number of ports allocated two at a time that are free for use.	—

Monitoring NAT Incoming Table Information

Purpose View NAT table information.

Action Select **Monitor>NAT>Incoming Table** in the J-Web user interface, or enter the following CLI command:

show security nat incoming-table

[Table 50 on page 79](#) summarizes key output fields in the incoming table display.

Table 50: Summary of Key Incoming Table Output Fields

Field	Values
Statistics	
In use	Number of entries in the NAT table.
Maximum	Maximum number of entries possible in the NAT table.
Entry allocation failed	Number of entries failed for allocation.
Incoming Table	
Clear	
Destination	Destination IP address and port number.

Table 50: Summary of Key Incoming Table Output Fields (continued)

Field	Values
Host	Host IP address and port number that the destination IP address is mapped to.
References	Number of sessions referencing the entry.
Timeout	Timeout, in seconds, of the entry in the NAT table.
Source-pool	Name of source pool where translation is allocated.

Security

- [Policy on page 80](#)
- [Screen Counters on page 86](#)
- [UTM on page 89](#)
- [ICAP Redirect on page 93](#)
- [IPS on page 94](#)
- [Flow Session on page 97](#)
- [Flow Gate on page 100](#)
- [Authentication on page 101](#)
- [Voice ALGs on page 104](#)
- [Application Firewall on page 118](#)
- [Application Tracking on page 119](#)
- [DS-Lite on page 122](#)
- [AppQoS on page 123](#)
- [Threat Prevention on page 125](#)

Policy

- [Monitoring Policies on page 80](#)
- [Checking Policies on page 83](#)

Monitoring Policies

Purpose Display, sort, and review policy activity for every activated policy configured on the device. Policies are grouped by Zone Context (the from and to zones of the traffic) to control the volume of data displayed at one time. From the policy list, select a policy to display statistics and current network activity.

Action To review policy activity:

1. Select **Monitor>Security>Policy>Activities** in the J-Web user interface. The Security Policies Monitoring page appears and lists the policies from the first Zone Context. See [Table 51 on page 81](#) for field descriptions.
2. Select the **Zone Context** of the policy you want to monitor, and click **Filter**. All policies within the zone context appear in match sequence.
3. Select a policy, and click **Clear Statistics** to set all counters to zero for the selected policy.

Table 51: Security Policies Monitoring Output Fields

Field	Value	Additional Information
Zone Context (Total #)	Displays a list of all from and to zone combinations for the configured policies. The total number of active policies for each context is specified in the Total # field. By default, the policies from the first Zone Context are displayed.	To display policies for a different context, select a zone context and click Filter . Both inactive and active policies appear for each context. However, the Total # field for a context specifies the number of active policies only.
Default Policy action	Specifies the action to take for traffic that does not match any of the policies in the context: <ul style="list-style-type: none"> • permit-all—Permit all traffic that does not match a policy. • deny-all—Deny all traffic that does not match a policy. 	—
From Zone	Displays the source zone to be used as match criteria for the policy.	—
To Zone	Displays the destination zone to be used as match criteria for the policy.	—
Name	Displays the name of the policy.	—
Source Address	Displays the source addresses to be used as match criteria for the policy. Address sets are resolved to their individual names. (In this case, only the names are given, not the IP addresses).	—
Destination Address	Displays the destination addresses (or address sets) to be used as match criteria for the policy. Addresses are entered as specified in the destination zone's address book.	—
Source Identity	Displays the name of the source identities set for the policy.	To display the value of the source identities, hover the mouse on this field. Unknown source identities are also displayed.
Application	Displays the name of a predefined or custom application signature to be used as match criteria for the policy.	—

Table 51: Security Policies Monitoring Output Fields (continued)

Field	Value	Additional Information
Dynamic App	<p>Displays the dynamic application signatures to be used as match criteria if an application firewall rule set is configured for the policy.</p> <p>For a network firewall, a dynamic application is not defined.</p>	<p>The rule set appears in two lines. The first line displays the configured dynamic application signatures in the rule set. The second line displays the default dynamic application signature.</p> <p>If more than two dynamic application signatures are specified for the rule set, hover over the output field to display the full list in a tooltip.</p>
Action	<p>Displays the action portion of the rule set if an application firewall rule set is configured for the policy.</p> <ul style="list-style-type: none"> • permit—Permits access to the network services controlled by the policy. A green background signifies permission. • deny—Denies access to the network services controlled by the policy. A red background signifies denial. 	<p>The action portion of the rule set appears in two lines. The first line identifies the action to be taken when the traffic matches a dynamic application signature. The second line displays the default action when traffic does not match a dynamic application signature.</p>
NW Services	<p>Displays the network services permitted or denied by the policy if an application firewall rule set is configured. Network services include:</p> <ul style="list-style-type: none"> • gprs-gtp-profile—Specify a GPRS Tunneling Protocol profile name. • idp—Perform intrusion detection and prevention. • redirect-wx—Set WX redirection. • reverse-redirect-wx—Set WX reverse redirection. • uac-policy—Enable unified access control enforcement of the policy. 	—
Policy Hit Counters Graph	<p>Provides a representation of the value over time for a specified counter. The graph is blank if Policy Counters indicates no data. As a selected counter accumulates data, the graph is updated at each refresh interval.</p>	<p>To toggle a graph on and off, click the counter name below the graph.</p>

Table 51: Security Policies Monitoring Output Fields (continued)

Field	Value	Additional Information
Policy Counters	<p>Lists statistical counters for the selected policy if Count is enabled. The following counters are available for each policy:</p> <ul style="list-style-type: none"> • input-bytes • input-byte-rate • output-bytes • output-byte-rate • input-packets • input-packet-rate • output-packets • output-packet-rate • session-creations • session-creation-rate • active-sessions 	To graph or to remove a counter from the Policy Hit Counters Graph, toggle the counter name. The names of enabled counters appear below the graph.

- See Also**
- [Checking Policies on page 83](#)
 - [Monitoring Screen Counters on page 86](#)

Checking Policies

Purpose Enter match criteria and conduct a policy search. The search results include all policies that match the traffic criteria in the sequence in which they will be encountered.

Because policy matches are listed in the sequence in which they would be encountered, you can determine whether a specific policy is being applied correctly or not. The first policy in the list is applied to all matching traffic. Policies listed after this one remain in the “shadow” of the first policy and are never encountered by this traffic.

By manipulating the traffic criteria and policy sequence, you can tune policy application to suit your needs. During policy development, you can use this feature to establish the appropriate sequence of policies for optimum traffic matches. When troubleshooting, use this feature to determine if specific traffic is encountering the appropriate policy.

- Action**
1. Select **Monitor>Security>Policy>Shadow Policies** in the J-Web user interface. The Check Policies page appears. [Table 52 on page 84](#) explains the content of this page.
 2. In the top pane, enter the From Zone and To Zone to supply the context for the search.
 3. Enter match criteria for the traffic, including the source address and port, the destination address and port, and the protocol of the traffic.

4. Enter the number of matching policies to display.
5. Click **Search** to find policies matching your criteria. The lower pane displays all policies matching the criteria up to the number of policies you specified.
 - The first policy will be applied to all traffic with this match criteria.
 - Remaining policies will not be encountered by any traffic with this match criteria.
6. To manipulate the position and activation of a policy, select the policy and click the appropriate button:
 - **Move**—Moves the selected policy up or down to position it at a more appropriate point in the search sequence.
 - **Move to**—Moves the selected policy by allowing you to drag and drop it to a different location on the same page.

Table 52: Check Policies Output

Field	Function
Check Policies Search Input Pane	
From Zone	Name or ID of the source zone. If a From Zone is specified by name, the name is translated to its ID internally.
To Zone	Name or ID of the destination zone. If a To Zone is specified by name, the name is translated to its ID internally.
Source Address	Address of the source in IP notation.
Source Port	Port number of the source.
Destination Address	Address of the destination in IP notation.
Destination Port	Port number of the destination.
Source Identity	Name of the source identity.

Table 52: Check Policies Output (continued)

Field	Function
Protocol	Name or equivalent value of the protocol to be matched. ah —51 egp —8 esp —50 gre —47 icmp —1 igmp —2 igp —9 ipip —94 ipv6 —41 ospf —89 pgm —113 pim —103 rdp —27 rsvp —46 sctp —132 tcp —6 udp —17 vrrp —112
Result Count	(Optional) Number of policies to display. Default value is 1. Maximum value is 16.
Check Policies List	
From Zone	Name of the source zone.
To Zone	Name of the destination zone.
Total Policies	Number of policies retrieved.
Default Policy action	The action to be taken if no match occurs.
Name	Policy name

Table 52: Check Policies Output (continued)

Field	Function
Source Address	Name of the source address (not the IP address) of a policy. Address sets are resolved to their individual names.
Destination Address	Name of the destination address or address set. A packet's destination address must match this value for the policy to apply to it.
Source Identity	Name of the source identity for the policy.
Application	Name of a preconfigured or custom application of the policy match.
Action	Action taken when a match occurs as specified in the policy.
Hit Counts	Number of matches for this policy. This value is the same as the Policy Lookups in a policy statistics report.
Active Sessions	Number of active sessions matching this policy.

Alternatively, to list matching policies using the CLI, enter the **show security match-policies** command and include your match criteria and the number of matching policies to display.

- See Also**
- [Monitoring Policies on page 80](#)
 - [Monitoring Screen Counters on page 86](#)

Screen Counters

- [Monitoring Screen Counters on page 86](#)

Monitoring Screen Counters

Purpose View screen statistics for a specified security zone.

Action Select **Monitor>Security>Screen Counters** in the J-Web user interface, or enter the following CLI command:

```
show security screen statistics zone zone-name
```

[Table 53 on page 86](#) summarizes key output fields in the screen counters display.

Table 53: Summary of Key Screen Counters Output Fields

Field	Values	Additional Information
Zones		

Table 53: Summary of Key Screen Counters Output Fields (continued)

Field	Values	Additional Information
ICMP Flood	Internet Control Message Protocol (ICMP) flood counter.	An ICMP flood typically occurs when ICMP echo requests use all resources in responding, such that valid network traffic can no longer be processed.
UDP Flood	User Datagram Protocol (UDP) flood counter.	UDP flooding occurs when an attacker sends IP packets containing UDP datagrams with the purpose of slowing down the resources, such that valid connections can no longer be handled.
TCP Winnuke	Number of Transport Control Protocol (TCP) WinNuke attacks.	WinNuke is a denial-of-service (DoS) attack targeting any computer on the Internet running Windows.
TCP Port Scan	Number of TCP port scans.	The purpose of this attack is to scan the available services in the hopes that at least one port will respond, thus identifying a service to target.
ICMP Address Sweep	Number of ICMP address sweeps.	An IP address sweep can occur with the intent of triggering responses from active hosts.
IP Tear Drop	Number of teardrop attacks.	Teardrop attacks exploit the reassembly of fragmented IP packets.
TCP SYN Attack	Number of TCP SYN attacks.	—
IP Spoofing	Number of IP spoofs.	IP spoofing occurs when an invalid source address is inserted in the packet header to make the packet appear to come from a trusted source.
ICMP Ping of Death	ICMP ping of death counter.	Ping of death occurs when IP packets are sent that exceed the maximum legal length (65,535 bytes).
IP Source Route	Number of IP source route attacks.	—
TCP Land Attack	Number of land attacks.	Land attacks occur when attacker sends spoofed SYN packets containing the IP address of the victim as both the destination and source IP address.
TCP SYN Fragment	Number of TCP SYN fragments.	—
TCP No Flag	Number of TCP headers without flags set.	A normal TCP segment header has at least one control flag set.
IP Unknown Protocol	Number of unknown Internet protocols.	—
IP Bad Options	Number of invalid options.	—

Table 53: Summary of Key Screen Counters Output Fields (continued)

Field	Values	Additional Information
IP Record Route Option	Number of packets with the IP record route option enabled.	This option records the IP addresses of the network devices along the path that the IP packet travels.
IP Timestamp Option	Number of IP timestamp option attacks.	This option records the time (in Universal Time) when each network device receives the packet during its trip from the point of origin to its destination.
IP Security Option	Number of IP security option attacks.	—
IP Loose route Option	Number of IP loose route option attacks.	This option specifies a partial route list for a packet to take on its journey from source to destination.
IP Strict Source Route Option	Number of IP strict source route option attacks.	This option specifies the complete route list for a packet to take on its journey from source to destination.
IP Stream Option	Number of stream option attacks.	This option provides a way for the 16-bit SATNET stream identifier to be carried through networks that do not support streams.
ICMP Fragment	Number of ICMP fragments.	Because ICMP packets contain very short messages, there is no legitimate reason for ICMP packets to be fragmented. If an ICMP packet is so large that it must be fragmented, something is amiss.
ICMP Large Packet	Number of large ICMP packets.	—
TCP SYN FIN Packet	Number of TCP SYN FIN packets.	—
TCP FIN without ACK	Number of TCP FIN flags without the acknowledge (ACK) flag.	—
TCP SYN-ACK-ACK Proxy	Number of TCP flags enabled with SYN-ACK-ACK.	To prevent flooding with SYN-ACK-ACK sessions, you can enable the SYN-ACK-ACK proxy protection screen option. After the number of connections from the same IP address reaches the SYN-ACK-ACK proxy threshold, Junos OS rejects further connection requests from that IP address.
IP Block Fragment	Number of IP block fragments.	—

- See Also**
- [Monitoring Policies on page 80](#)
 - [Checking Policies on page 83](#)

UTM

- [Monitoring Antivirus on page 89](#)
- [Monitoring Web Filtering on page 90](#)
- [Monitoring Antispam on page 91](#)
- [Monitoring Content Filtering on page 92](#)

Monitoring Antivirus

Purpose Use the monitoring functionality to view the antivirus page.

Action To monitor antivirus select **Monitor>UTM>Antivirus** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Monitor>Security>UTM>Antivirus** in the J-Web user interface.

Meaning [Table 54 on page 89](#) summarizes key output fields in the antivirus page.

Table 54: Antivirus Monitoring Page

Field	Value	Additional Information
UTM Antivirus		
AV Key Expire Date	Displays antivirus licence key expiration date.	—
Update Server	Displays antivirus pattern update server settings.	—
Interval	Displays antivirus pattern interval.	—
Auto Update Status	Displays antivirus pattern auto update status.	—
Last Result	Displays last result of database loading.	—
AV Signature Version	Displays database version timestamp virus record number.	—
Scan Engine Info	Displays the information of the scan engine.	—
Pattern Type	Displays the pattern type.	—
UTM Antivirus Statistics		

Table 54: Antivirus Monitoring Page (continued)

Field	Value	Additional Information
Antivirus statistics	Displays the antivirus statistics <ul style="list-style-type: none"> • The number of scan request being pre-windowed. • The total number of scan request forwarded to the engine. • The number of scan requests using scan-all mode. • The number of scan requests using scan-by-extension mode. 	—
Clear Anti-Virus Statistics	Clear all current viewable statistics and begin collecting new statistics.	—

- See Also**
- [Monitoring Web Filtering on page 90](#)
 - [Monitoring Antispam on page 91](#)
 - [Monitoring Content Filtering on page 92](#)

Monitoring Web Filtering

Purpose Use the monitoring functionality to view the web filtering page.

Action To monitor web filtering select **Monitor>UTM>Web Filtering** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Monitor>Security>UTM>Web Filtering** in the J-Web user interface.

Meaning [Table 55 on page 90](#) summarizes key output fields in the web filtering page.

Table 55: web filtering Monitoring Page

Field	Value	Additional Information
UTM Web Filtering Statistics		

Table 55: web filtering Monitoring Page (continued)

Field	Value	Additional Information
Statistics type	Displays the available information <ul style="list-style-type: none"> • white list hit • Black list hit • Queries to server • Server reply permit • Server reply block • Custom category permit • Custom category block • Site reputation permit • Site reputation block • Cache hit permit • Cache hit block • Safe-search redirect • Web-filtering sessions in total • Web-filtering sessions in use • Fall back: log-and-permit block • Default • Timeout • Connectivity • Too-many-requests 	—
Clear Web Filtering Statistics	Clear all current viewable statistics and begin collecting new statistics.	Click Clear Web Filtering Statistics.

- See Also**
- [Monitoring Antivirus on page 89](#)
 - [Monitoring Antispam on page 91](#)
 - [Monitoring Content Filtering on page 92](#)

Monitoring Antispam

- Purpose** Use the monitoring functionality to view the antispam page.
- Action** To monitor antispam, select **Monitor>Security>UTM>Anti Spam**.
- Meaning** [Table 56 on page 92](#) summarizes key output fields in the antispam page.

Table 56: Anti Spam Monitoring Page

Field	Value	Additional Information
UTM Anti Spam Status	Displays the DNS server setting IP and interface details for the following servers: <ul style="list-style-type: none"> • Primary • Secondary • Ternary 	–
UTM Anti-spam Statistics	Displays the antispam statistics type and counter information: <ul style="list-style-type: none"> • SBL Whitelist Server • SBL Blacklist Server • DNS Server • Primary • Secondary • Ternary • Total connections • Denied connections • Total greetings • Denied greetings • Total e-mail scanned • Spam total • Spam tagged • Spam dropped • DNS errors • Timeout errors • Return errors • Invalid parameter errors • Statistics start time 	–
Clear Anti-spam statistics	Clear all current viewable statistics and begin collecting new statistics.	Click Clear Anti-spam statistics .

- See Also**
- [Monitoring Antivirus on page 89](#)
 - [Monitoring Web Filtering on page 90](#)
 - [Monitoring Content Filtering on page 92](#)

Monitoring Content Filtering

Purpose Use the monitoring functionality to view the content filtering page.

Action To monitor content filtering select **Monitor>Security>UTM>Content Filtering**.

Meaning [Table 57 on page 93](#) summarizes key output fields in the content filtering page.

Table 57: content filtering Monitoring Page

Field	Value	Additional Information
UTM Content Filtering Statistics	Displays the statistics type, counter passed, and counter blocked details: <ul style="list-style-type: none"> • Base on command list • Base on mime list • Base on extension list • ActiveX plugin • Java applet • EXE files • ZIP files • HTTP cookie 	
Clear Content Filtering statistics	Clear all current viewable statistics and begin collecting new statistics.	Click Clear Content Filtering statistics

- See Also**
- [Monitoring Antivirus on page 89](#)
 - [Monitoring Web Filtering on page 90](#)
 - [Monitoring Antispam on page 91](#)

ICAP Redirect

- [Monitoring ICAP Redirect on page 93](#)

Monitoring ICAP Redirect

Purpose Use the monitoring functionality to view the events page.

Action To monitor ICAP redirects select **Monitor>Security Services>ICAP Redirect** in the J-Web user interface.

Meaning The SRX Series device acts as an SSL proxy, decrypts HTTP or HTTPS traffic, and redirects the HTTP message to a third-party, on-premise DLP server through the Internet Content Adaptation Protocol (ICAP) channel. To enable ICAP redirection service, you must configure an ICAP redirect profile.

This page displays ICAP Redirect statistics such as - message redirected, message received, and fallback options details, to the permitted traffic.

The **Message Redirected** and the **Message Received** displays the number of HTTP requests that have passed through the ICAP channel.

In the **Refresh Interval(sec)** list you can select the refresh rate. Alternatively you can use the **Refresh** button as any point to refresh irrespective of the refresh rate set.

Clear Statistics clears all the collated data.

Server Status displays the status of the ICAP server.

Message REQMOD Redirected displays the number of messages that went through the redirect request on HTTP request.

Message RESPMOD Redirected displays the number of messages that went through the redirect response on HTTP request.

The **Fallback Details** section displays the Timeout, Connectivity, and Default values for Permitted, Rejected, and Log permitted parameters if the ICAP server is unavailable.

- See Also**
- [Monitoring Alarms on page 21](#)
 - [Monitoring Security Events by Policy on page 22](#)

IPS

- [Monitoring Attacks on page 94](#)
- [Monitoring IDP Status on page 96](#)

Monitoring Attacks

Purpose Use the monitoring functionality to view the Attacks page.

Action To monitor attacks, select **Monitor>Security>IDP>Attacks** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Monitor>Security>IPS>Attacks** in the J-Web user interface.

Meaning [Table 58 on page 94](#) summarizes key output fields in the attacks page.

Table 58: Attacks Monitoring Page

Field	Description	Additional Information
Enable Log	An option to enable event logs.	Click Enable Log to enable logs.
Clear Log	An option to clear all the logs that is created during the session.	Click Clear Log.
Refresh interval (sec)	Displays the time interval, in seconds, set for page refresh. The default interval is 30 seconds	Select the time interval from the list.

Table 58: Attacks Monitoring Page (continued)

Field	Description	Additional Information
Refresh	Displays the option to refresh the page. If Manual option is set, then manually click the Refresh button to refresh the page.	Click Refresh to refresh the page.
Clear	Provides an option to clear the data of the status type.	Click Clear to clear the details.
Attack Table		
Filter By Attack Name	Specifies the string to search.	Enter the string and then click Go to execute the searching operation.
Clear	Provides an option to disable the searching operation and show all results.	Click Clear to show all results.
Active IDP policy	Displays active IDP policy that is used in the session.	—
Attack Name	<p>Displays the kind of attacks in the attack table. Double click on Attack Name, Attack Details are displayed.</p> <p>The available options are:</p> <ul style="list-style-type: none"> • Display Name — Displays the name of the attack. • Severity — Displays the severity of the attack. • Category — Displays the category of attack in which the attacks are placed. • Recommended — Displays True or false to determined whether recommended or not. • Recommended Option — Displays a recommended action, when the security device detects an attack. • Type — Displays the type of attack. • Direction — Displays the connection direction of the attack. • False positives — Specifies the name of the false positives filter. • Services — Displays the service name. 	Double click Attack Name.
Severity	Displays the severity of the attack. The severity levels are: critical, info, minor, major and warning.	—

Table 58: Attacks Monitoring Page (continued)

Field	Description	Additional Information
Hits	Displays the count of hits. Double click on hits count, Attack Records are displayed. The available options are: <ul style="list-style-type: none"> • Filter Log— To filter the attack records. • Go— To execute searching operation. • Clear— To clear the attack records. 	Double click hits count, and then select an option.
Top N Attack Hits	Displays statistics about hits and shows top 10 hits.	—
Description	Displays information about attack.	—

See Also • [Monitoring Flow Session Statistics on page 97](#)

Monitoring IDP Status

Purpose View detailed information about the IDP Status, Memory, Counters, Policy Rulebase Statistics, and Attack table statistics.

Action To view Intrusion Detection and Prevention (IDP) table information, do one of the following:

- If you are using SRX5400, SRX5600, or SRX5800 platforms, select **Monitor>Security>IDP>Status** in the J-Web user interface, or enter the following CLI commands:

```
show security idp status
show security idp memory
```
- Select **Monitor>Security>IPS>Status** in the J-Web user interface.

[Table 59 on page 96](#) summarizes key output fields in the IDP display.

Table 59: Summary of IDP Status Output Fields

Field	Values	Additional Information
IDP Status		
Status of IDP	Displays the status of the current IDP policy.	—
Up Since	Displays the time from when the IDP policy first began running on the system.	—

Table 59: Summary of IDP Status Output Fields (continued)

Field	Values	Additional Information
Packets/Second	Displays the number of packets received and returned per second.	–
Peak	Displays the maximum number of packets received per second and the time when the maximum was reached.	–
Kbits/Second	Displays the aggregated throughput (kilobits per second) for the system.	–
Peak Kbits	Displays the maximum kilobits per second and the time when the maximum was reached.	–
Latency (Microseconds)	Displays the delay, in microseconds, for a packet to receive and return by a node .	–
Current Policy	Displays the name of the current installed IDP policy.	–
IDP Memory Status		
IDP Memory Statistics	Displays the status of all IDP data plane memory.	–
PIC Name	Displays the name of the PIC.	–
Total IDP Data Plane Memory (MB)	Displays the total memory space, in megabytes, allocated for the IDP data plane.	–
Used (MB)	Displays the used memory space, in megabytes, for the data plane.	–
Available (MB)	Displays the available memory space, in megabytes, for the data plane.	–

See Also • [Monitoring Flow Session Statistics on page 97](#)

Flow Session

- [Monitoring Flow Session Statistics on page 97](#)

Monitoring Flow Session Statistics

Purpose Use the monitoring functionality to view the flow session statistics page.

Action To monitor flow session statistics, select **Monitor>Security>Flow Session Statistics** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Monitor>Security>Flow Session** in the J-Web user interface.

Meaning Table 60 on page 98 summarizes key output fields in the flow session statistics page.

Table 60: Flow Session Statistics Monitoring Page

Field	Value	Additional Information
Session Filter	Provides the option to filter sessions. The available options are: <ul style="list-style-type: none"> all application destination-port destination-prefix interface protocol source-port source-prefix 	Select an option.
Clear	Provides the option to clear the session details statistics.	Click Clear to clear the details session statistics.
Show	Provides the option to show the session details statistics.	Click Show to show the details session statistics.
Session Summary - all		
Valid sessions	Displays the summary of valid sessions.	—
Pending sessions	Displays the summary of pending sessions.	—
Invalidated sessions	Displays the summary of invalid sessions.	—
Sessions in other states	Displays the summary of sessions in other states	—
Unicast-sessions	Displays the total number of active unicast sessions.	—
Multicast-sessions	Displays the total number of active multicast sessions.	—
Failed-sessions	Displays the total number of failed sessions.	—
Active-sessions	Displays the total number of active sessions.	—
Maximum-sessions	Displays the maximum number of supported sessions.	—
Session Summary — application		
Application name	Displays the application name for the session summary.	Select the application from the drop down box.

Table 60: Flow Session Statistics Monitoring Page (continued)

Field	Value	Additional Information
Session ID	Displays the number that identifies the session. Use this ID to get more information about the session.	–
Policy name	Displays the policy that permitted the traffic.	–
Timeout	Displays the idle timeout after which the session expires.	–
In	Displays the incoming flow (source and destination IP addresses, application protocol, and interface).	–
Out	Displays the reverse flow (source and destination IP addresses, application protocol, and interface).	–
Session Summary — destination-port		
Port	Provides the option to enter the destination port address.	Enter the destination port address.
Session ID	Displays the number that identifies the session. Use this ID to get more information about the session.	–
Policy name	Displays the policy that permitted the traffic.	–
Timeout	Displays the idle timeout after which the session expires.	–
In	Displays the incoming flow (source and destination IP addresses, application protocol, and interface).	–
Out	Displays the reverse flow (source and destination IP addresses, application protocol, and interface).	–
Session Summary — destination-prefix		
IP Prefix	Provides the option to enter destination IP prefix or IP address.	Enter the destination prefix address.
Session ID	Displays the number that identifies the session. Use this ID to get more information about the session.	–
Policy name	Displays the policy that permitted the traffic.	–
Timeout	Displays the idle timeout after which the session expires.	–
In	Displays the incoming flow (source and destination IP addresses, application protocol, and interface).	–
Out	Displays the reverse flow (source and destination IP addresses, application protocol, and interface).	–
Session Summary — interface		

Table 60: Flow Session Statistics Monitoring Page (continued)

Field	Value	Additional Information
Interface	Provides the option to enter interface details.	Enter the interface details.
Session ID	Displays the number that identifies the session. Use this ID to get more information about the session.	–
Policy name	Displays the policy that permitted the traffic.	–
Timeout	Displays the idle timeout after which the session expires.	–
In	Displays the incoming flow (source and destination IP addresses, application protocol, and interface).	–
Out	Displays the reverse flow (source and destination IP addresses, application protocol, and interface).	–
Session Summary — protocol		
Protocol	Provides the option to enter protocol details.	Enter the protocol details.
Session ID	Displays the number that identifies the session. Use this ID to get more information about the session.	–
Policy name	Displays the policy that permitted the traffic.	–
Timeout	Idle timeout after which the session expires.	–
In	Displays the incoming flow (source and destination IP addresses, application protocol, and interface).	–
Out	Displays the reverse flow (source and destination IP addresses, application protocol, and interface).	–

- See Also**
- [Monitoring IDP Status on page 96](#)
 - [Monitoring Flow Gate Information on page 100](#)

Flow Gate

- [Monitoring Flow Gate Information on page 100](#)

Monitoring Flow Gate Information

- Purpose** View information about temporary openings known as pinholes or gates in the security firewall.
- Action** Select **Monitor>Security>Flow Gate** in the J-Web user interface, or enter the **show security flow gate** command.

Table 61 on page 101 summarizes key output fields in the flow gate display.

Table 61: Summary of Key Flow Gate Output Fields

Field	Values	Additional Information
Flow Gate Information		
Hole	Range of flows permitted by the pinhole.	—
Translated	Tuples used to create the session if it matches the pinhole: <ul style="list-style-type: none"> • Source address and port • Destination address and port 	—
Protocol	Application protocol, such as UDP or TCP.	—
Application	Name of the application.	—
Age	Idle timeout for the pinhole.	—
Flags	Internal debug flags for pinhole.	—
Zone	Incoming zone.	—
Reference count	Number of resource manager references to the pinhole.	—
Resource	Resource manager information about the pinhole.	—

- See Also**
- [Monitoring Flow Session Statistics on page 97](#)
 - [Monitoring Firewall Authentication on page 101](#)

Authentication

- [Monitoring Firewall Authentication on page 101](#)
- [Monitoring Local Authentication on page 103](#)
- [Monitoring UAC Authentication on page 103](#)

Monitoring Firewall Authentication

Purpose Use the monitoring functionality to view the firewall authentication page.

Action To monitor firewall authentication, select **Monitor>Security>Firewall Authentication** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Monitor>Security>Authentication>Firewall Auth** in the J-Web user interface.

Meaning [Table 62 on page 102](#) summarizes key output fields in the firewall authentication page.

Table 62: Firewall Authentication Monitoring Page

Field	Value	Additional Information
Virtual Chassis Member	Displays the list of virtual chassis member.	Select one of the virtual chassis members listed.
Refresh Interval (30 sec)	Displays the time interval set for page refresh.	Select the time interval from the drop-down list.
Refresh	Displays the option to refresh the page.	–
Clear	Provides an option to clear the monitor summary.	Click Clear to clear the monitor summary.
User Table		
ID	Displays the authentication identification number.	–
Source IP	Displays the IP address of the authentication source.	–
Age	Displays the idle timeout for the user.	–
Status	Displays the status of authentication (success or failure).	–
User	Displays the name of the user.	–
History Table		
ID	Displays the identification number.	–
Source IP	Displays the IP address of the authentication source.	–
Duration	Displays the authentication duration.	–
Status	Displays the status of authentication (success or failure).	–
User	Displays the name of the user.	–

See Also

- [Monitoring Flow Gate Information on page 100](#)
- [Monitoring Flow Session Statistics on page 97](#)

Monitoring Local Authentication

Purpose Use the monitoring functionality to view the local authentication page.

Action To monitor local authentication, select **Monitor>Authentication>Local Auth** in the J-Web user interface.



NOTE:

- Starting in Junos OS Release 18.2R1, **Monitor>Authentication>Local Auth** option is enabled for logical system users.
- Starting in Junos OS Release 19.1R1, **Monitor>Authentication>Local Auth** option is enabled for tenant users.
- **Clear All** option is not available for both logical system and tenant users.

Meaning [Table 63 on page 103](#) summarizes key output fields in the local authentication page.

Table 63: Local Authentication Monitoring Page

Field	Value	Additional Information
Virtual Chassis Member	Displays the list of virtual chassis members.	Select one of the virtual chassis members listed.
Filter by	Displays the local authentication information based on the selected filter.	–
IP	Displays the IP address.	–
User Name	Displays the name of the user.	–
Role List	Displays the list of roles assigned to the username.	–

See Also

- [Monitoring Firewall Authentication on page 101](#)
- [Monitoring UAC Authentication on page 103](#)

Monitoring UAC Authentication

Purpose Use the monitoring functionality to view the UAC authentication page.

Action To monitor UAC authentication, select **Monitor>Security>Authentication>UAC Auth** in the J-Web user interface.

Meaning [Table 64 on page 104](#) summarizes key output fields in the UAC authentication page.

Table 64: UAC Authentication Monitoring Page

Field	Value	Additional Information
Filter by	Displays the UAC authentication value based on the selected filter.	–
ID	Displays the authentication identification number.	–
Source IP	Displays the IP address of the authentication source.	–
User Name	Displays the name of the user.	–
Age	Displays the idle timeout for the user.	–
Role List	Displays the list of roles assigned to the username.	–

See Also

- [Monitoring Firewall Authentication on page 101](#)
- [Monitoring Local Authentication on page 103](#)

Voice ALGs

- [Monitoring Voice ALG Summary on page 104](#)
- [Monitoring Voice ALG H.323 on page 105](#)
- [Monitoring Voice ALG MGCP on page 107](#)
- [Monitoring Voice ALG SCCP on page 110](#)
- [Monitoring Voice ALG SIP on page 113](#)

Monitoring Voice ALG Summary

Purpose Use the monitoring functionality to view the voice ALG summary page.

Action To monitor voice ALG summary, select **Monitor>Security>Voice ALGs>Summary** in the J-Web user interface.

Meaning [Table 65 on page 105](#) summarizes key output fields in the voice ALG summary page.

Table 65: Voice ALG Summary Monitoring Page

Field	Value	Additional Information
Virtual Chassis Member	Display the list of virtual chassis member.	Select one of the virtual chassis members listed.
Refresh Interval (30 sec)	Displays the time interval set for page refresh.	Select the time interval from the drop-down list.
Refresh	Displays the option to refresh the page.	–
Clear	Provides an option to clear the monitor summary.	Click Clear to clear the monitor summary.
Protocol Name	Displays the protocols configured.	–
Total Calls	Displays the total number of calls.	–
Number of Active Calls	Displays the number of active calls.	–
Number of Received Packets	Displays the number of packets received.	–
Number of Errors	Displays the number of errors.	–
H.323 Calls Chart	Displays the H.323 calls chart.	–
MGCP Calls Chart	Displays the MGCP calls chart.	–
SCCP Calls Chart	Displays the SCCP calls chart.	–
SIP Calls Chart	Displays the SIP calls chart.	–

- See Also**
- [Monitoring Voice ALG H.323 on page 105](#)
 - [Monitoring Voice ALG MGCP on page 107](#)
 - [Monitoring Voice ALG SCCP on page 110](#)
 - [Monitoring Voice ALG SIP on page 113](#)

Monitoring Voice ALG H.323

Purpose Use the monitoring functionality to view the ALG H.323 page.

Action To monitor ALG H.323 select **Monitor>Security>Voice ALGs>H.323** in the J-Web user interface.

Meaning [Table 66 on page 106](#) summarizes key output fields in the ALG H.323 page.

Table 66: ALG H.323 Monitoring Page

Field	Value	Additional Information
Virtual Chassis Member	Display the list of virtual chassis member.	Select one of the virtual chassis members listed.
Refresh Interval (30 sec)	Displays the time interval set for page refresh.	Select the time interval from the drop-down list.
Refresh	Displays the option to refresh the page.	—
Clear	Provides an option to clear the monitor summary.	Click clear to clear the monitor summary.

H.323 Counter Summary

Category	Displays the following categories:	—
	<ul style="list-style-type: none"> • Packets received—Number of ALG H.323 packets received. • Packets dropped—Number of ALG H.323 packets dropped. • RAS message received—Number of incoming RAS (Registration, Admission, and Status) messages per second per gatekeeper received and processed. • Q.931 message received—Counter for Q.931 message received. • H.245 message received—Counter for H.245 message received. • Number of calls—Total number of ALG H.323 calls. • Number of active calls—Number of active ALG H.323 calls. • Number of DSCP Marked—Number of DSCP Marked on ALG H.323 calls. 	
Count	Provides count of response codes for each H.323 counter summary category.	—

H.323 Error Counter

Category	Displays the following categories:	—
	<ul style="list-style-type: none"> • Decoding errors—Number of decoding errors. • Message flood dropped—Error counter for message flood dropped. • NAT errors—H.323 ALG NAT errors. • Resource manager errors—H.323 ALG resource manager errors. • DSCP Marked errors—H.323 ALG DSCP marked errors. 	
Count	Provides count of response codes for each H.323 error counter category.	—

Counter Summary Chart

Table 66: ALG H.323 Monitoring Page (continued)

Field	Value	Additional Information
Packets Received	Provides the graphical representation of the packets received.	—
H.323 Message Counter		
Category	Displays the following categories: <ul style="list-style-type: none"> • RRQ—Registration Request message counter. • RCF—Registration Confirmation Message. • ARQ—Admission Request message counter. • ACF—Admission Confirmation • URQ—Unregistration Request. • UCF—Unregistration Confirmation. • DRQ—Disengage Request. • DCF—Disengage Confirmation. • Oth RAS—Other incoming Registration, Admission, and Status messages message counter. • Setup—Timeout value, in seconds, for the response of the outgoing setup message. • Alert—Alert message type. • Connect—Connect setup process. • CallProd—Number of call production messages sent. • Info—Number of info requests sent. • RelCmpl—Number of Rel Cmpl message ssent. • Facility—Number of facility messages sent. • Empty—Empty capabilities to the support message counter. • OLC—Open Local Channel message counter. • OLC ACK—Open Local Channel Acknowledge message counter. • Oth H245—Other H.245 message counter 	—
Count	Provides count of response codes for each H.323 message counter category.	—

- See Also**
- [Monitoring Voice ALG Summary on page 104](#)
 - [Monitoring Voice ALG MGCP on page 107](#)
 - [Monitoring Voice ALG SCCP on page 110](#)
 - [Monitoring Voice ALG SIP on page 113](#)

Monitoring Voice ALG MGCP

Purpose Use the monitoring functionality to view the voice ALG MGCP page.

Action To monitor ALG MGCP, select **Monitor>Security>Voice ALGs>MGCP** in the J-Web user interface.

Meaning [Table 67 on page 108](#) summarizes key output fields in the voice ALG MGCP page.

Table 67: Voice ALG MGCP Monitoring Page

Field	Value	Additional Information
Virtual Chassis Member	Displays the list of virtual chassis member.	Select one of the virtual chassis members listed.
Refresh Interval (30 sec)	Displays the time interval set for page refresh.	Select the time interval from the drop-down list.
Refresh	Displays the option to refresh the page.	—
Clear	Provides an option to clear the monitor summary.	Click Clear to clear the monitor summary.

Counters		
MGCP Counters Summary		
Category	Displays the following categories: <ul style="list-style-type: none"> • Packets Received—Number of ALG MGCP packets received. • Packets Dropped— Number of ALG MGCP packets dropped. • Message received— Number of ALG MGCP messages received. • Number of connections— Number of ALG MGCP connections. • Number of active connections— Number of active ALG MGCP connections. • Number of calls— Number of ALG MGCP calls. • Number of active calls— Number of active ALG MGCP calls. • Number of active transactions— Number of active transactions. • Number of transactions— Number of transactions. • Number of re-transmission—Number of ALG MGCP retransmissions. • Number of active endpoints— Number of MGCP active endpoints. • Number of DSCP marked— Number of MGCP DSCPs marked. 	—
Count	Provides the count of response codes for each MGCP counter summary category.	—

Table 67: Voice ALG MGCP Monitoring Page (continued)

Field	Value	Additional Information
MGCP Error Counter		
Category	Displays the following categories: <ul style="list-style-type: none"> • Unknown-method— MGCP ALG unknown method errors. • Decoding error— MGCP ALG decoding errors. • Transaction error— MGCP ALG transaction errors. • Call error— MGCP ALG call ounter errors. • Connection error— MGCP ALG connection errors. • Connection flood drop— MGCP ALG connection flood drop errors. • Message flood drop— MGCP ALG message flood drop error. • IP resolve error— MGCP ALG IP address resolution errors. • NAT error— MGCP ALG NAT errors. • Resource manager error— MGCP ALG resource manager errors. • DSCP Marked error— MGCP ALG DSCP marked errors. 	—
Count	Provides the count of response codes for each summary error counter category.	—
Counter Summary Chart	Displays the Counter Summary Chart.	—
MGCP Packet Counters		
Category	Displays the following categories: <ul style="list-style-type: none"> • CRCX— Create Connection • MDCX— Modify Connection • DLCX— Delete Connection • AUEP— Audit Endpoint • AUCX— Audit Connection • NTFY— Notify MGCP • RSIP— Restart in Progress • EPCF— Endpoint Configuration • RQNT— Request for Notification • 000-199—Respond code is 0-199 • 200-299—Respond code is 200-299 • 300-399—Respond code is 300-399 	—
Count	Provides count of response codes for each MGCP packet counter category.	—

Table 67: Voice ALG MGCP Monitoring Page (continued)

Field	Value	Additional Information
Calls		
Endpoint@GW	Displays the endpoint name.	—
Zone	Displays the following options: <ul style="list-style-type: none"> • trust—Trust zone. • untrust—Untrust zone. 	—
Endpoint IP	Displays the endpoint IP address.	—
Call ID	Displays the call identifier for ALG MGCP.	—
RM Group	Displays the resource manager group ID.	—
Call Duration	Displays the duration for which connection is active.	—

- See Also**
- [Monitoring Voice ALG Summary on page 104](#)
 - [Monitoring Voice ALG H.323 on page 105](#)
 - [Monitoring Voice ALG SCCP on page 110](#)
 - [Monitoring Voice ALG SIP on page 113](#)

Monitoring Voice ALG SCCP

Purpose Use the monitoring functionality to view the voice ALG SCCP page.

Action To monitor voice ALG SCCP, select **Monitor>Security>Voice ALGs>SCCP** in the J-Web user interface.

Meaning [Table 68 on page 110](#) summarizes key output fields in the voice ALG SCCP page.

Table 68: Voice ALG SCCP Monitoring Page

Field	Value	Additional Information
Virtual Chassis Member	Displays the list of virtual chassis member.	Select one of the virtual chassis members listed.
Refresh Interval (30 sec)	Displays the time interval set for page refresh.	Select the time interval from the drop-down list.
Refresh	Displays the option to refresh the page.	—

Table 68: Voice ALG SCCP Monitoring Page (continued)

Field	Value	Additional Information
Clear	Provides an option to clear the monitor summary.	Click Clear to clear the monitor summary.
SCCP Call Statistics		
Category	Displays the following categories: <ul style="list-style-type: none"> • Active client sessions— Number of active SCCP ALG client sessions. • Active calls— Number of active SCCP ALG calls. • Total calls— Total number of SCCP ALG calls. • Packets received— Number of SCCP ALG packets received. • PDUs processed— Number of SCCP ALG protocol data units (PDUs) processed. • Current call rate— Number of calls per second. • DSCPs Marked— Number of DSCP marked. 	—
Count	Provides count of response codes for each SCCP call statistics category.	—
Call Statistics Chart	Displays the Call Statistics chart.	—
SCCP Error Counters		

Table 68: Voice ALG SCCP Monitoring Page (continued)

Field	Value	Additional Information
Category	Displays the following categories: <ul style="list-style-type: none"> • Packets dropped— Number of packets dropped by the SCCP ALG. • Decode errors— Number of SCCP ALG decoding errors. • Protocol errors— Number of protocol errors. • Address translation errors— Number of NAT errors encountered by SCCP ALG. • Policy lookup errors— Number of packets dropped because of a failed policy lookup. • Unknown PDUs— Number of unknown PDUs. • Maximum calls exceed— Number of times the maximum SCCP calls limit was exceeded. • Maximum call rate exceed— Number of times the maximum SCCP call rate was exceeded. • Initialization errors— Number of initialization errors. • Internal errors— Number of internal errors. • Nonspecific errors— Number of nonspecific errors. • No active calls to be deleted— Number of no active calls to be deleted. • No active client sessions to be deleted— Number of no active client sessions to be deleted. • Session cookie created error— Number of session cookie created errors. • Invalid NAT cookies deleted— Number of invalid NAT cookies deleted. • NAT cookies not found— Number of NAT cookies not found. • DSCP Marked Error— Number of DSCP marked errors. 	—
Count	Provides count of response codes for each SCCP error counter category.	—
Calls		
Client IP	Displays the IP address of the client.	—
Zone	Displays the client zone identifier.	—
Call Manager	Displays the IP address of the call manager.	—
Conference ID	Displays the conference call identifier.	—
RM Group	Displays the resource manager group identifier.	—

See Also • [Monitoring Voice ALG Summary on page 104](#)

- [Monitoring Voice ALG H.323 on page 105](#)
- [Monitoring Voice ALG MGCP on page 107](#)
- [Monitoring Voice ALG SIP on page 113](#)

Monitoring Voice ALG SIP

Purpose Use the monitoring functionality to view the voice ALG SIP page.

Action To monitor voice ALG SIP select **Monitor>Security>Voice ALGs>SIP** in the J-Web user interface.

Meaning [Table 69 on page 113](#) summarizes key output fields in the voice ALG SIP page.

Table 69: Voice ALG SIP Monitoring Page

Field	Value	Additional Information
Virtual Chassis Member	Displays the list of virtual chassis members.	Select one of the virtual chassis members listed.
Refresh Interval (30 sec)	Displays the time interval set for page refresh.	Select the time interval from the drop-down list.
Refresh	Displays the option to refresh the page.	—
Clear	Provides an option to clear the monitor summary.	Click Clear to clear the monitor summary.

Counters

SIP Counters Information

Table 69: Voice ALG SIP Monitoring Page (continued)

Field	Value	Additional Information
Method	<p>Displays the SIP counter information. The available options are:</p> <ul style="list-style-type: none"> • BYE— Number of BYE requests sent. A user sends a BYE request to abandon a session. A BYE request from either user automatically terminates the session. • REGISTER— Number of REGISTER requests sent. A user sends a REGISTER request to a SIP registrar server to inform it of the current location of the user. The SIP registrar server records all the information it receives in REGISTER requests and makes this information available to any SIP server attempting to locate a user. • OPTIONS— Number of OPTIONS requests sent. An OPTION message is used by the User Agent (UA) to obtain information about the capabilities of the SIP proxy. A server responds with information about what methods, session description protocols, and message encoding it supports. • INFO— Number of INFO requests sent. An INFO message is used to communicate mid-session signaling information along the signaling path for the call. • MESSAGE— Number of MESSAGE requests sent. SIP messages consist of requests from a client to the server and responses to the requests from the server to a client for the purpose of establishing a session (or a call). 	—

SIP Counters Information (continued)

Table 69: Voice ALG SIP Monitoring Page (continued)

Field	Value	Additional Information
Method	<ul style="list-style-type: none"> • NOTIFY— Number of NOTIFY requests sent. A NOTIFY message is sent to inform subscribers about the change in state of the subscription. • PRACK— Number of PRACK requests sent. The PRACK request plays the same role as the ACK request, but for provisional responses. • PUBLISH— Number of PUBLISH requests sent. The PUBLISH request is used for publishing the event state. PUBLISH is similar to REGISTER that allows a user to create, modify, and remove state in another entity which manages this state on behalf of the user. • REFER— Number of REFER requests sent. A REFER request is used to refer the recipient (identified by the Request-URI) to a third party identified by the contact information provided in the request. • SUBSCRIBE— Number of SUBSCRIBE requests sent. A SUBSCRIBE request is used to request current state and state information updates from a remote node. • UPDATE— Number of UPDATE requests sent. An UPDATE request is used to create a temporary opening in the firewall (pinhole) for new or updated Session Description Protocol (SDP) information. The following header fields are modified: Via, From, To, Call-ID, Contact, Route, and Record-Route. • BENOTIFY— Number of BENOTIFY requests sent. A BENOTIFY request is used to reduce the unnecessary SIP signaling traffic on application servers. Applications that do not need a response for a NOTIFY request can enhance performance by enabling BENOTIFY. • SERVICE— Number of SERVICE requests sent. The SERVICE method is used by a SIP client to request a service from a SIP server. It is a standard SIP message and will be forwarded until it reaches the server or end user that is performing the service. • OTHER— Number of OTHER requests sent. 	—
T, RT	Displays the transmit and retransmit method.	—
1xx, RT	Displays one transmit and retransmit method.	—
2xx, RT	Displays two transmit and retransmit methods.	—
3xx, RT	Displays three transmit and retransmit methods.	—
4xx, RT	Displays four transmit and retransmit methods.	—
5xx, RT	Displays five transmit and retransmit methods.	—
6xx, RT	Displays six transmit and retransmit methods.	—
Calls		
Call ID	Displays the call ID.	—

Table 69: Voice ALG SIP Monitoring Page (continued)

Field	Value	Additional Information
Method	Displays the call method used.	—
State	Displays the state of the ALG SIP.	—
Group ID	Displays the group identifier.	—
Invite Method Chart	Displays the invite method chart. The available options are: <ul style="list-style-type: none">• T/RT• 1xx/ RT• 2xx/ RT• 3xx/ RT• 4xx/ RT• 5xx/ RT• 6xx/ RT	—

SIP Error Counters

Table 69: Voice ALG SIP Monitoring Page (continued)

Field	Value	Additional Information
Category	<p>Displays the SIP error counters. The available options are:</p> <ul style="list-style-type: none"> • Total Pkt-in— Number of SIP ALG total packets received. • Total Pkt dropped on error— Number of packets dropped by the SIP ALG. • Call error— SIP Number of ALG call errors. • IP resolve error— Number of SIP ALG IP address resolution errors. • NAT error— SIP Number of ALG NAT errors. • Resource manager error— Number of SIP ALG resource manager errors. • RR header exceeded max— Number of times the SIP ALG RR (Record-Route) headers exceeded the maximum limit. • Contact header exceeded max— Number of times the SIP ALG contact header exceeded the maximum limit. • Call dropped due to limit— Number of SIP ALG calls dropped because of call limits. • SIP stack error— Number of SIP ALG stack errors. • SIP Decode error— Number of SIP ALG decode errors. • SIP unknown method error— Number of SIP ALG unknow method errors. • SIP DSCP marked—SIP ALG DSCP marked. • SIP DSCP marked error— Number of SIP ALG DSCPs marked. • RTO message sent— Number of SIP ALG marked RTO messages sent. • RTO message received— Number of SIP ALG RTO messages received. • RTO buffer allocation failure— Number of SIP ALG RTO buffer allocation failures. • RTO buffer transmit failure— Number of SIP ALG RTO buffer transmit failures. • RTO send processing error— Number of SIP ALG RTO send processing errors. • RTO receiving processing error— Number of SIP ALG RTO receiving processing errors. • RTO receive invalid length— Number of SIP ALG RTOs receiving invalid length. • RTO receive call process error— Number of SIP ALG RTO receiving call process errors. • RTO receive call allocation error— Number of SIP ALG RTO receiving call allocation error. • RTO receive call register error— Number of SIP ALG RTO receiving call register errors. • RTO receive invalid status error— Number of SIP ALG RTO receiving register errors. 	—
Count	Provides count of response codes for each SIP ALG counter category.	—

- See Also**
- [Monitoring Voice ALG Summary on page 104](#)
 - [Monitoring Voice ALG H.323 on page 105](#)
 - [Monitoring Voice ALG MGCP on page 107](#)
 - [Monitoring Voice ALG SCCP on page 110](#)

Application Firewall

- [Monitoring Application Firewalls on page 118](#)

Monitoring Application Firewalls

Purpose Use the monitoring functionality to view the application firewall page. Applications can breach IP and port-based security policies by accessing standard HTTP ports 80 and 443 to tunnel non-HTTP traffic or by using ports other than 80 or 443 for HTTP traffic. An application firewall screens traffic based on an application signature rather than IP or port address. The implementation of both application firewall and network firewall policies contributes to the full security of the network.

Action To monitor application firewall select **Monitor>Security>Application FW**.

The upper pane of the Application Firewall Monitoring page provides a list of the rule sets currently configured on your device. When you select a rule set in the upper pane, the lower panes display the rules and counters associated with that rule set. Each rule entry identifies dynamic application signatures for match criteria and the action to be taken with an application signature match.

The counter pane maintains current statistics about the actions taken for the application signatures that are encountered. The Clear Counters button resets all counters to zero and begins counting again. After the number of seconds specified in the Refresh Interval has expired, the new counter values are displayed.

Meaning [Table 70 on page 118](#) summarizes key output fields in the application firewall page.

Table 70: Application firewall Monitoring Page

Field	Value	Additional Information
Rule Set		
Name	Displays the rule sets configured for the device.	Select a rule set to display its associated rules and counters in the lower panes.
Default Rule	Displays the action taken when traffic does not match any of the associated rules. <ul style="list-style-type: none"> • permit—Permits all traffic that does not match any rule in the rule set. • deny—Denies all traffic that does not match any rule in the rule set. 	—

Table 70: Application firewall Monitoring Page (continued)

Field	Value	Additional Information
Rules	Displays the rule names associated with the rule set.	—
Rules in Selected Rule Set		
Rule Name	Lists the names of the rules included in the rule set.	—
Match Dynamic Applications	Displays the dynamic applications used as match criteria for the associated rule.	—
Action	Displays the action to be taken if the traffic matches the associated rule's match criteria. <ul style="list-style-type: none"> • permit—Permits traffic that matches the rule. • deny—Denies traffic that matches the rule. 	—
Counters for Selected Rule-Set		
Refresh interval (sec)	Specifies the interval in seconds when counter values are refreshed.	—
Counter	Displays the counter for rule in the rule set	—
Value	Displays the value for rule in the rule set	—

See Also • [Monitoring 802.1x](#)

Application Tracking

- [Monitoring Application Statistics \(Application Tracking\)](#) on page 119

Monitoring Application Statistics (Application Tracking)

Purpose Use the Application Tracking functions to monitor sessions and bytes of a particular application or application group.

Action To monitor and track applications, select **Monitor>Security>Application Tracking** in the J-Web user interface.



NOTE: If application tracking is disabled, the Application Tracking page is also disabled. To enable application tracking, select **Configure>Security>Logging** in the J-Web user interface.

Meaning Table 71 on page 120 summarizes key output fields in the Application Tracking page.

Table 71: Application Tracking Monitoring Page

Field	Value	Additional Information
Risk	Displays the risk as critical, moderate, low, or unsafe. The risk factor is based on the predefined security standard. NOTE: Risk is displayed only for applications.	—
Name	Displays the name of the application or application group.	—
# Sessions	Displays the number of active sessions.	—
Traffic	Displays the application or application group traffic in kilobytes.	—
Session %	Displays the session percentage of the current application or application groups.	—
Traffic %	Displays the traffic percentage of the application or application groups.	—
Selected Statistics		
Cumulative	Refers to the statistics that are collected from the last clearing time specified to the current time.	—
Time Interval	Enables you to set an interval of time during which statistics are collected. You can specify the time interval in minutes, hours, or days. The default is 1 minute.	For example, if you set 5 minutes as the time interval at 13:00 hours, then statistics are collected from 13:00 to 13:05.
Details		
Time Interval Began	If Cumulative is selected, this field displays the last reset time that was set. If Time Interval is selected, this field displays the last interval that was set.	—
Elapsed Time	Displays the time elapsed since the last time interval began.	—
Clear	If Cumulative is selected, the cumulative statistics are cleared. If Time Interval is selected, the statistics collected during the last specified interval are cleared.	You are prompted to confirm that you want to clear the statistics.
View		

Table 71: Application Tracking Monitoring Page (continued)

Field	Value	Additional Information
Switch to Grid	In the grid view, data is displayed in a table.	By default, application tracking statistics are displayed in the grid view.
Switch to Graphical	<p>In the graphical view, data is displayed in a chart. The two types of charts supported are:</p> <ul style="list-style-type: none"> • Bar • Pie <p># Displayed – Enables you to set the number of applications or application groups to be displayed in the chart. The maximum number allowed is 10, and the default is 3.</p> <p>Display order – Enables you to sort the application and application groups in ascending or descending order. By default, applications are displayed in descending order.</p> <p>Display by – Enables you to filter the display of applications and application groups by the following:</p> <ul style="list-style-type: none"> • # Sessions • Session % • Traffic • Traffic % 	Bar chart is the default.
Refresh Display	Click Refresh Display to retrieve the most current data.	–
Settings	<p>Enables you to set some additional options. You can set the following:</p> <ul style="list-style-type: none"> • Display Refresh Interval - Enables you to set the interval for refreshing. You can specify a refresh time from 1 minute to 24 hours. The default is 1 minute. • Display Columns – Enables you to select the columns you want to display in the output. <p>NOTE: The Display Columns option is available only in the grid view.</p>	–

Filter By

Table 71: Application Tracking Monitoring Page (continued)

Field	Value	Additional Information
Application	Enables you to collect application level statistics.	You can filter application or application group statistics by the following:
Application Group	Enables you to collect application group statistics.	<ul style="list-style-type: none"> • Name (default filter) Filters the application or application groups by the name specified. Contains and Exact Match filters are supported. • # Session • Session % • Traffic • Traffic %
Add to Results	Adds the filtered results to the output.	—

See Also • [Security Logging Configuration Page Options on page 185](#)

DS-Lite

- [Monitoring DS-Lite on page 122](#)

Monitoring DS-Lite

Purpose Use the monitoring functionality to view the DS-Lite page.

Action To monitor DS-Lite select **Monitor>Security>DS-Lite** in the J-Web user interface.

Meaning [Table 72 on page 122](#) summarizes key output fields on the DS-Lite page.

Table 72: DS-Lite Monitoring Page

Field	Value	Additional Information
Virtual Chassis Member	Displays the virtual chassis of the device	—
Refresh Interval	Displays the time interval for page refresh.	Select the time interval from the list.
General Info		
Name	Displays the name of the DS-Lite configuration.	—
Address	Displays the IP address of the device.	—

Table 72: DS-Lite Monitoring Page (continued)

Field	Value	Additional Information
Status	Displays the status of the DS-Lite configuration. <ul style="list-style-type: none"> • Connected—DS-Lite configuration is connected. • Disconnected—DS-Lite configuration is not connected. 	—
Num of softwire initiator	Displays the number of softwire initiators connected to the device.	—
Softwire Initiator from Selected Item		
Address	Displays the IP address of the softwire of the selected DS-Lite configuration.	—
Status	Displays the status of the softwire initiator. <ul style="list-style-type: none"> • Active—The softwire initiator is active. • Inactive—The softwire initiator is inactive. 	The status types displayed are active and inactive.
spu-id	Displays the identification number of the Services Processing Unit.	—

See Also • [DS-Lite Configuration Page Options on page 465](#)

AppQoS

- [Monitoring AppQoS on page 123](#)

Monitoring AppQoS

Purpose Use the Application QoS Monitoring page to view counters and statistics for AppQoS activity.

Action To monitor AppQoS, select **Monitor>Security>Application QoS**.

Refresh—Updates the display with current information. The refresh limit updates the display automatically at the interval specified. To change the refresh rate, select the number of seconds in the Refresh interval (sec) field.

Clear statistics—Clears the statistics in the associated pane.

Clear counter—Resets the counters to 0 in the associated pane.

Meaning The rate limiters statistics pane displays transfer rate information for recent traffic per PIC. For a summary of this pane, refer to [Table 73 on page 124](#).

The rules statistics pane displays the amount of traffic on each PIC broken down by the rule set and rule applied to each session. For a summary of this pane, refer to [Table 74 on page 124](#).

Counters for Selected Rule-Set pane displays AppQoS session activity per PIC. For a summary of this pane, refer to [Table 75 on page 124](#).

Table 73: Rate limiter statistics Pane

Field	Value	Additional Information
PIC	PIC for which the AppQoS settings of the most recent sessions are displayed.	Select the PIC to display AppQoS rate-limiter information for its recent traffic.
Rule-set Name	Name of the rule set applied to each session.	—
Application	Applications associated with the applied rule set.	—
Client2server rate limiter	Name of the rate limiter applied in the client-to-server direction.	—
Rate (bps)	Maximum transfer rate specified for the client-to-server rate limiter.	—
Server2client rate limiter	Name of the rate limiter applied in the server-to-client direction.	—
Rate (bps)	Maximum transfer rate specified for the server-to-client rate limiter.	—

Table 74: Rules statistics Pane

Field	Value	Additional Information
PIC	PIC for which the rule statistics are displayed.	Select the PIC to display the number of times each AppQoS rule set and rule are applied on this PIC.
Rule- set name	Name of the rule set applied to each session.	—
Rule name	Name of the rule in the rule set.	—
Hits	Number of occurrences when this rule has been matched and applied.	—

Table 75: Counters for Selected Rule-Set Pane

Field	Value	Additional Information
PIC	PIC number for which the AppQoS counts apply.	—

Table 75: Counters for Selected Rule-Set Pane (continued)

Field	Value	Additional Information
Sessions processed	The number of sessions processed on the PIC.	–
Sessions marked	The number of sessions where the DSCP setting was marked.	–
Sessions honored	The number of sessions where an existing DSCP setting was honored.	–
Sessions rate limited	The number of sessions that were rate limited.	–
Client2server flows rate limited	The number of client-to-server flows that were rate limited.	–
Server2client flows rate limited	The number of server-to-client flows that were rate limited.	–

See Also • [Monitoring IPsec VPN—Phase I on page 128](#)

Threat Prevention

- [Monitoring Threat Prevention—Diagnostics on page 125](#)
- [Monitoring Threat Prevention—Statistics on page 126](#)

Monitoring Threat Prevention—Diagnostics

Purpose Juniper Sky Advanced Threat Prevention (ATP) uses real-time information from the cloud to provide your business with anti-malware protection.

The monitoring functionality is use to view and diagnose threat prevention policies.

[Table 76 on page 125](#) examines the content present in the page.

Action To monitor and diagnose threat prevention policies select **Monitor > Security Services > Sky ATP > Diagnostics** in the J-Web user interface.

Meaning Summarizes key output fields on the page.

Table 76: Diagnostics page option

Field	Value	Additional Information
Diagnostics		
SKY ATP Diagnostics	Specify to diagnose.	Select an option from the drop down list.

Table 76: Diagnostics page option (continued)

Field	Value	Additional Information
Diagnostics Logs	Displays the diagnostic logs for the selected option.	-
Check Connectivity		
Check	Check the connectivity.	Click on the Check .
Server Details		
Server hostname	Specify the host name of the server.	-
Server realm	Specifies the name of a server realm.	-
Server port	Specify the server port number.	-
Connection Plane		
Connection time	Specify the connection time of the server.	-
Connection Status	Specify the connection status.	-
Service Plane		
Card Info	Specify the card number.	-
Connection Active Number	Specify the connection active numbers.	-
Connection Relay statistics	Specify the connection relay statistics.	-
Other Details		
Configured Proxy Server	Specify the configured proxy server.	-
Port Number	Specify the port number of the proxy server.	-

Monitoring Threat Prevention—Statistics

Purpose Use this page to verify the statistics of advanced-anti-malware sessions and security Intelligence sessions

Action To monitor and diagnose threat prevention policies select **Monitor>Security Services >SKY ATP >Statistics** in the J-Web user interface.

[Table 77 on page 127](#) examines the content present in the field.

Meaning Summarizes key output fields on the Statistics page.

Table 77: Statistics Page options

Field	Value	Additional Information
Advanced Anti Malware Session Statistics		
TOTAL	Specify the TOTAL Session.	-
HTTP	Specify the HTTP Session.	-
HTTPS	Specify the HTTP Session.	-
SMTP	Specify the simple mail transfer protocol session.	-
SMTPS	Specify SMTPS seesion.	-
Clear Staistics	Clear the statistics.	-
Sessions		
activities	Specify the total session activities.	-
blocked	Specify the blocked session.	-
permitted	Specify the permitted session .	-
Security Intelligence Session Statistics		
Profiles	Displays the IP address of the softwire of the selected DS-Lite configuration.	-
Sessions		
TOTAL	Displays the identification number of the Services Processing Unit.	-
PERMIT	Specify the permitted session.	-
BLOCK-DROP	Specify the block drop.	-
BLOCK-CLOSE	Specify the block close.	-
CLOSE-REDIRECT	Specify the closure of the redirect session.	-
Clear Statistics	Clear the statistics.	-

IPsec VPN

- [Monitoring IPsec VPN—Phase I on page 128](#)
- [Monitoring IPsec VPN—Phase II on page 129](#)

Monitoring IPsec VPN—Phase I

Purpose View IPsec VPN Phase I information.

Action Select **Monitor>IPSec VPN>Phase I** in the J-Web user interface.

[Table 78 on page 128](#) describes the available options for monitoring IPsec VPN-Phase I.

Table 78: IPsec VPN—Phase I Monitoring Page

Field	Values	Additional Information
IKE SA Tab Options		
IKE Security Associations		
SA Index	Index number of an SA.	—
Remote Address	IP address of the destination peer with which the local peer communicates.	—
State	State of the IKE security associations: <ul style="list-style-type: none"> DOWN—SA has not been negotiated with the peer. UP—SA has been negotiated with the peer. 	—
Initiator Cookie	Random number, called a cookie, which is sent to the remote node when the IKE negotiation is triggered.	—
Responder Cookie	Random number generated by the remote node and sent back to the initiator as a verification that the packets were received.	A cookie is aimed at protecting the computing resources from attack without spending excessive CPU resources to determine the cookie's authenticity.

Table 78: IPsec VPN—Phase I Monitoring Page (continued)

Field	Values	Additional Information
Mode	<p>Negotiation method agreed upon by the two IPsec endpoints, or peers, used to exchange information. Each exchange type determines the number of messages and the payload types that are contained in each message. The modes, or exchange types, are:</p> <ul style="list-style-type: none"> • Main—The exchange is done with six messages. This mode, or exchange type, encrypts the payload, protecting the identity of the neighbor. The authentication method used is displayed: preshared keys or certificate. • Aggressive—The exchange is done with three messages. This mode, or exchange type, does not encrypt the payload, leaving the identity of the neighbor unprotected. 	—

See Also • [Monitoring IPsec VPN—Phase II on page 129](#)

Monitoring IPsec VPN—Phase II

Purpose View IPsec VPN Phase II information.

Action Select **Monitor>IPSec VPN>Phase II** in the J-Web user interface.

[Table 79 on page 129](#) describes the available options for monitoring IPsec VPN-Phase II.

Table 79: IPsec VPN—Phase II Monitoring Page

Field	Values	Additional Information
Statistics Tab Details		
By bytes	Provides total number of bytes encrypted and decrypted by the local system across the IPsec tunnel.	—
By packets	Provides total number of packets encrypted and decrypted by the local system across the IPsec tunnel.	—
IPsec Statistics	Provides details of the IPsec statistics.	—
IPsec SA Tab Details		
IPsec Security Associations		
ID	Index number of the SA.	—

Table 79: IPsec VPN—Phase II Monitoring Page (continued)

Field	Values	Additional Information
Gateway/Port	IP address of the remote gateway/port.	—
Algorithm	<p>Cryptography scheme used to secure exchanges between peers during the IKE Phase II negotiations:</p> <ul style="list-style-type: none"> An authentication algorithm used to authenticate exchanges between the peers. Options are hmac-md5-95 or hmac-sha1-96. 	—
SPI	<p>Security parameter index (SPI) identifier. An SA is uniquely identified by an SPI. Each entry includes the name of the VPN, the remote gateway address, the SPIs for each direction, the encryption and authentication algorithms, and keys. The peer gateways each have two SAs, one resulting from each of the two phases of negotiation: Phase I and Phase II.</p>	—
Life	The lifetime of the SA, after which it expires, expressed either in seconds or kilobytes.	—
Monitoring	Specifies if VPN-Liveliness Monitoring has been enabled/disabled. Enabled - 'U ', Disabled- '—'	—
Vsys	Specifies the root system.	—

See Also • [Monitoring IPsec VPN—Phase I on page 128](#)

Ethernet Switching

- [Monitoring Ethernet Switching on page 130](#)
- [Monitoring Spanning Tree on page 132](#)
- [Monitoring IGMP Snooping on page 133](#)
- [Monitoring GVRP on page 134](#)

Monitoring Ethernet Switching

Purpose Use the monitoring functionality to view the Ethernet switching page.

Action To monitor Ethernet switching, select **Monitor>Switching>Ethernet Switching** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Monitor>Ethernet Switching** in the J-Web user interface.

Meaning [Table 80 on page 131](#) summarizes key output fields in the Ethernet switching page.

Table 80: Ethernet Switching Monitoring Page

Field	Value	Additional Information
Ethernet Switching Table Information		
VLAN	The VLAN for which Ethernet switching is enabled.	—
MAC Address	The MAC address associated with the VLAN. If a VLAN range has been configured for a VLAN, the output displays the MAC addresses for the entire series of VLANs that were created with that name.	—
Type	The type of MAC address. Values are: <ul style="list-style-type: none"> static—The MAC address is manually created. learn—The MAC address is learned dynamically from a packet's source MAC address. flood—The MAC address is unknown and flooded to all members. 	—
Age	The time remaining before the entry ages out and is removed from the Ethernet switching table.	—
Interfaces	Interface associated with learned MAC addresses or All-members (flood entry).	—
MAC Learning Log		
VLAN-ID	Displays the VLAN ID.	—
MAC Address	Displays the learned MAC address.	—
Time	Displays timestamp when the MAC address was added or deleted from the log.	—
State	Indicates the MAC address learned on the interface.	—

See Also

- [Monitoring Spanning Tree on page 132](#)
- [Monitoring GVRP on page 134](#)

Monitoring Spanning Tree

Purpose Use the monitoring functionality to view the Spanning Tree page.

Action To monitor spanning tree, select **Monitor>Switching>Spanning Tree** in the J-Web user interface.

Meaning [Table 81 on page 132](#) summarizes key output fields in the spanning tree page.

Table 81: Spanning Tree Monitoring Page

Field	Value	Additional Information
Bridge parameters		
Context ID	An internally generated identifier.	—
Enabled Protocol	Spanning tree protocol type enabled.	—
Root ID	Bridge ID of the elected spanning tree root bridge.	The bridge ID consists of a configurable bridge priority and the MAC address of the bridge.
Bridge ID	Locally configured bridge ID.	—
Inter instance ID	An internally generated instance identifier.	—
Extended system ID	Extended system generated instance identifier.	—
Maximum age	Maximum age of received bridge protocol data units (BPDUs).	—
Number of topology changes	Total number of STP topology changes detected since the switch last booted.	—
Forward delay	Spanning tree forward delay.	—
Interface List		
Interface Name	Interface configured to participate in the STP instance.	—
Port ID	Logical interface identifier configured to participate in the STP instance.	—
Designated Port ID	Port ID of the designated port for the LAN segment to which the interface is attached.	—
Port Cost	Configured cost for the interface.	—

Table 81: Spanning Tree Monitoring Page (continued)

Field	Value	Additional Information
State	STP port state. Forwarding (FWD), blocking (BLK), listening, learning, or disabled.	–
Role	MSTP or RSTP port role. Designated (DESG), backup (BKUP), alternate (ALT), or root.	–

- See Also**
- [Monitoring Ethernet Switching](#)
 - [Monitoring GVRP on page 134](#)

Monitoring IGMP Snooping

Purpose Use the monitoring functionality to view the IGMP Snooping page.

Action To display IGMP snooping details in the J-Web user interface, select **Monitor>Switching>IGMP Snooping**.

To display IGMP snooping details in the CLI, enter the following commands:

- **show igmp-snooping route**
- **show igmp-snooping statistics**
- **show igmp-snooping vlans**

Meaning [Table 82 on page 133](#) summarizes the IGMP snooping details displayed.

Table 82: Summary of IGMP Snooping Output Fields

Field	Values
IGMP Snooping Monitor	
VLAN	The VLAN for which IGMP snooping is enabled.
Interfaces	Indicates the interfaces configured as switching interfaces that are associated with the multicast router.
Groups	Indicates the number of the multicast groups learned by the VLAN.
MRouters	Specifies the multicast router.
Receivers	Specifies the multicast receiver.
IGMP Route Information	
VLAN	The VLAN for which IGMP snooping is enabled.

Table 82: Summary of IGMP Snooping Output Fields (continued)

Field	Values
Group	Indicates the multicast groups learned by the VLAN.
Next-Hop	Specifies the next hop assigned by the switch after performing the route lookup.

- See Also**
- [Monitoring Ethernet Switching](#)
 - [Monitoring GVRP on page 134](#)
 - [Monitoring Spanning Tree on page 132](#)

Monitoring GVRP

Purpose Use the monitoring functionality to view the GVRP page.

Action To monitor GVRP select **Monitor>Switching>GVRP** in the J-Web user interface.

Meaning [Table 83 on page 134](#) summarizes key output fields in the GVRP page.

Table 83: GVRP Monitoring Page

Field	Value	Additional Information
Global GVRP Configuration		
GVRP Status	Displays whether GVRP is enabled or disabled.	—
GVRP Timer	Displays the GVRP timer in millisecond.	—
Join	The number of milliseconds the interfaces must wait before sending VLAN advertisements.	—
Leave	The number of milliseconds an interface must wait after receiving a Leave message to remove the interface from the VLAN specified in the message.	—
Leave All	The interval in milliseconds at which Leave All messages are sent on interfaces. Leave All messages maintain current GVRP VLAN membership information in the network.	—
GVRP Interface Details		
Interface Name	The interface on which GVRP is configured.	—
Protocol Status	Displays whether GVRP is enabled or disabled.	—

- See Also**
- *Monitoring Ethernet Switching*
 - *Monitoring Spanning Tree on page 132*

Routing

- *Monitoring Route Information on page 135*
- *Monitoring RIP Routing Information on page 137*
- *Monitoring OSPF Routing Information on page 139*
- *Monitoring BGP Routing Information on page 141*

Monitoring Route Information

Purpose View information about the routes in a routing table, including destination, protocol, state, and parameter information.

Action Select **Monitor>Routing>Route Information** in the J-Web user interface, or enter the following CLI commands:

- **show route terse**
- **show route detail**



NOTE: When you use an HTTPS connection in the Microsoft Internet Explorer browser to save a report from this page in the J-Web interface, the error message "Internet Explorer was not able to open the Internet site" is displayed. This problem occurs because the Cache-Control: no cache HTTP header is added on the server side and Internet Explorer does not allow you to download the encrypted file with the Cache-Control: no cache HTTP header set in the response from the server.

As a workaround, refer to Microsoft Knowledge Base article 323308, which is available at this URL: <http://support.microsoft.com/kb/323308>. Also, you can alternatively use HTTP in the Internet Explorer browser or use HTTPS in the Mozilla Firefox browser to save a file from this page.

Table 84 on page 135 describes the different filters, their functions, and the associated actions.

Table 85 on page 136 summarizes key output fields in the routing information display.

Table 84: Filtering Route Messages

Field	Function	Your Action
Destination Address	Specifies the destination address of the route.	Enter the destination address.

Table 84: Filtering Route Messages (continued)

Field	Function	Your Action
Protocol	Specifies the protocol from which the route was learned.	Enter the protocol name.
Next hop address	Specifies the network layer address of the directly reachable neighboring system (if applicable) and the interface used to reach it.	Enter the next hop address.
Receive protocol	Specifies the dynamic routing protocol using which the routing information was received through a particular neighbor.	Enter the routing protocol.
Best route	Specifies only the best route available.	Select the view details of the best route.
Inactive routes	Specifies the inactive routes.	Select the view details of inactive routes.
Exact route	Specifies the exact route.	Select the view details of the exact route.
Hidden routes	Specifies the hidden routes.	Select the view details of hidden routes.
Search	Applies the specified filter and displays the matching messages.	To apply the filter and display messages, click Search .
Reset	Resets selected options to default	To reset the filter, click Reset .

Table 85: Summary of Key Routing Information Output Fields

Field	Values	Additional Information
Static Route Addresses	The list of static route addresses.	—
Protocol	Protocol from which the route was learned: Static , Direct , Local , or the name of a particular protocol.	—
Preference	The preference is the individual preference value for the route.	The route preference is used as one of the route selection criteria.

Table 85: Summary of Key Routing Information Output Fields (continued)

Field	Values	Additional Information
Next-Hop	Network Layer address of the directly reachable neighboring system (if applicable) and the interface used to reach it.	<p>If a next hop is listed as Discard, all traffic with that destination address is discarded rather than routed. This value generally means that the route is a static route for which the discard attribute has been set.</p> <p>If a next hop is listed as Reject, all traffic with that destination address is rejected. This value generally means that the address is unreachable. For example, if the address is a configured interface address and the interface is unavailable, traffic bound for that address is rejected.</p> <p>If a next hop is listed as Local, the destination is an address on the host (either the loopback address or Ethernet management port 0 address, for example).</p>
Age	How long the route has been active.	—
State	Flags for this route.	There are many possible flags.
AS Path	<p>AS path through which the route was learned. The letters of the AS path indicate the path origin:</p> <ul style="list-style-type: none"> • I—IGP. • E—EGP. • ?—Incomplete. Typically, the AS path was aggregated. 	—

- See Also**
- [Monitoring RIP Routing Information on page 137](#)
 - [Monitoring OSPF Routing Information on page 139](#)
 - [Monitoring BGP Routing Information on page 141](#)

Monitoring RIP Routing Information

Purpose View RIP routing information, including a summary of RIP neighbors and statistics.

Action Select **Monitor>Routing>RIP Information** in the J-Web user interface, or enter the following CLI commands:

- **show rip statistics**
- **show rip neighbors**

[Table 86 on page 138](#) summarizes key output fields in the RIP routing display in the J-Web user interface.

Table 86: Summary of Key RIP Routing Output Fields

Field	Values	Additional Information
RIP Statistics		
Protocol Name	The RIP protocol name.	—
Port number	The port on which RIP is enabled.	—
Hold down time	The interval during which routes are neither advertised nor updated.	—
Global routes learned	Number of RIP routes learned on the logical interface.	—
Global routes held down	Number of RIP routes that are not advertised or updated during the hold-down interval.	—
Global request dropped	Number of requests dropped.	—
Global responses dropped	Number of responses dropped.	—
RIP Neighbors		
Details	Tab used to view the details of the interface on which RIP is enabled.	—
Neighbor	Name of the RIP neighbor.	This value is the name of the interface on which RIP is enabled. Click the name to see the details for this neighbor.
State	State of the RIP connection: Up or Dn (Down).	—
Source Address	Local source address.	This value is the configured address of the interface on which RIP is enabled.
Destination Address	Destination address.	This value is the configured address of the immediate RIP adjacency.
Send Mode	The mode of sending RIP messages.	—
Receive Mode	The mode in which messages are received.	—
In Metric	Value of the incoming metric configured for the RIP neighbor.	—

- See Also**
- [Monitoring Route Information on page 135](#)
 - [Monitoring OSPF Routing Information on page 139](#)

- [Monitoring BGP Routing Information on page 141](#)

Monitoring OSPF Routing Information

Purpose View OSPF routing information, including a summary of OSPF neighbors, interfaces, and statistics.

Action Select **Monitor>Routing>OSPF Information** in the J-Web user interface, or enter the following CLI commands:

- **show ospf neighbors**
- **show ospf interfaces**
- **show ospf statistics**

[Table 87 on page 139](#) summarizes key output fields in the OSPF routing display in the J-Web user interface.

Table 87: Summary of Key OSPF Routing Output Fields

Field	Values	Additional Information
OSPF Interfaces		
Details	Tab used to view the details of the selected OSPF.	—
Interface	Name of the interface running OSPF.	—
State	State of the interface: BDR , Down , DR , DROther , Loop , PtToPt , or Waiting .	The Down state, indicating that the interface is not functioning, and PtToPt state, indicating that a point-to-point connection has been established, are the most common states.
Area	Number of the area that the interface is in.	—
DR ID	ID of the area's designated device.	—
BDR ID	ID of the area's backup designated device.	—
Neighbors	Number of neighbors on this interface.	—
OSPF Statistics		
Packets tab		
Sent	Displays the total number of packets sent.	—
Received	Displays the total number of packets received.	—
Details tab		
Flood Queue Depth	Number of entries in the extended queue.	—

Table 87: Summary of Key OSPF Routing Output Fields (continued)

Field	Values	Additional Information
Total Retransmits	Number of retransmission entries enqueued.	–
Total Database Summaries	Total number of database description packets.	–
OSPF Neighbors		
Address	Address of the neighbor.	–
Interface	Interface through which the neighbor is reachable.	–
State	State of the neighbor: Attempt, Down, Exchange, ExStart, Full, Init, Loading, or 2way.	Generally, only the Down state, indicating a failed OSPF adjacency, and the Full state, indicating a functional adjacency, are maintained for more than a few seconds. The other states are transitional states that a neighbor is in only briefly while an OSPF adjacency is being established.
ID	ID of the neighbor.	–
Priority	Priority of the neighbor to become the designated router.	–
Activity Time	The activity time.	–
Area	Area that the neighbor is in.	–
Options	Option bits received in the hello packets from the neighbor.	–
DR Address	Address of the designated router.	–
BDR Address	Address of the backup designated router.	–
Uptime	Length of time since the neighbor came up.	–
Adjacency	Length of time since the adjacency with the neighbor was established.	–

- See Also**
- [Monitoring Route Information on page 135](#)
 - [Monitoring RIP Routing Information on page 137](#)
 - [Monitoring BGP Routing Information on page 141](#)

Monitoring BGP Routing Information

Purpose Monitor BGP routing information on the routing device, including a summary of BGP routing and neighbor information.

Action Select **Monitor>Routing>BGP Information** in the J-Web user interface, or enter the following CLI commands:

- **show bgp summary**
- **show bgp neighbor**

[Table 88 on page 141](#) summarizes key output fields in the BGP routing display in the J-Web user interface.

Table 88: Summary of Key BGP Routing Output Fields

Field	Values	Additional Information
BGP Peer Summary		
Total Groups	Number of BGP groups.	—
Total Peers	Number of BGP peers.	—
Down Peers	Number of unavailable BGP peers.	—
Unconfigured Peers	Address of each BGP peer.	—
RIB Summary tab		
RIB Name	Name of the RIB group.	—
Total Prefixes	Total number of prefixes from the peer, both active and inactive, that are in the routing table.	—
Active Prefixes	Number of prefixes received from the EBGp peers that are active in the routing table.	—
Suppressed Prefixes	Number of routes received from EBGp peers currently inactive because of damping or other reasons.	—
History Prefixes	History of the routes received or suppressed.	—
Dumped Prefixes	Number of routes currently inactive because of damping or other reasons. These routes do not appear in the forwarding table and are not exported by routing protocols.	—
Pending Prefixes	Number of pending routes.	—

Table 88: Summary of Key BGP Routing Output Fields (continued)

Field	Values	Additional Information
State	Status of the graceful restart process for this routing table: BGP restart is complete, BGP restart in progress, VPN restart in progress, or VPN restart is complete.	—
BGP Neighbors		
Details	Click this button to view the selected BGP neighbor details.	—
Peer Address	Address of the BGP neighbor.	—
Autonomous System	AS number of the peer.	—
Peer State	<p>Current state of the BGP session:</p> <ul style="list-style-type: none"> • Active—BGP is initiating a TCP connection in an attempt to connect to a peer. If the connection is successful, BGP sends an open message. • Connect—BGP is waiting for the TCP connection to become complete. • Established—The BGP session has been established, and the peers are exchanging BGP update messages. • Idle—This is the first stage of a connection. BGP is waiting for a Start event. • OpenConfirm—BGP has acknowledged receipt of an open message from the peer and is waiting to receive a keepalive or notification message. • OpenSent—BGP has sent an open message and is waiting to receive an open message from the peer. 	Generally, the most common states are Active , which indicates a problem establishing the BGP connection, and Established , which indicates a successful session setup. The other states are transition states, and BGP sessions normally do not stay in those states for extended periods of time.
Elapsed Time	Elapsed time since the peering session was last reset.	—
Description	Description of the BGP session.	—

- See Also**
- [Monitoring Route Information on page 135](#)
 - [Monitoring RIP Routing Information on page 137](#)
 - [Monitoring OSPF Routing Information on page 139](#)

Class of Service

- [Monitoring CoS Interfaces on page 143](#)
- [Monitoring CoS Classifiers on page 144](#)
- [Monitoring CoS Value Aliases on page 145](#)
- [Monitoring CoS RED Drop Profiles on page 146](#)
- [Monitoring CoS Forwarding Classes on page 147](#)
- [Monitoring CoS Rewrite Rules on page 148](#)
- [Monitoring CoS Scheduler Maps on page 149](#)

Monitoring CoS Interfaces

Purpose Display details about the physical and logical interfaces and the CoS components assigned to them.

Action Select **Monitor>Class of Service>Interfaces** in the J-Web user interface, or enter the **show class-of-service interface *interface*** command.

[Table 89 on page 143](#) summarizes key output fields for CoS interfaces.

Table 89: Summary of Key CoS Interfaces Output Fields

Field	Values	Additional Information
Interface	Name of a physical interface to which CoS components are assigned.	To display names of logical interfaces configured on this physical interface, click the plus sign (+).
Scheduler Map	Name of the scheduler map associated with this interface.	—
Queues Supported	Number of queues you can configure on the interface.	—
Queues in Use	Number of queues currently configured.	—
Logical Interface	Name of a logical interface on the physical interface, to which CoS components are assigned.	—
Object	Category of an object—for example, classifier , scheduler-map , or rewrite .	—
Name	Name that you have given to an object—for example, ba-classifier .	—
Type	Type of an object—for example, dscp , or exp for a classifier.	—

Table 89: Summary of Key CoS Interfaces Output Fields (continued)

Field	Values	Additional Information
Index	Index of this interface or the internal index of a specific object.	—

- See Also**
- [Monitoring CoS Classifiers on page 144](#)
 - [Monitoring CoS Value Aliases on page 145](#)
 - [Monitoring CoS RED Drop Profiles on page 146](#)
 - [Monitoring CoS Forwarding Classes on page 147](#)
 - [Monitoring CoS Rewrite Rules on page 148](#)
 - [Monitoring CoS Scheduler Maps on page 149](#)

Monitoring CoS Classifiers

Purpose Display the mapping of incoming CoS value to forwarding class and loss priority.

Action For each classifier, select **Monitor>Class of Service>Classifiers** in the J-Web user interface, or enter the **show class-of-service classifier** command.

[Table 90 on page 144](#) summarizes key output fields for CoS classifiers.

Table 90: Summary of Key CoS Classifier Output Fields

Classifier Name	Name of a classifier.	To display classifier assignments, click the plus sign (+).
CoS Value Type	The classifiers are displayed by type: <ul style="list-style-type: none"> • dscp—All classifiers of the DSCP type. • dscp ipv6—All classifiers of the DSCP IPv6 type. • exp—All classifiers of the MPLS EXP type. • ieee-802.1—All classifiers of the IEEE 802.1 type. • inet-precedence—All classifiers of the IP precedence type. 	
Index	Internal index of the classifier.	
Incoming CoS Value	CoS value of the incoming packets, in bits. These values are used for classification.	

Table 90: Summary of Key CoS Classifier Output Fields (continued)

Assign to Forwarding Class	Forwarding class that the classifier assigns to an incoming packet. This class affects the forwarding and scheduling policies that are applied to the packet as it transits the device.
Assign to Loss Priority	Loss priority value that the classifier assigns to the incoming packet based on its CoS value.

- See Also**
- [Monitoring CoS Interfaces on page 143](#)
 - [Monitoring CoS Value Aliases on page 145](#)
 - [Monitoring CoS RED Drop Profiles on page 146](#)
 - [Monitoring CoS Forwarding Classes on page 147](#)
 - [Monitoring CoS Rewrite Rules on page 148](#)
 - [Monitoring CoS Scheduler Maps on page 149](#)

Monitoring CoS Value Aliases

Purpose Display information about the CoS value aliases that the system is currently using to represent DSCP, DSCP IPv6, MPLS EXP, and IPv4 precedence bits.

Action Select **Monitor>Class of Service>CoS Value Aliases** in the J-Web user interface, or enter the **show class-of-service code-point-aliases** command.

[Table 91 on page 145](#) summarizes key output fields for CoS value aliases.

Table 91: Summary of Key CoS Value Alias Output Fields

Field	Values	Additional Information
CoS Value Type	Type of the CoS value: <ul style="list-style-type: none"> • dscp—Examines Layer 3 packet headers for IP packet classification. • dscp ipv6—Examines Layer 3 packet headers for IPv6 packet classification. • exp—Examines Layer 2 packet headers for MPLS packet classification. • ieee-802.1—Examines Layer 2 packet header for packet classification. • inet-precedence—Examines Layer 3 packet headers for IP packet classification. 	To display aliases and bit patterns, click the plus sign (+).
CoS Value Alias	Name given to a set of bits—for example, af11 is a name for 001010 bits.	—

Table 91: Summary of Key CoS Value Alias Output Fields (continued)

Field	Values	Additional Information
Bit Pattern	Set of bits associated with an alias.	—

- See Also**
- [Monitoring CoS Interfaces on page 143](#)
 - [Monitoring CoS Classifiers on page 144](#)
 - [Monitoring CoS RED Drop Profiles on page 146](#)
 - [Monitoring CoS Forwarding Classes on page 147](#)
 - [Monitoring CoS Rewrite Rules on page 148](#)
 - [Monitoring CoS Scheduler Maps on page 149](#)

Monitoring CoS RED Drop Profiles

Purpose Display data point information for each CoS random early detection (RED) drop profile currently on a system.

Action Select **Monitor>Class of Service>RED Drop Profiles** in the J-Web user interface, or enter the **show class-of-service drop-profile** command.

[Table 92 on page 146](#) summarizes key output fields for CoS RED drop profiles.

Table 92: Summary of Key CoS RED Drop Profile Output Fields

Field	Values	Additional Information
RED Drop Profile Name	Name of the RED drop profile. A drop profile consists of pairs of values between 0 and 100, one for queue buffer fill level and one for drop probability, that determine the relationship between a buffer's fullness and the likelihood it will drop packets.	To display profile values, click the plus sign (+).
Graph RED Profile	Link to a graph of a RED curve that the system uses to determine the drop probability based on queue buffer fullness.	The x axis represents the queue buffer fill level, and the y axis represents the drop probability.
Type	Type of a specific drop profile: <ul style="list-style-type: none"> • interpolated—The two coordinates (x and y) of the graph are interpolated to produce a smooth profile. • segmented—The two coordinates (x and y) of the graph are represented by line fragments to produce a segmented profile. 	—

Table 92: Summary of Key CoS RED Drop Profile Output Fields (continued)

Field	Values	Additional Information
Index	Internal index of this drop profile.	–
Fill Level	Percentage fullness of a buffer queue. This value is the x coordinate of the RED drop profile graph.	–
Drop Probability	Drop probability of a packet corresponding to a specific queue buffer fill level. This value is the y coordinate of the RED drop profile graph.	–

- See Also**
- [Monitoring CoS Interfaces on page 143](#)
 - [Monitoring CoS Classifiers on page 144](#)
 - [Monitoring CoS Value Aliases on page 145](#)
 - [Monitoring CoS Forwarding Classes on page 147](#)
 - [Monitoring CoS Rewrite Rules on page 148](#)
 - [Monitoring CoS Scheduler Maps on page 149](#)

Monitoring CoS Forwarding Classes

Purpose View the current assignment of CoS forwarding classes to queue numbers on the system.

Action Select **Monitor>Class of Service>Forwarding Classes** in the J-Web user interface, or enter the **show class-of-service forwarding-class** command.

[Table 93 on page 148](#) summarizes key output fields for CoS forwarding classes.

Table 93: Summary of Key CoS Forwarding Class Output Fields

Field	Values	Additional Information
Forwarding Class	Names of forwarding classes assigned to queue numbers. By default, the following forwarding classes are assigned to queues 0 through 3: <ul style="list-style-type: none"> • best-effort—Provides no special CoS handling of packets. Loss priority is typically not carried in a CoS value, and RED drop profiles are more aggressive. • expedited-forwarding—Provides low loss, low delay, low jitter, assured bandwidth, and end-to-end service. • assured-forwarding—Provides high assurance for packets within specified service profile. Excess packets are dropped. • network-control—Packets can be delayed but not dropped. 	—
Queue	Queue number corresponding to the forwarding class name.	By default, four queues, 0 through 3, are assigned to forwarding classes.

- See Also**
- [Monitoring CoS Interfaces on page 143](#)
 - [Monitoring CoS Classifiers on page 144](#)
 - [Monitoring CoS Value Aliases on page 145](#)
 - [Monitoring CoS RED Drop Profiles on page 146](#)
 - [Monitoring CoS Rewrite Rules on page 148](#)
 - [Monitoring CoS Scheduler Maps on page 149](#)

Monitoring CoS Rewrite Rules

Purpose Display information about CoS value rewrite rules, which are based on the forwarding class and loss priority.

Action Select **Monitor>Class of Service>Rewrite Rules** in the J-Web user interface, or enter the **show class-of-service rewrite-rules** command.

[Table 94 on page 148](#) summarizes key output fields for CoS rewrite rules.

Table 94: Summary of Key CoS Rewrite Rules Output Fields

Field	Values	Additional Information
Rewrite Rule Name	Names of rewrite rules.	—

Table 94: Summary of Key CoS Rewrite Rules Output Fields (continued)

Field	Values	Additional Information
CoS Value Type	Rewrite rule type: <ul style="list-style-type: none"> • dscp—For IPv4 DiffServ traffic. • dscp-ipv6—For IPv6 DiffServ traffic. • exp—For MPLS traffic. • ieee-802.1—For Layer 2 traffic. • inet-precedence—For IPv4 traffic. 	To display forwarding classes, loss priorities, and rewritten CoS values, click the plus sign (+).
Index	Internal index for this particular rewrite rule.	—
Forwarding Class	Forwarding class that in combination with loss priority is used to determine CoS values for rewriting.	Rewrite rules are applied to CoS values in outgoing packets based on forwarding class and loss priority setting.
Loss Priority	Loss priority that in combination with forwarding class is used to determine CoS values for rewriting.	—
Rewrite CoS Value To	Value that the CoS value is rewritten to.	—

- See Also**
- [Monitoring CoS Interfaces on page 143](#)
 - [Monitoring CoS Classifiers on page 144](#)
 - [Monitoring CoS Value Aliases on page 145](#)
 - [Monitoring CoS RED Drop Profiles on page 146](#)
 - [Monitoring CoS Forwarding Classes on page 147](#)
 - [Monitoring CoS Scheduler Maps on page 149](#)

Monitoring CoS Scheduler Maps

Purpose Display assignments of CoS forwarding classes to schedulers.

Action Select **Monitor>Class of Service>Scheduler Maps** in the J-Web user interface, or enter the **show class-of-service scheduler-map** command.

[Table 95 on page 149](#) summarizes key output fields for CoS scheduler maps.

Table 95: Summary of Key CoS Scheduler Maps Output Fields

Field	Values	Additional Information
Scheduler Map	Name of a scheduler map.	For details, click the plus sign (+).

Table 95: Summary of Key CoS Scheduler Maps Output Fields (continued)

Field	Values	Additional Information
Index	Index of a specific object—scheduler maps, schedulers, or drop profiles.	—
Scheduler Name	Name of a scheduler.	—
Forwarding Class	Forwarding classes this scheduler is assigned to.	—
Transmit Rate	<p>Configured transmit rate of the scheduler in bits per second (bps). The rate value can be either of the following:</p> <ul style="list-style-type: none"> A percentage—The scheduler receives the specified percentage of the total interface bandwidth. remainder—The scheduler receives the remaining bandwidth of the interface after allocation to other schedulers. 	—
Rate Limit	<p>Rate limiting configuration of the queue:</p> <ul style="list-style-type: none"> none—No rate limiting. exact—The queue transmits at only the configured rate. 	—
Buffer Size	<p>Delay buffer size in the queue or the amount of transmit delay (in milliseconds). The buffer size can be either of the following:</p> <ul style="list-style-type: none"> A percentage—The buffer is a percentage of the total buffer allocation. remainder—The buffer is sized according to what remains after other scheduler buffer allocations. 	—
Priority	<p>Scheduling priority of a queue:</p> <ul style="list-style-type: none"> high—Packets in this queue are transmitted first. low—Packets in this queue are transmitted last. medium-high—Packets in this queue are transmitted after high-priority packets. medium-low—Packets in this queue are transmitted before low-priority packets. 	—
Drop Profiles	Name and index of a drop profile that is assigned to a specific loss priority and protocol pair.	—

Table 95: Summary of Key CoS Scheduler Maps Output Fields (continued)

Field	Values	Additional Information
Loss Priority	Packet loss priority corresponding to a drop profile: <ul style="list-style-type: none"> • low—Packet has a low loss priority. • high—Packet has a high loss priority. • medium-low—Packet has a medium-low loss priority. • medium-high—Packet has a medium-high loss priority. 	—
Protocol	Transport protocol corresponding to a drop profile.	—
Drop Profile Name	Name of the drop profile.	—

- See Also**
- [Monitoring CoS Interfaces on page 143](#)
 - [Monitoring CoS Classifiers on page 144](#)
 - [Monitoring CoS Value Aliases on page 145](#)
 - [Monitoring CoS RED Drop Profiles on page 146](#)
 - [Monitoring CoS Forwarding Classes on page 147](#)
 - [Monitoring CoS Rewrite Rules on page 148](#)

MPLS

- [Monitoring MPLS Interfaces on page 151](#)
- [Monitoring MPLS LSP Information on page 152](#)
- [Monitoring MPLS LSP Statistics on page 153](#)
- [Monitoring RSVP Session Information on page 155](#)
- [Monitoring MPLS RSVP Interfaces Information on page 156](#)

Monitoring MPLS Interfaces

Purpose View the interfaces on which MPLS is configured, including operational state and any administrative groups applied to an interface.

Action Select **Monitor>MPLS>Interfaces** in the J-Web user interface, or enter the **show mpls interface** command.

[Table 96 on page 152](#) summarizes key output fields in the MPLS interface information display.

Table 96: Summary of Key MPLS Interface Information Output Fields

Field	Values	Additional Information
Interface	Name of the interface on which MPLS is configured.	–
State	State of the specified interface: Up or Dn (down).	–
Administrative groups	Administratively assigned colors of the MPLS link configured on the interface.	–

- See Also**
- [Monitoring MPLS LSP Information on page 152](#)
 - [Monitoring MPLS LSP Statistics on page 153](#)
 - [Monitoring RSVP Session Information on page 155](#)
 - [Monitoring MPLS RSVP Interfaces Information on page 156](#)

Monitoring MPLS LSP Information

Purpose View all label-switched paths (LSPs) configured on the services router, including all inbound (ingress), outbound (egress), and transit LSP information.

Action Select **Monitor>MPLS>LSP Information** in the J-Web user interface, or enter the **show mpls lsp** command.

[Table 97 on page 152](#) summarizes key output fields in the MPLS LSP information display.

Table 97: Summary of Key MPLS LSP Information Output Fields

Field	Values	Additional Information
Ingress LSP	Information about LSPs on the inbound device. Each session has one line of output.	–
Egress LSP	Information about the LSPs on the outbound device. Each session has one line of output.	MPLS learns this information by querying RSVP, which holds all the transit and outbound session information.
Transit LSP	Number of LSPs on the transit routers and the state of these paths.	MPLS learns this information by querying RSVP, which holds all the transit and outbound session information.
To	Destination (outbound device) of the session.	–
From	Source (inbound device) of the session.	–
State	State of the path. It can be Up , Down , or AdminDn .	AdminDn indicates that the LSP is being taken down gracefully.

Table 97: Summary of Key MPLS LSP Information Output Fields (continued)

Field	Values	Additional Information
Rt	Number of active routes (prefixes) installed in the routing table.	For inbound RSVP sessions, the routing table is the primary IPv4 table (inet.0). For transit and outbound RSVP sessions, the routing table is the primary MPLS table (mpls.0).
Active Path	Name of the active path: Primary or Secondary .	This field is used for inbound LSPs only.
P	An asterisk (*) in this column indicates that the LSP is a primary path.	This field is used for inbound LSPs only.
LSPname	Configured name of the LSP.	—
Style	RSVP reservation style. This field consists of two parts. The first is the number of active reservations. The second is the reservation style, which can be FF (fixed filter), SE (shared explicit), or WF (wildcard filter).	This field is used for outbound and transit LSPs only.
Labelin	Incoming label for this LSP.	—
Labelout	Outgoing label for this LSP.	—
Total	Total number of LSPs displayed for the particular type— ingress (inbound), egress (outbound), or transit .	—

- See Also**
- [Monitoring MPLS Interfaces on page 151](#)
 - [Monitoring MPLS LSP Statistics on page 153](#)
 - [Monitoring RSVP Session Information on page 155](#)
 - [Monitoring MPLS RSVP Interfaces Information on page 156](#)

Monitoring MPLS LSP Statistics

Purpose Display statistics for LSP sessions currently active on the device, including the total number of packets and bytes forwarded through an LSP.

Action Select **Monitor>MPLS>LSP Statistics** in the J-Web user interface, or enter the **show mpls lsp statistics** command.



NOTE: Statistics are not available for LSPs on the outbound device, because the penultimate device in the LSP sets the label to 0. Also, as the packet arrives at the outbound device, the hardware removes its MPLS header and the packet reverts to being an IPv4 packet. Therefore, it is counted as an IPv4 packet, not an MPLS packet.

Table 98 on page 154 summarizes key output fields in the MPLS LSP statistics display.

Table 98: Summary of Key MPLS LSP Statistics Output Fields

Field	Values	Additional Information
Ingress LSP	Information about LSPs on the inbound device. Each session has one line of output.	—
Egress LSP	Information about the LSPs on the outbound device. Each session has one line of output.	MPLS learns this information by querying RSVP, which holds all the transit and outbound session information.
Transit LSP	Number of LSPs on the transit routers and the state of these paths.	MPLS learns this information by querying RSVP, which holds all the transit and outbound session information.
To	Destination (outbound device) of the session.	—
From	Source (inbound device) of the session.	—
State	State of the path: Up , Down , or AdminDn .	AdminDn indicates that the LSP is being taken down gracefully.
Packets	Total number of packets received on the LSP from the upstream neighbor.	—
Bytes	Total number of bytes received on the LSP from the upstream neighbor.	—
LSPname	Configured name of the LSP.	—
Total	Total number of LSPs displayed for the particular type— ingress (inbound), egress (outbound), or transit .	—

- See Also**
- [Monitoring MPLS Interfaces on page 151](#)
 - [Monitoring MPLS LSP Information on page 152](#)
 - [Monitoring RSVP Session Information on page 155](#)
 - [Monitoring MPLS RSVP Interfaces Information on page 156](#)

Monitoring RSVP Session Information

- Purpose** View information about RSVP-signaled LSP sessions currently active on the device, including inbound (ingress) and outbound (egress) addresses, LSP state, and LSP name.
- Action** Select **Monitor>MPLS>RSVP Sessions** in the J-Web user interface, or enter the **show rsvp session** command.

Table 99 on page 155 summarizes key output fields in the RSVP session information display.

Table 99: Summary of Key RSVP Session Information Output Fields

Field	Values	Additional Information
Ingress LSP	Information about inbound RSVP sessions. Each session has one line of output.	–
Egress LSP	Information about outbound RSVP sessions. Each session has one line of output.	MPLS learns this information by querying RSVP, which holds all the transit and outbound session information.
Transit LSP	Information about transit RSVP sessions.	MPLS learns this information by querying RSVP, which holds all the transit and outbound session information.
To	Destination (outbound device) of the session.	–
From	Source (inbound device) of the session.	–
State	State of the path: Up , Down , or AdminDn .	AdminDn indicates that the LSP is being taken down gracefully.
Rt	Number of active routes (prefixes) installed in the routing table.	For inbound RSVP sessions, the routing table is the primary IPv4 table (inet.0). For transit and outbound RSVP sessions, the routing table is the primary MPLS table (mpls.0).
Style	RSVP reservation style. This field consists of two parts. The first is the number of active reservations. The second is the reservation style, which can be FF (fixed filter), SE (shared explicit), or WF (wildcard filter).	This field is used for outbound and transit LSPs only.
Labelin	Incoming label for this RSVP session.	–
Labelout	Outgoing label for this RSVP session.	–
LSPname	Configured name of the LSP.	–

Table 99: Summary of Key RSVP Session Information Output Fields (continued)

Field	Values	Additional Information
Total	Total number of RSVP sessions displayed for the particular type— ingress (inbound), egress (outbound), or transit .	—

- See Also**
- [Monitoring MPLS Interfaces on page 151](#)
 - [Monitoring MPLS LSP Information on page 152](#)
 - [Monitoring MPLS LSP Statistics on page 153](#)
 - [Monitoring MPLS RSVP Interfaces Information on page 156](#)

Monitoring MPLS RSVP Interfaces Information

Purpose View information about the interfaces on which RSVP is enabled, including the interface name, total bandwidth through the interface, and total current reserved and reservable (available) bandwidth on the interface.

Action Select **Monitor>MPLS>RSVP Interfaces** in the J-Web user interface, or enter the **show rsvp interface** command.

[Table 100 on page 156](#) summarizes key output fields in the RSVP interfaces information display.

Table 100: Summary of Key RSVP Interfaces Information Output Fields

Field	Values	Additional Information
RSVP Interface	Number of interfaces on which RSVP is active. Each interface has one line of output.	—
Interface	Name of the interface.	—
State	State of the interface: <ul style="list-style-type: none"> • Disabled—No traffic engineering information is displayed. • Down—The interface is not operational. • Enabled—Displays traffic engineering information. • Up—The interface is operational. 	—
Active resv	Number of reservations that are actively reserving bandwidth on the interface.	—
Subscription	User-configured subscription factor.	—

Table 100: Summary of Key RSVP Interfaces Information Output Fields (continued)

Field	Values	Additional Information
Static BW	Total interface bandwidth, in bits per second (bps).	–
Available BW	Amount of bandwidth that RSVP is allowed to reserve, in bits per second (bps). It is equal to (static bandwidth X subscription factor).	–
Reserved BW	Currently reserved bandwidth, in bits per second (bps).	–
Highwater mark	Highest bandwidth that has ever been reserved on this interface, in bits per second (bps).	–

- See Also**
- [Monitoring MPLS Interfaces on page 151](#)
 - [Monitoring MPLS LSP Information on page 152](#)
 - [Monitoring MPLS LSP Statistics on page 153](#)
 - [Monitoring RSVP Session Information on page 155](#)

PPPoE

- [Monitoring PPPoE on page 157](#)

Monitoring PPPoE

Purpose Display the session status for PPPoE interfaces, cumulative statistics for all PPPoE interfaces on the device, and the PPPoE version configured on the device.

Action Select **Monitor>PPPoE** in the J-Web user interface. To view interface-specific properties in the J-Web interface, select the interface name on the PPPoE page.

[Table 101 on page 157](#) summarizes key output fields in PPPoE displays.

Table 101: Summary of Key PPPoE Output Fields

Field	Values	Additional Information
PPPoE Interfaces		
Interface	Name of the PPPoE interface.	Click the interface name to display PPPoE information for the interface.
State	State of the PPPoE session on the interface.	–

Table 101: Summary of Key PPPoE Output Fields (continued)

Field	Values	Additional Information
Session ID	Unique session identifier for the PPPoE session.	To establish a PPPoE session, first the device acting as a PPPoE client obtains the Ethernet address of the PPPoE server or access concentrator, and then the client and the server negotiate a unique session ID. This process is referred to as PPPoE active discovery and is made up of four steps: initiation, offer, request, and session confirmation. The access concentrator generates the session ID for session confirmation and sends it to the PPPoE client in a PPPoE Active Discovery Session-Confirmation (PADS) packet.
Service Name	Type of service required from the access concentrator.	Service Name identifies the type of service provided by the access concentrator, such as the name of the Internet service provider (ISP), class, or quality of service.
Configured AC Name	Configured access concentrator name.	—
Session AC Names	Name of the access concentrator.	—
AC MAC Address	Media access control (MAC) address of the access concentrator.	—
Session Uptime	Number of seconds the current PPPoE session has been running.	—
Auto-Reconnect Timeout	Number of seconds to wait before reconnecting after a PPPoE session is terminated.	—
Idle Timeout	Number of seconds a PPPoE session can be idle without disconnecting.	—
Underlying Interface	Name of the underlying logical Ethernet or ATM interface on which PPPoE is running—for example, ge-0/0/0.1 .	—
PPPoE Statistics		
Active PPPoE Sessions	Total number of active PPPoE sessions.	—

Table 101: Summary of Key PPPoE Output Fields (continued)

Field	Values	Additional Information
Packet Type	Packets sent and received during the PPPoE session, categorized by packet type and packet error: <ul style="list-style-type: none"> • PADI—PPPoE Active Discovery Initiation packets. • PADO—PPPoE Active Discovery Offer packets. • PADR—PPPoE Active Discovery Request packets. • PADS—PPPoE Active Discovery Session-Confirmation packets. • PADT—PPPoE Active Discovery Terminate packets. • Service Name Error—Packets for which the Service-Name request could not be honored. • AC System Error—Packets for which the access concentrator experienced an error in processing the host request. For example, the host had insufficient resources to create a virtual circuit. • Generic Error—Packets that indicate an unrecoverable error occurred. • Malformed Packet—Malformed or short packets that caused the packet handler to disregard the frame as unreadable. • Unknown Packet—Unrecognized packets. 	—
Sent	Number of the specific type of packet sent from the PPPoE client.	—
Received	Number of the specific type of packet received by the PPPoE client.	—
Timeout	Information about the timeouts that occurred during the PPPoE session. <ul style="list-style-type: none"> • PADI—Number of timeouts that occurred for the PADI packet. • PADO—Number of timeouts that occurred for the PADO packet. (This value is always 0 and is not supported.) • PADR—Number of timeouts that occurred for the PADR packet. 	—
Sent	Number of the timeouts that occurred for PADI, PADO, and PADR packets.	—
PPPoE Version		
Maximum Sessions	Maximum number of active PPPoE sessions the device can support. The default is 256 sessions.	—

Table 101: Summary of Key PPPoE Output Fields (continued)

Field	Values	Additional Information
PADI Resend Timeout	Initial time, (in seconds) the device waits to receive a PADO packet for the PADI packet sent—for example, 2 seconds. This timeout doubles for each successive PADI packet sent.	The PPPoE Active Discovery Initiation (PADI) packet is sent to the access concentrator to initiate a PPPoE session. Typically, the access concentrator responds to a PADI packet with a PPPoE Active Discovery Offer (PADO) packet. If the access concentrator does not send a PADO packet, the device sends the PADI packet again after timeout period is elapsed. The PADI Resend Timeout doubles for each successive PADI packet sent. For example, if the PADI Resend Timeout is 2 seconds, the second PADI packet is sent after 2 seconds, the third after 4 seconds, the fourth after 8 seconds, and so on.
PADR Resend Timeout	Initial time (in seconds) the device waits to receive a PADS packet for the PADR packet sent. This timeout doubles for each successive PADR packet sent.	The PPPoE Active Discovery Request (PADR) packet is sent to the access concentrator in response to a PADO packet, and to obtain the PPPoE session ID. Typically, the access concentrator responds to a PADR packet with a PPPoE Active Discovery Session-Confirmation (PADS) packet, which contains the session ID. If the access concentrator does not send a PADS packet, the device sends the PADR packet again after the PADR Resend Timeout period is elapsed. The PADR Resend Timeout doubles for each successive PADR packet sent.
Maximum Resend Timeout	Maximum value (in seconds) that the PADI or PADR resend timer can accept—for example, 64 seconds. The maximum value is 64.	—
Maximum Configured AC Timeout	Time (in seconds), within which the configured access concentrator must respond.	—

Alternatively, enter the following CLI commands:

- **show pppoe interfaces**
- **show pppoe statistics**
- **show pppoe version**

You can also view status information about the PPPoE interface by entering the **show interfaces pp0** command in the CLI editor.

- See Also**
- [Monitoring Overview](#)
 - [Monitoring Interfaces on page 11](#)
 - [Monitoring DHCP Client Bindings on page 161](#)

DHCP

- [Monitoring DHCP Client Bindings on page 161](#)
- [Monitoring DHCP Server on page 161](#)
- [Monitoring DHCP Relay on page 163](#)

Monitoring DHCP Client Bindings

Purpose View information about DHCP client bindings.

Action Select **Monitor>Services>DHCP>Binding** in the J-Web user interface, or enter the **show system services dhcp binding** command.

[Table 102 on page 161](#) summarizes the key output fields in the DHCP client binding displays.

Table 102: Summary of Key DHCP Client Binding Output Fields

Field	Values	Additional Information
IP Address	List of IP addresses the DHCP server has assigned to clients.	—
Hardware Address	Corresponding media access control (MAC) address of the client.	—
Type	Type of binding assigned to the client: dynamic or static.	—
Lease Expires at	Date and time the lease expires, or never for leases that do not expire.	—

- See Also**
- [Monitoring PPPoE on page 157](#)
 - [Understanding DHCP Client Operation](#)

Monitoring DHCP Server

Purpose Use the monitoring functionality to view information about dynamic and static DHCP leases, conflicts, pools, and statistics.

Action To monitor DHCP server, select **Monitor>DHCP>DHCP Server** in the J-Web user interface.

Meaning [Table 103 on page 162](#) summarizes key output fields in the events page.

Table 103: DHCP Server Monitoring Page

Field	Value	Additional Information
Binding Information		
IP address	Specifies the IP address of the DHCP server.	
Session id	Specifies the Session ID of the subscriber session.	—
Hardware address	Specifies the Hardware address of the DHCP server.	—
Expires	Specifies the number of seconds in which the lease expires.	—
State	State of the address binding table on the extended DHCP local server: <ul style="list-style-type: none"> • BOUND—Client has an active IP address lease. • FORCERENEW—Client has received the FORCERENEW message from the server. • INIT—Initial state. • RELEASE—Client is releasing the IP address lease. • RENEWING—Client is sending a request to renew the IP address lease. • REQUESTING—Client is requesting a DHCP server. • SELECTING—Client is receiving offers from DHCP servers. 	—
Interface	Specifies the interface on which the request was received.	—
Interface Details	Specifies the interface on which the DHCP server is configured.	—
Clear All Bindings	Clears all the binding information.	—
Statistics Information		
Sent	Number of BOOTREPLY, DHCP OFFER, DHCP ACK, DHCP NAK, DHCP FORCERENEW, DHCP LEASED UNASSIGNED, DHCP LEASE UNKNOWN, AND DHCP LEASE ACTIVE messages sent from the DHCP server to DHCP clients.	These information are displayed in a bar chart.

Table 103: DHCP Server Monitoring Page (continued)

Field	Value	Additional Information
Received	Number of BOOTREQUEST, DHCPDECLINE, DHCPDISCOVER, DHCPINFORM, DHCPRELEASE, DHCPREQUEST, DHCPLEASEQUERY, and DHCPBULKLEASE messages sent from DHCP clients and received by the DHCP server.	These information are displayed in a bar chart.
Dropped Packet Counters	Displays the number of dropped packet counters in a piechart.	—
Clear All Statistics	Clears all the collected statistical information.	—

- See Also**
- [Monitoring Alarms on page 21](#)
 - [Monitoring Security Events by Policy on page 22](#)

Monitoring DHCP Relay

Purpose Use the monitoring functionality to view information about dynamic and static DHCP leases, conflicts, pools, and statistics.

Action To monitor DHCP relay, select **Monitor>DHCP>DHCP Relay** in the J-Web user interface.

Meaning [Table 104 on page 163](#) summarizes key output fields in the events page.

Table 104: DHCP Relay Monitoring Page

Field	Value	Additional Information
Binding Information		
IP address	Specifies the IP address of the DHCP relay.	
Session id	Specifies the Session ID of the subscriber session.	—
Hardware address	Specifies the Hardware address of the DHCP relay.	—
Expires	Specifies the number of seconds in which the lease expires.	—

Table 104: DHCP Relay Monitoring Page (continued)

Field	Value	Additional Information
State	State of the address binding table on the extended DHCP local server: <ul style="list-style-type: none"> • BOUND—Client has an active IP address lease. • FORCERENEW—Client has received the FORCERENEW message from the server. • INIT—Initial state. • RELEASE—Client is releasing the IP address lease. • RENEWING—Client is sending a request to renew the IP address lease. • REQUESTING—Client is requesting a DHCP server. • SELECTING—Client is receiving offers from DHCP servers. 	—
Interface	Specifies the interface on which the request was received.	—
Interface Details	Specifies the interface on which the DHCP relay is configured.	—
Clear All Bindings	Clears all the binding information.	—
Statistics Information		
Sent	Number of BOOTREPLY, DHCPOFFER, DHCPACK, DHCPNAK, DHCPFORCERENEW, DHCPLEASEDUNASSIGNED, DHCPLEASEUNKNOWN, AND DHCPLEASEACTIVE messages sent from the DHCP server to DHCP clients.	These information are displayed in a bar chart.
Received	Number of BOOTREQUEST, DHCPDECLINE, DHCPDISCOVER, DHCPINFORM, DHCPRELEASE, DHCPREQUEST, DHCPLEASEQUERY, and DHCPBULKLEASE messages sent from DHCP clients and received by the DHCP server.	These information are displayed in a bar chart.
Dropped Packet Counters	Displays the number of dropped packet counters in a piechart.	—
Clear All Statistics	Clears all the collected statistical information.	—

- See Also**
- [Monitoring Alarms on page 21](#)
 - [Monitoring Security Events by Policy on page 22](#)

Wireless LAN

- [Monitoring Access Points on page 165](#)

Monitoring Access Points

Purpose Use the monitoring functionality to view the Access Points page.

Action To monitor access points, select **Monitor>Wireless LAN** in the J-Web interface.

Meaning [Table 105 on page 165](#) summarizes key output fields in the Access Points page.

Table 105: Access Points Monitoring Page

Field	Value	Additional Information
-------	-------	------------------------

Access Point Details

Table 105: Access Points Monitoring Page (continued)

Field	Value	Additional Information
Name	<p>Displays the following names:</p> <ul style="list-style-type: none"> • Access Point—Name of the access point. • Type—Type of access point (internal or external). • Location—Location of the access point. • Serial Number—Serial number of the access point. • Firmware Version—Firmware version for the access point. • Alternate Version—Backup firmware for the access point. • Regulatory Domain—Regulatory domain of the access point, such as FCC (Federal Communications Commission), ETSI (European Union Telecommunications Institute), TELEC, or WORLD. • Country—Country name. • Access Interface—Port where the access point is connected. • Packet Capture—ON or OFF. The default is OFF. • MAC Address—MAC address of the external access point. • IPv4 Address—IPv4 address of the access point. • Status—ON or OFF. • MAC Address—MAC address of radio 1. • Mode—Mode of radio 1. The mode can be a, an, or 5GHz 802.11n. The default is 802.11 a/n. • Channel—Frequency at which radio 1 operates. • Status—ON or OFF. • MAC Address—MAC address of radio 2 • Mode—Mode of radio 2. The mode can be bg, bgn, or 2.4GHz 802.11n. The default is 802.11 b/g/n • Channel—Frequency at which radio 2 operates 	
Value	Displays the values for the respective names	

Client Associations

Table 105: Access Points Monitoring Page (continued)

Field	Value	Additional Information
VAP	<p>Virtual access point with which the client is associated. For example, wlan0vap2 means the client is associated with VAP 2 on radio 1.</p> <p>wlan0 means the client is associated with VAP 0 on radio 1.</p> <p>wlan1 means the client is associated with VAP 0 on radio 2.</p>	
Client MAC Address	MAC address of the associated wireless client.	
Authentication	<p>Underlying IEEE 802.11 authentication status, if the virtual access point security mode is set to none or static WEP.</p> <p>This status does not show IEEE 802.1x authentication or association status. If the virtual access point security mode is set to 802.1x or WPA, it is possible for a client association to be shown as being authenticated when it has actually not been authenticated through the second layer of security.</p>	
Packets Rx/Tx	The number of packets received from the wireless clients and transmitted from the access point to the wireless client.	
Bytes Rx/Tx	The number of bytes received from the wireless clients and transmitted from the access point to the wireless client.	
Neighboring Access Points		
MAC Address	MAC address of the neighbor access point.	
Privacy	<p>Security on the neighbor access point:</p> <ul style="list-style-type: none"> • Off—Security mode is set to none (no security). • On—There is some security in place. 	
WPA	WPA security is on or off on the neighbor access point.	

Table 105: Access Points Monitoring Page (continued)

Field	Value	Additional Information
Band	IEEE 802.11 mode being used on the neighbor access point: <ul style="list-style-type: none"> • 2.4—IEEE 802.11b, 802.11g, or 802.11n mode, or a combination of these modes.. • 5—IEEE 802.11a or 802.11n mode, or both modes. 	
Channel	Channel on which the neighbor access point is currently broadcasting.	
SSID	Service set identifier that identifies the WLAN that the neighbor access point is broadcasting.	

- See Also**
- [Monitoring IPsec VPN—Phase II on page 129](#)
 - [Monitoring Ethernet Switching on page 130](#)

VLAN

- [Monitoring VLAN on page 168](#)

Monitoring VLAN

Purpose Use the monitoring functionality to view the VLAN information page.

Action To monitor VLAN information, select **Monitor>VLAN** in the J-Web user interface.

Meaning [Table 106 on page 168](#) summarizes key output fields in the VLAN information page.

Table 106: VLAN Information Monitoring Page

Field	Value	Additional Information
VLAN		
Routing Instance	Displays the routing instance name.	
VLAN Name	Displays the name of the VLAN.	
VLAN ID	Displays the VLAN ID number.	
MAC Table		
Select a VLAN	Displays the configured VLANs.	Select a VLAN from the drop-down list.

Table 106: VLAN Information Monitoring Page (continued)

Field	Value	Additional Information
MAC Address	Displays the MAC address associated with the VLAN.	
MAC Flags	Displays the flags associated with the MAC address.	
Logical Interface	Displays the name of a logical interface associated with the VLAN.	

See Also • [Monitoring CoS Classifiers on page 144](#)

Threats Map (Live)

- [Monitor Threats Map \(Live\) on page 169](#)

Monitor Threats Map (Live)

Starting in Junos OS 19.2R1 Release, Threats Map (Live) page is available on all the SRX Series devices except the SRX5000 line of devices. To monitor threats map, select **Monitor > Threats Map (Live)**.

Use this page to visualize incoming and outgoing threats between geographic regions. You can view blocked and allowed threat events based on feeds from intrusion prevention systems (IPS), antivirus, antispam engines, Juniper Sky ATP, and screen options. You can also click a specific geographical location to view the event count and the top five inbound and outbound IP addresses.



NOTE: To view the data on the Threats Map (Live) page, ensure that:

- Security logging is enabled. If not, go to **Configure > Device Settings > Basic Settings > Security Logging** and enable **Logging**.
- Required firewall policy is configured on the device.
- Required licenses are configured for IPS and antivirus.
- Your device is enrolled to the Juniper Sky ATP server.

The threat data is displayed starting from 12:00 AM (midnight) up to the current time (in your time zone) on that day and is updated every 30 seconds. The current date and time is displayed at the top right and a legend is displayed at the bottom left of the page.

If a threat occurs when you are viewing the page, an animation shows the country from which the threat originated (source) and the country in which the threat occurred (destination).



NOTE: Threats with unknown geographical IP addresses and private IP addresses are displayed as UNKNOWN_COUNTRY.

Field Descriptions

Table 107 on page 170 displays the fields of the Threats Map (Live) page.

Table 107: Fields on the Threats Map (Live) Page

Field	Description
Total Threats Blocked & Allowed	Displays the total number of threats blocked and allowed. Click the hyperlinked number to go to the All Events (Monitor > Events > All Events) page (filtered view of the Grid View tab), where you can view more information about the IPS, virus, spam, Juniper Sky ATP, and screen events.
Threats Blocked & Allowed	<p>Displays the total number of threats blocked and allowed by the following categories:</p> <ul style="list-style-type: none"> • IPS Threats • Virus • Spam • Screen • Juniper Sky ATP <p>Click the hyperlinked number for a category to go to the page for that category, where you can view more information about that category. For example, clicking the hyperlinked number for IPS threats takes you to the IPS (Monitor > Events > IPS) page (filtered view of the Grid View tab).</p>
Top Destination Countries	Displays the top five destination countries and the number of threats per country. Click the hyperlink for a country to go to the All Events (Monitor > Events > All Events) page (filtered view of the Grid View tab), where you can view more information about the IPS, virus, spam, Juniper Sky ATP, and screen events for that country.
Top Source Countries	Displays the top five source countries and the number of threats per country. Click the hyperlink for a country to go to the All Events (Monitor > Events > All Events) page (filtered view of the Grid View tab), where you can view more information about the IPS, virus, spam, Juniper Sky ATP, and screen events for that country.

Threat Types

The Threats Map (Live) page displays blocked and allowed threat events based on feeds from IPS, antivirus, antispam engines, Juniper Sky ATP, and screen options.

Table 108 on page 171 describes different types of threats blocked and allowed.

Table 108: Types of Threats

Attack	Description
IPS threat events	<p>Intrusion detection and prevention (IDP) attacks detected by the IDP module.</p> <p>The information reported about the attack (displayed on the IPS (Monitor > Events > IPS) page) includes information about:</p> <ul style="list-style-type: none"> • Specific events names • Specific event names with either source or destination country
Virus	<p>Virus attacks detected by the antivirus engine.</p> <p>The information reported about the attack (displayed on the Antivirus (Monitor > Events > Antivirus) page) includes information about:</p> <ul style="list-style-type: none"> • Specific events names • Specific event names with either source or destination country
Spam	<p>E-mail spam that is detected based on the blacklist spam e-mails.</p> <p>The information reported about the attack (displayed on the Antispam (Monitor > Events > Antispam) page) includes information about:</p> <ul style="list-style-type: none"> • Specific events names • Specific event names with source country
Juniper Sky ATP	<p>Events that are detected based on Juniper Sky ATP policies.</p> <p>The information reported about the attack (displayed on the Screen (Monitor > Events > ATP) page) includes information about:</p> <ul style="list-style-type: none"> • Specific events names • Specific event names with either source or destination country
Screen	<p>Events that are detected based on screen options.</p> <p>The information reported about the attack (displayed on the Screen (Monitor > Events > Screen) page) includes information about:</p> <ul style="list-style-type: none"> • Specific events names • Specific event names with either source or destination country

Tasks You Can Perform

You can perform the following tasks from this page:

- Toggle between updating the data and allowing live updates—Click the **Pause** icon to stop the page from updating the threat map data and to stop animations. Click the **Play** icon to update the page data and resume animations.
- Zoom in and out of the page—Click the zoom in (+) and zoom out (–) icons to zoom in and out of the page.
- Pan the page—Click and drag the mouse to pan the page.
- View country-specific details:

- Click a country on the threat map to view threat information specific to that country. A *Country-Name* pop-up appears displaying country-specific information.
- Click **View Details** in the *Country-Name* pop-up to view additional details. The *Country-Name (Details)* panel appears.

[Table 109 on page 172](#) provides more details on the country-specific threat information.

Table 109: Country-Specific Threat Information

Field	Description
Displayed in Country-Name pop-up	
<i>Number of threat events</i> Threat Events since 12:00 am	<p>Displays the total number of threat events (inbound and outbound) since midnight for that country.</p> <p>Click the hyperlinked number to go to the All Events (Monitor > Events > All Events) page, where you can view more information about the events.</p>
Inbound (<i>Number of threat events</i>)	<p>Displays the total number of inbound threats for the country and the IP address and the number of events for that IP address for the top five inbound events.</p> <p>Click View All to view all the destination IP address with threat events count.</p>
Outbound (<i>Number of threat events</i>)	<p>Displays the total number of outbound threats for the country and the IP address and the number of events for that IP address for the top five outbound events.</p> <p>Click View All to view all the source IP address with threat events count.</p>
View Details—Displayed in Country-Name (Details) panel	
<i>Number of threat events</i> Threat Events since 12:00 am	<p>Displays the total number of threat events (inbound and outbound) since midnight for that country.</p> <p>Click the hyperlinked number to go to the All Events (Monitor > Events > All Events) page, where you can view more information about the events.</p>

Table 109: Country-Specific Threat Information (continued)

Field	Description
Number of Inbound Events	<p>Displays the total number of inbound threats for the country and the number of inbound threat events for each of the following categories:</p> <ul style="list-style-type: none"> • IPS Threats • Virus • Spam • Screen • Juniper Sky ATP <p>Click the hyperlinked number for a category to go to the page for that category, where you can view more information about that category. For example, clicking the hyperlinked number for IPS threats takes you to the IPS (Monitor > Events > IPS) page.</p> <p>Click Top 5 IP Addresses (Inbound) to view the IP address and the number of events for that IP address for the top five inbound events.</p> <p>Click View All IP Addresses to view all the destination IP addresses and number of events for that IP address.</p> <p>NOTE: You can view or select View All IP Addresses only after you click Top 5 IP Addresses (Inbound).</p>
Number of Outbound Events	<p>Displays the total number of outbound threats for the country and the number of outbound threat events for each of the following categories:</p> <ul style="list-style-type: none"> • IPS Threats • Virus • Spam • Screen • Juniper Sky ATP <p>Click the hyperlinked number for a category to go to the page for that category, where you can view more information about that category. For example, clicking the hyperlinked number for screens takes you to the Screen (Monitor > Events > Screen) page.</p> <p>Click Top 5 IP Addresses (Outbound) to view the IP address and the number of events for that IP address for the top five outbound events.</p> <p>Click View All IP Addresses to view all the source IP addresses and number of events for that IP address.</p> <p>NOTE: You can view or select View All IP Addresses only after you click Top 5 IP Addresses (Outbound).</p>

- See Also**
- [Monitoring Flow Gate Information on page 100](#)
 - [Monitoring Firewall Authentication on page 101](#)

CHAPTER 3

Configure

- [Device Setup on page 175](#)
- [Interfaces on page 203](#)
- [Users on page 216](#)
- [Network on page 230](#)
- [Security on page 282](#)
- [Multi Tenancy on page 466](#)
- [Chassis Cluster on page 489](#)
- [CLI Tools on page 497](#)

Device Setup

- [Basic Settings on page 175](#)
- [Configuring Cluster \(HA\) Setup on page 190](#)
- [Set Up on page 200](#)
- [PPPoE on page 201](#)
- [VPN Wizard on page 202](#)
- [NAT Wizard on page 202](#)

Basic Settings

- [System Identity Configuration Page Options on page 175](#)
- [Date and Time Configuration Page Options on page 177](#)
- [Management Access Configuration Page Options on page 179](#)
- [Security Logging Configuration Page Options on page 185](#)
- [SNMP Configuration Page Options on page 187](#)

System Identity Configuration Page Options

1. Select **Configure>System Properties>System Identity** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Configure>Device Setup>Basic Settings>System Identity** in the J-Web user interface.

The System Identity configuration page appears.

2. (Junos OS Release 18.3R1 and later releases) Select **Configure>Device Settings>Basic Settings>System Identity Details** in the J-Web user interface.

[Table 110 on page 176](#) explains the contents of this page.

3. Click one:

- **Save**—Saves all the basic settings configuration and returns to the main configuration page.



NOTE: For all the configuration options under Basic Settings:

- Tool tip on the right-side represents different icons for notifications, validation errors, and successful configuration.
- When you make a configuration change and navigate to a different page without saving it, a pop-up message is displayed to save the configuration.

- **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
- **Cancel**—Cancels all your entries and returns to the main configuration page.

Table 110: System Identity Details Configuration Details

Field	Function	Action
Host Name	Specifies the hostname of the device.	Enter a name.
Domain Name	Specifies the network or subnetwork to which the device belongs.	Enter a name.
Root Password	Specifies a password for the root user. NOTE: After you have defined a root password, that password is required when you log in to the J-Web or the CLI.	Enter a password.
Confirm Password	Specifies the password for the root user.	Re-enter the password.

Table 110: System Identity Details Configuration Details (continued)

Field	Function	Action
DNS Servers	<p>Specifies the DNS server settings. The options available are:</p> <ul style="list-style-type: none"> • Add • Edit • Delete 	<p>Select an option:</p> <ul style="list-style-type: none"> • To specify a server that the device can use to resolve hostnames into addresses, click Add in the DNS Servers section. Then, enter the IP address of the server in the Add DNS Server dialog box and click OK. • To edit an existing DNS server hostname, select it and click Edit or right-click on it and click Edit Row. Then, edit the IP address in the Edit DNS Server dialog box and click OK. • To remove an existing DNS server hostname, select it and click Delete or right-click on it and click Delete Row.
Domain Search	<p>Specifies the DNS hostname settings. The options available are:</p> <ul style="list-style-type: none"> • Add • Edit • Delete 	<p>Select an option:</p> <ul style="list-style-type: none"> • To include the device's domain name in a DNS search, click Add in the Domain Search section. Then enter the domain name in the Add Domain Search dialog box and click OK. • To edit an existing domain name, select it and click Edit or right-click on it and click Edit Row. Then, edit the domain name in the Edit Domain Search dialog box and click OK. • To remove an existing domain name, select it and click Delete or right-click on it and click Delete Row.

- See Also**
- [Management Access Configuration Page Options on page 179](#)
 - [User Management Configuration Page Options on page 216](#)
 - [Date and Time Configuration Page Options on page 177](#)

Date and Time Configuration Page Options

1. Select **Configure>System Properties>Date and Time** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platform.
Or
Select **Configure>Device Setup>Basic Settings>Date Time** in the J-Web user interface.
The Date and Time configuration page appears.

2. (Junos OS Release 18.3R1 and later releases) Select **Configure>Device Setup>Basic Settings>Date & Time Details** in the J-Web user interface. [Table 111 on page 178](#) explains the contents of this page.

3. Click one:

- **Save**—Saves all the basic settings configuration and returns to the main configuration page.



NOTE: For all the configuration options under Basic Settings:

- Tool tip on the right-side represents different icons for notifications, validation errors, and successful configuration.
 - When you make a configuration change and navigate to a different page without saving it, a pop-up message is displayed to save the configuration.
-
- **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
 - **Cancel**—Cancels all your entries and returns to the main configuration page.

Table 111: Date and Time Configuration Details

Field	Function	Action
Time Zone	Specifies the time zone in which the router resides.	Select a time zone from the list.
Current date/time	Displays the current date and time.	—

Table 111: Date and Time Configuration Details (continued)

Field	Function	Action
Time Source	Specifies which method the device should use to set the system time.	
	<p>Sync with NTP Server—Synchronizes the system time with the NTP server that you select. The available options are:</p> <ul style="list-style-type: none"> • Add • Edit. • Delete 	<p>Select an option.</p> <ul style="list-style-type: none"> • To add an NTP server, click Add. Then, enter the NTP server, key, and version in the Add NTP Server dialog box, and click OK. • To edit the settings for an existing NTP server, select it and click Edit or right-click on it and click Edit Row. Then, edit the key and version in the Edit NTP Server dialog box, and click OK. • To delete an existing NTP server, select it and click Delete or right-click on it and click Delete Row, and click OK.
	<p>Sync with Computer Time—Uses the computer that you are currently logged into to determine the system time for the device.</p>	When you select this option, the PC time that will be used is displayed in the Current Date & Time field.
	<p>Manual Configure Time—Enables you to manually select the date and time for the device.</p> <p>NOTE: After you configure the time manually, the session will expire. Log in to J-Web.</p>	Set the date and time using the calendar pick tool and time fields.

- See Also**
- [System Identity Configuration Page Options on page 175](#)
 - [Management Access Configuration Page Options on page 179](#)
 - [User Management Configuration Page Options on page 216](#)

Management Access Configuration Page Options

1. Select **Configure>System Properties>Management Access** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platform.

Or

Select **Configure>Device Setup>Basic Settings>Management Access** in the J-Web user interface.

The Management Access configuration page appears.

2. (Junos OS Release 18.3R1 and later releases) Select **Configure>Device Setup>Basic Settings>Management Access Configuration** in the J-Web user interface.

[Table 112 on page 180](#) explains the contents of this page.

3. Click one:

- **Save**—Saves all the basic settings configuration and returns to the main configuration page.



NOTE: For all the configuration options under Basic Settings:

- Tool tip on the right-side represents different icons for notifications, validation errors, and successful configuration.
- When you make a configuration change and navigate to a different page without saving it, a pop-up message is displayed to save the configuration.

- **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
- **Cancel**—Cancels all your entries and returns to the main configuration page.

Table 112: Management Access Configuration Details

Field	Function	Action
Loopback Address	Specifies a loopback address for the device.	Enter the IP address. NOTE: If the SRX device does not have a dedicated management port (fxp0), then Loopback Address and Subnet are the only options available for the management access configuration.
Subnet	Specifies the range of logical addresses within the address space that is assigned to an organization.	Enter the address, for example, 255.255.255.0. You can also specify the address prefix.
IPv4	Displays whether or not IPv4 is enabled.	Select this option to enable IPv4. NOTE: IPv4 configuration is supported only on the SRX devices with fxp0 port.
Management Access Port	Specifies an IPv4 address for the device.	Enter the IP address.
Subnet	Specifies the range of logical addresses within the address space that is assigned to an organization.	Enter the address, for example, 255.255.255.0. You can also specify the address prefix.
Default Gateway	Specifies the default gateway address for IPv4.	Enter the IP address.
Services		

Table 112: Management Access Configuration Details (continued)

Field	Function	Action
Telnet	Provides secure Telnet connections.	Select this option to enable telnet.
SSH	Provides secure SSH connections.	Select this option to enable SSH.
FTP	Provides secure file transfers	Select this option to enable FTP.
Netconf	Provides NETCONF connections.	Select this option to enable NETCONF.
RFC Complaint	Provides NETCONF sessions complaint with RFC 4741.	Select this option to enable RFC complaint.
Netconf -> SSH	Provides NETCONF connections over SSH connections.	Select this option to enable Netconf -> SSH.
Trace Options	Provides NETCONF trace options.	Select this option to enable trace options.
On Demand	Provides on-demand tracing.	Select this option to enable on-demand.
No Remote Trace	Disables remote tracing.	Select this option to enable no remote tracing.
Junoscript Over Clear Text	Provides clear text based Junoscript connections.	Select this option to enable Junoscript over clear text.
Junoscript Over SSL	Provides SSL based Junoscript connections.	Select this option to enable Junoscript over SSL.
Junoscript Certificate	Provides the local certificate for SSL.	Select the local certificate for SSL from the list.
HTTP	Enables unencrypted HTTP connection settings.	Select this option to enable HTTP.
Interface	Provides interfaces that accept HTTP access.	Select the interface in order of your preference and click on the left arrow/right arrow to add.
HTTPS	Enables encrypted HTTPS connection settings.	Select this option to enable HTTPS.
Interface	Provides interfaces that accept HTTPS access.	Select the interface in order of your preference and click on the left arrow/right arrow to add.
HTTPS Certificate	Specifies the certificate that you want to use to secure the connection from the HTTPS certificates list when you enable HTTPS.	Select the HTTPS certificate form the list.

Table 112: Management Access Configuration Details (continued)

Field	Function	Action
HTTPS Port	Provides TCP ports for incoming HTTPS connections.	Select the HTTPS port by clicking top or bottom arrows.
WEB API		
Web API	Enables Web API configuration.	Select this option to enable Web API.
Client	Enables client for the Web API.	Select this option to enable client.
Host Name	Provides the address of permitted HTTP/HTTPS request originators.	Select this option to add or delete the address of permitted HTTP/HTTPS request originators. To add, click + and enter the IPv4 address of the request originator.
HTTP	Enables unencrypted HTTP connection settings.	Select this option to enable HTTP.
HTTP Port	Provides TCP ports for incoming HTTP connections.	Select this option to enable HTTP port.
HTTPSs	Enables encrypted HTTPS connection settings.	Select this option to enable HTTPS.
HTTPS Port	Provides TCP ports for incoming HTTPS connections.	Click top or bottom arrows to select the HTTPS port.

Table 112: Management Access Configuration Details (continued)

Field	Function	Action
Certificate Type	Specifies the certificate that you want to use to secure the connection from the HTTPS certificates list when you enable HTTPS for Web API.	Select an option.
	Default	-
	PKI Certificate	The option available is PKI Certificate . Select a PKI certificate from the list for HTTPS of Web API.
	File Path	<p>The options available are as follows:</p> <ul style="list-style-type: none"> • File Path: <ul style="list-style-type: none"> • Browse—Click and select a certificate from your desired location. • Upload—Click and upload the selected certificate. • Certificate—Displays the file path of the uploaded certificate. • Certificate Key: <ul style="list-style-type: none"> • Browse—Click and select the certificate key from your desired location. • Upload—Click and upload the selected certificate key. • Certificate Key—Displays the file path of the uploaded certificate key.
User	Provides the user credential details.	Select this option to enable user.
Name	Specifies the username.	Enter the username.
Password	Specifies the user password.	Enter the password.
REST API		
REST API	Allows RPC execution over HTTP(S) connection.	Select this option to enable REST API.
Explorer	Provides the REST API explorer tool.	Select this option to enable REST API explorer.
Control	Controls the REST API process.	Select this option to enable control.
Allowed Sources	Provides the source IP address.	Click + and enter the IPv4 address of the source.

Table 112: Management Access Configuration Details (continued)

Field	Function	Action
Connection Limit	Provides the maximum number of simultaneous connections.	Click top or bottom arrows to select the number of simultaneous connections.
HTTP	Enables unencrypted HTTP connections for REST API.	Select this option to enable HTTP.
Address	Provides addresses for the incoming connections for HTTP of REST API.	Click + and enter the IPv4 address.
Port	Provides ports to accept HTTP connections for REST API.	Click top or bottom arrows to select the HTTP port. NOTE: The default port for HTTP of REST API is 3000.
HTTPS	Enables encrypted HTTPS connections for REST API.	Select this option to enable HTTPS.
Address	Provides addresses for the incoming connections for HTTPS of REST API.	Click + and enter the IPv4 address.
Cipher List	Provides the Cipher suites for HTTPS of REST API.	Select the Cipher suites in order of your preference and click on the left arrow or right arrow to add.
Port	Provides the port to accept the HTTPS connection of REST API.	Click top or bottom arrows to select the HTTPS port. NOTE: The default port for HTTPS of REST API is 3443.
Server Certificate	Provides the server certificate for HTTPS of REST API.	Select the server certificate from the list.

Table 112: Management Access Configuration Details (continued)

Field	Function	Action
Certificate Authority Profile	Provides the certificate authority profile for HTTPS of REST API.	<p>Select the certificate authority profile from the list.</p> <p>To create Certificate Authority:</p> <ul style="list-style-type: none"> Click Create Certificate Authority Profile. Enter the following details: <ul style="list-style-type: none"> CA Profile *—Enter the CA profile name. CA Identifier *— File Path on Device for Certificate: <ul style="list-style-type: none"> Browse—Click and select the certificate from your desired location. Upload—Click and upload the selected certificate. File Path on Device for Certificate—Displays the file path of the selected certificate. Click OK.
Certificate		
Certificate	Specifies the certificate name to secure HTTPS connections.	<p>Select an option:</p> <ul style="list-style-type: none"> To add a new certificate, click +. Then enter the certificate name and certificate content in the Create certificate page, and then click OK. To edit an existing certificate, select it and click Edit or right-click on it and click Edit Row. Then, edit the certificate content in the Edit Certificate page and click OK. To delete an existing certificate, select it and click Delete or right-click on it and click Delete Row.

- See Also**
- [System Identity Configuration Page Options on page 175](#)
 - [User Management Configuration Page Options on page 216](#)
 - [Date and Time Configuration Page Options on page 177](#)

Security Logging Configuration Page Options

J-Web enables you to forward logs using stream mode and event mode. All the categories can be configured for sending specific category logs to different log servers in stream mode log forwarding.

1. Select **Configure>Device Setup>Basic Settings>Security Logging** in the J-Web user interface.

The Security Logging configuration page appears.



NOTE: Starting in Junos OS 19.1R1, Security Logging page supports only Stream Mode.

2. Select **Apply** to apply the security log settings.

Table 113: Security Logging Configuration Page

Field	Function	Action
Logging	Enables the security logging.	Select this option to enable logging. NOTE: Starting in Junos OS Release 19.1R1, the Enable Traffic Logs option is available for user logical system and tenants.
UTC Timestamp	Allows use of Coordinated Universal Time (UTC) for security log timestamps.	Select this option to enable UTC Timestamp.
Log On	Provides log on types for logging.	Select Source Address or Source Interface .
IP Address	Specifies a source IP address or the IP address used when exporting security logs.	Enter the IP address.
Interface	Specifies the interface of the log source.	Select the interface from the list.
Format	Specifies the format in which the logs are stored.	Select the logging format. By default, None logging format is selected. Options available are: <ul style="list-style-type: none"> • binary—Binary encoded text to conserve resources. • SD-Syslog—Structured system log file. • Syslog—Traditional system log file.
Transport Protocol	Specifies the type of transport protocol to be used to log the data.	Select the logging transport protocol. By default, None is selected. Options available are: <ul style="list-style-type: none"> • TCP—Set the transport protocol to TCP. • UDP—Set the transport protocol to UDP. • TLS—Set the transport protocol to TLS.

Table 113: Security Logging Configuration Page (continued)

Field	Function	Action
Syslog Server	Enables you to configure syslog servers. You can configure a maximum of three syslog servers.	<p>Select an option:</p> <ul style="list-style-type: none"> To create syslog server, click +, enter the following details and then click OK. <ul style="list-style-type: none"> Name—Enter the name of the new stream configuration. Save At—Select the location from the drop-down list to save the stream. Type—Select a format in which the logs are stored from the drop-down list. The log types are: <ul style="list-style-type: none"> Structure Standard Web Host—Enter the IP address for the stream host name. To edit an existing syslog server, select it and click Edit. Then, edit the saving mode, streaming type, and host in the Edit Syslog page and click OK. To delete an existing syslog server, select it and click Delete.

See Also • [Monitoring Application Statistics \(Application Tracking\) on page 119](#)

SNMP Configuration Page Options

1. Select **Configure>Service>SNMP** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platform.

Or

Select **Configure>Device Setup>Basic Settings>SNMP** in the J-Web user interface.

The SNMP configuration page appears.

2. (Junos OS Release 18.3R1 and later releases) Select **Configure>Device Setup>Basic Settings>SNMP** in the J-Web user interface.
3. Click one:
 - **Save**—Saves all the basic settings configuration and returns to the main configuration page.



NOTE: For all the configuration options under Basic Settings:

- Tool tip on the right-side represents different icons for notifications, validation errors, and successful configuration.
 - When you make a configuration change and navigate to a different page without saving it, a pop-up message is displayed to save the configuration.
- **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
 - **Cancel**—Cancels all your entries and returns to the main configuration page.

Table 114: SNMP Configuration Details

Field	Function	Action
Contact Information	Specifies the administrative contact for the system.	Enter any contact information for the administrator of the system (such as name and phone number).
System Description	Specifies the description for the system.	Enter any information that describes the system.
Local Engine ID	Specifies the administratively unique identifier of an SNMPv3 engine for system identification. The local engine ID contains a prefix and a suffix. The prefix is formatted according to specifications defined in RFC 3411. The suffix is defined by the local engine ID. Generally, the local engine ID suffix is the MAC address of Ethernet management port 0.	Enter the MAC address of Ethernet management port 0.
System Location	Specifies the location of the system.	Enter any location information for the system (lab name or rack name, for example).
System Name Override	Specifies the option to override the system hostname.	Enter the name of the system.
Community	Specifies the name and authorization for the SNMP community.	<ul style="list-style-type: none"> • Click +. • Enter the name of the community being added. • Select the desired authorization (either read-only or read-write) from the list.
Trap Groups		
Name	Specifies the name of the SNMP trap group being configured.	Enter the SNMP trap group name.

Table 114: SNMP Configuration Details (continued)

Field	Function	Action
Categories	<p>Specifies which trap categories to add to the trap group being configured. The options available are:</p> <ul style="list-style-type: none"> • Authentication • Chassis • Configuration • Link • Remote operations • RMON alarm • Routing • Startup • CRRP events 	Select an option.
Targets	Specifies one or more IP addresses that specify the systems to receive SNMP traps that are generated by the trap group being configured.	Click + , enter the target IP address for SNMP trap group, and click OK .
Health Monitoring	<p>Specifies the option to check the SNMP health monitor on the device. The health monitor periodically checks the following key indicators of device health:</p> <ul style="list-style-type: none"> • Percentage of file storage used • Percentage of Routing Engine CPU used • Percentage of Routing Engine memory used • Percentage of memory used for each system process • Percentage of CPU used by the forwarding process • Percentage of memory used for temporary storage by the forwarding process 	Enable the option.
Interval	Specifies the sampling frequency interval, in seconds, over which the key health indicators are sampled and compared with the rising and falling thresholds. For example, if you configure the interval as 100 seconds, the values are checked every 100 seconds.	Enter a value from 1 through 24855. The default value is 300 seconds.
Rising Threshold	Specifies the value at which you want SNMP to generate an event (trap and system log message) when the value of a sampled indicator is increasing. For example, if the rising threshold is 90, SNMP generates an event when the value of any key indicator reaches or exceeds 90 seconds.	Enter a value from 1 through 100. The default value is 90 seconds.

Table 114: SNMP Configuration Details (continued)

Field	Function	Action
Falling Threshold	Specifies a value at which you want SNMP to generate an event (trap and system log message) when the value of a sampled indicator is decreasing. For example, if the falling threshold is 80, SNMP generates an event when the value of any key indicator falls back to 80 seconds or less.	Enter a value 0 through 100. The default value is 80 seconds.

See Also • [Boot DHCP Relay Configuration Page Options](#)

Configuring Cluster (HA) Setup

The Junos OS provides high availability on SRX Series device by using chassis clustering. SRX Series Services Gateways can be configured to operate in cluster mode, where a pair of devices can be connected together and configured to operate like a single node, providing device, interface, and service level redundancy.

A chassis cluster can be configured in the following modes:

- **Active/passive mode:** In active/passive mode, transit traffic passes through the primary node while the backup node is used only in the event of a failure. When a failure occurs, the backup device becomes master and takes over all forwarding tasks.
- **Active/active mode:** In active/active mode, has transit traffic passing through both nodes of the cluster all of the time.



NOTE: In the J-Web cluster (HA) setup, you can only configure active/passive mode (RG1). Navigate to **Configure > Device Settings > Cluster Configuration** to configure active/active mode (RG1+).

You can set up chassis cluster using a simplified Cluster (HA) Mode wizard when the standalone SRX Series devices are in factory default. You can also create HA using the same wizard from **Configure > Device Settings > Cluster (HA) Setup** when the devices are already in the network.



NOTE:

In the factory default settings:

- A warning message is displayed in SRX300, SRX320, SRX320-POE, SRX340, and SRX345 devices to disconnect the ports between the two nodes. This is to avoid displaying the details of the other nodes.
- The Cluster (HA) Mode Wizard is supported only on SRX300, SRX320, SRX320-POE, SRX340, SRX345, SRX550M, SRX4100, and SRX4200 devices.

Before you begin:

- Establish a chassis cluster connection between the two units, ensure that you have physical access to both the devices.
- You must configure the two devices separately.
- Your other unit must be on the same hardware and software version as the current unit.
- Note that both units are erased and rebooted, after which all existing data is irretrievable. You have the option to save a backup copy of your configuration before rebooting.

To set up cluster (HA):

1. Select **Configure > Device Setup > Cluster (HA) Setup**.

The Chassis Cluster Setup Wizard configuration page appears. This wizard guides you through configuring chassis cluster on a two-unit cluster.

Select the unit

The welcome page shows the possible chassis cluster connections that you can configure for your SRX Series device. It shows a graphical representation for primary unit (Node 0) and secondary unit (Node 1) and guides you to first configure the primary unit (node 0).

2. Select **Yes, this is the primary unit (Node 0)** to select the unit.



NOTE: If you have already configured the primary node settings, then select **No, this is the secondary unit (Node 1)** and follow the instructions from [Step 8](#).

3. Click **Next**.
4. To configure the primary unit, complete the configuration according to the guidelines provided in [Table 115 on page 193](#).
5. Click **Reboot and Continue** to restart the primary unit to configure chassis cluster.
6. After rebooting the primary unit (node 0), connect to the management port of the secondary unit to switch to the secondary unit.
7. Click **Refresh** if the management IP address of the secondary unit is same as the existing device default IP address. If not, open a new browser with the new secondary device IP address.

8. To configure the secondary unit, complete the configuration according to the guidelines provided in [Table 116 on page 196](#).
9. Click **Reboot and Continue** to restart the secondary unit to configure chassis cluster.
10. After rebooting the secondary unit (node 1), launch the J-Web UI using primary unit management IP address.
11. Navigate to the Cluster Status step in the wizard.



NOTE:

- J-Web uses **show chassis cluster status** to verify control link status. Number on the link signifies if it is single (1) or dual links (2).

The control and fabric link status colors are as follows:

- Green—Indicates that the links are up.
- Red—Indicates that the links are down.
- Orange—Indicates that one of the dual links is up.
- Grey—Indicates that the fabric link is not configured.
- If chassis cluster is not connected, then the connection is failed and the all possible failure reasons will be displayed. For information on troubleshooting tips, see [Juniper Knowledge Search](#).
- You can configure fabric link only after the chassis cluster is formed. For the first time configuration, the chassis status displays as **The fabric ports links is not yet configured**.

12. To configure fabric link, complete the configuration according to the guidelines provided in [Table 117 on page 197](#).
13. Click **Configure Link**.
14. Click **Next**.
15. To add redundant Ethernet (reth) interface, click **+** and complete the configuration according to the guidelines provided in [Table 118 on page 198](#).



NOTE: You can also use the pencil icon to edit the reth interface and delete icon to delete the reth interfaces.

16. Click **Save**.

Virtual reth interface is created.

17. To add a logical interface to the new virtual reth interfaces, complete the configuration according to the guidelines provided in [Table 119 on page 199](#).

18. Click **OK**.

19. To configure zones, complete the configuration according to the guidelines provided in [Table 120 on page 199](#).



NOTE:

- With factory default configuration, trust and untrust zones are displayed by default.
- You can edit the security zone, add new zones, and delete the newly added zones. You will receive an error message while committing if you try to delete a default zone. This is because, the default zones are referenced in the security policies.
- You can also edit zone description, application tracking, source identity log, interfaces, system services, protocols, and traffic control options.

20. Click **OK**.

21. Click **Finish**.

A cluster setup success message appears.

If you click the Cluster (HA) Setup menu again, a cluster setup success message appears and you can click **Cluster Configuration** to view and edit the chassis cluster configuration.



NOTE: If the chassis cluster configuration fails after you click **Finish**, then edit the configuration as required and commit the changes again.

Table 115: Primary Unit Configuration

Field	Description	Action
System Identity		
Node 0 Cluster ID	Specifies the number by which a cluster is identified.	Enter a number from 1 through 255. By default, 1 is assigned.
Node 0 Priority	Specifies the device priority for being elected to be the master device in the VRRP group.	Enter a number from 1 through 255. By default, 200 is assigned.

Table 115: Primary Unit Configuration (continued)

Field	Description	Action
Node 1 Priority	Specifies the device priority for being elected to be the master device in the VRRP group.	Enter a number from 1 through 255. By default, 100 is assigned.
Node 0 Host Name	Specifies the device host name of the node 0.	By default, host name is assigned. For example, SRX1500-01.
Node 1 Host Name	Specifies the device host name of the node 1.	By default, host name is assigned. For example, SRX1500-02.
Allow root user SSH login	Allows users to log in to the device as root through SSH.	Enable this option.

Management Interface

IPv4 Address

NOTE: Make a note of the IPv4 address as you need it to access the settings after you commit the configuration.

Node 0 Management IPv4	Specifies the management IPv4 address of node 0.	Enter a valid IPv4 address for the management interface.
Node 0 Subnet Mask	Specifies subnet mask for IPv4 address.	Enter a subnet mask for the IPv4 address.
Node 1 Management IPv4	Specifies the management IPv4 address of node 1.	Enter a valid IPv4 address for the management interface.
Node 1 Subnet Mask	Specifies subnet mask for IPv4 address.	Enter a subnet mask for the IPv4 address.
Static Route IP	Defines how to route to the other network devices.	Enter an IPv4 address for the static route.
Static Route Subnet	Specifies the subnet for the static route IPv4 address.	Enter a subnet mask for the static route IPv4 address.
Next Hop IPv4	Specifies next hop gateway for the IPv4 address.	Enter a valid IPv4 address for the next hop.

IPv6 Address (Optional)

Node 0 Management IPv6	Specifies the management IPv6 address of node 0.	Enter a valid IPv6 address for the management interface.
Node 0 Subnet Prefix	Specifies subnet prefix for IPv6 address.	Enter a subnet prefix for the IPv6 address.
Node 1 Management IPv6	Specifies the management IPv6 address of node 1.	Enter a valid IPv6 address for the management interface.
Node 1 Subnet Prefix	Specifies subnet prefix for IPv6 address.	Enter a subnet prefix for the IPv6 address.

Table 115: Primary Unit Configuration (continued)

Field	Description	Action
Static Route IPv6	Defines how to route to the other network devices.	Enter an IPv6 address for the static route.
Static Route Subnet Prefix	Specifies the subnet prefix for the static route IPv6 address.	Enter a subnet prefix for the static route IPv6 address.
Next Hop IPv6	Specifies next hop gateway for the IPv6 address.	Enter a valid IPv6 address for the next hop.
Device Password		
Root Password	Specifies root password of the device.	Enter root password if not already configured for the device.
Re-Enter Password	-	Reenter the root password.
Control Ports		
NOTE: This option is available only for SRX5600 and SRX5800 devices.		
Dual Link	Provides redundant link for failover.	<p>By default, this option is disabled.</p> <p>Once you enable this option, the following fields appear:</p> <ul style="list-style-type: none"> • Link 1 <ul style="list-style-type: none"> • Node 0 FPC—Select an option from the list. • Node 0 Port—Select an option from the list. • Node 1 FPC. • Node 1 Port. • Link 2 (Optional) <ul style="list-style-type: none"> • Node 0 FPC—Select an option from the list. • Node 0 Port—Select an option from the list. • Node 1 FPC. • Node 1 Port.
Node 0 FPC	Specifies FPC slot number on which to configure the control port.	Select an option from the list.
Node 0 Port	Specifies port number on which to configure the control port.	Select an option from the list.
Node 1 FPC	Optional. Specifies FPC slot number on which to configure the control port.	Select an option from the list.

Table 115: Primary Unit Configuration (continued)

Field	Description	Action
Node 1 Port	Optional. Specifies port number on which to configure the control port.	Select an option from the list.
Save Backup (Optional)		
Save Backup (to client)	Saves backup of the current configuration to the client local machine. NOTE: When restarting the primary unit, J-Web deletes the existing configuration to configure chassis cluster. Therefore, it is recommended that you save a backup file of your current settings before committing the new configuration.	Enable the option to save the backup file of your settings.

Table 116: Secondary Unit Configuration

Field	Description	Action
Secondary Unit Information		
Cluster ID	Specifies the number by which a cluster is identified. NOTE: Cluster ID must be same for both primary and secondary units.	Enter a number from 1 through 255. By default, 1 is assigned.
Device Password		
Root Password	Specifies root password of the device.	Enter new root password.
Re-Enter Password	-	Reenter the root password.
Control Ports		
NOTE: This option is available only for SRX5600 and SRX5800 devices.		

Table 116: Secondary Unit Configuration (continued)

Field	Description	Action
Dual Link	Provides redundant link for failover.	<p>By default, this option is disabled.</p> <p>Once you enable dual link option, the following fields appear:</p> <ul style="list-style-type: none"> • Link 1 <ul style="list-style-type: none"> • Node 0 FPC—Select an option from the list. • Node 0 Port—Select an option from the list. • Node 1 FPC. • Node 1 Port. • Link 2 (Optional) <ul style="list-style-type: none"> • Node 0 FPC—Select an option from the list. • Node 0 Port—Select an option from the list. • Node 1 FPC. • Node 1 Port.
Node 0 FPC	Specifies FPC slot number on which to configure the control port.	Select an option from the list.
Node 0 Port	Specifies port number on which to configure the control port.	Select an option from the list.
Node 1 FPC	Optional. Specifies FPC slot number on which to configure the control port.	Select an option from the list.
Node 1 Port	Optional. Specifies port number on which to configure the control port.	Select an option from the list.
Save Backup (Optional)		
Save Backup (to client)	<p>Saves backup of the current configuration to the client local machine.</p> <p>NOTE: When restarting the secondary unit, J-Web deletes the existing configuration to configure chassis cluster. Therefore, it is recommended that you save a backup file of your current settings before committing the new configuration.</p>	Enable the option to save the backup file of your settings.

Table 117: Fabric Link Configuration

Field	Description	Action
Fabric Link Details		

Table 117: Fabric Link Configuration (continued)

Field	Description	Action
Dual Link	Provides redundant link for failover.	Enable this option.
Link 1		
Fabric 0	Specifies the fabric port link for node 0.	Select an interface from the list.
Fabric 1	Specifies the fabric port link for node 1.	-
Link 2 (Optional)		
Fabric 0	Specifies the secondary fabric port link for node 0.	Select an interface from the list.
Fabric 1	Specifies the secondary fabric port link for node 1.	-

Table 118: Add Reth Interface

Field	Description	Action
RETH Name	Specifies the reth interface name.	Enter a name for reth interface.
Node 0 Interfaces	Specifies the list of Node 0 interfaces.	Select an interface from the Available column and move it to the Selected column.
Node 1	Specifies the Node 1 interfaces based on the node 0 interfaces.	-
Advance Settings		
LACP Configuration	Optional. Configure Link Aggregation Control Protocol (LACP).	-
LACP Mode	Optional. Specifies the LACP mode. Available options are: <ul style="list-style-type: none"> • active—Initiate transmission of LACP packets. • passive—Respond to LACP packets. • periodic—Interval for periodic transmission of LACP packets. 	Select an option from the list.
Periodicity	Optional. Specifies the interval at which the interfaces on the remote side of the link transmit link aggregation control protocol data units (PDUs). Available options are: <ul style="list-style-type: none"> • fast—Transmit link aggregation control PDUs every second. • slow—Transmit link aggregation control PDUs every 30 seconds. 	Select an option from the list.
Description	Optional. Specifies the description for LACP.	Enter a description.
VLAN Tagging	Optional. Specifies whether or not to enable VLAN tagging.	Enable this option.

Table 118: Add Reth Interface (continued)

Field	Description	Action
Redundancy Group	Specifies the number of the redundancy group that the reth interface belongs to.	-

Table 119: Add Reth Logical Interface

Field	Description	Action
General		
Reth Interface Name	Specifies the name of the reth interface.	Enter a name for the reth interface.
Logical Interface Unit	Specifies the logical interface unit.	Enter the logical interface unit.
Description	Specifies the description of the reth interface.	Enter the description.
VLAN ID	Optional. Specifies the VLAN ID.	Enter the VLAN ID.
IPv4 Address		
IPv4 Address	Specifies the IPv4 address.	Click + and enter a valid IP address.
Subnet Mask	Specifies the subnet mask for IPv4 address.	Enter a valid subnet mask.
IPv6 Address (Optional)		
IPv6 Address	Specifies the IPv6 address.	Enter a valid IP address.
Prefix Length	Specifies the number of bits set in the subnet mask.	Enter the prefix length.

Table 120: Create Zones

Field	Description	Action
General Information		
Name	Specifies the name of the zone.	Enter a name for the zone.
Description	Specifies a description for the zone.	Enter a description for the zone.
Application Tracking	Enables application tracking (AppTrack) to collect statistics for the application usage on the device, and when the session closes	Enable this option.
Source Identity Log	Specifies the source-identity-log parameter as part of the configuration for a zone to enable it to trigger user identity logging when that zone is used as the source zone (from-zone) in a security policy.	Enable this option.

Table 120: Create Zones (continued)

Field	Description	Action
Interfaces		
Interfaces	Specifies the list of reth interfaces available.	Select an interface from the Available column and move it to the Selected column.
System Services		
Except	Drops the selected services.	Enable this option if you want to drop the selected services.
Services	Specify the types of incoming system service traffic that can reach the device for all interfaces in a zone.	Select a service from the Available column and move it to the Selected column.
Protocols		
Except	Drops the selected protocols.	Enable this option if you want to drop the selected protocols.
Protocols	Specify the types of routing protocol traffic that can reach the device on a per-interface basis.	Select a protocol from the Available column and move it to the Selected column.
Traffic Control Options		
TCP Reset	Specifies the device to send a TCP segment with the RST (reset) flag set to 1 (one) in response to a TCP segment with any flag other than SYN set and that does not belong to an existing session.	Enable this option.

See Also • [Chassis Cluster Configuration Page Options on page 489](#)

Set Up

You can use the Setup wizard to configure a device or edit an existing configuration.

- Use the **Edit Existing Configuration** mode if you have already configured the device using the factory mode.
- Use the **Create New Configuration** mode to configure a device using the wizard.

Using the Setup wizard, you can configure the following:

- Basic settings
- Security topology
- Security policy
- Network Address Translation

**NOTE:**

On all branch SRX Series devices, the New Setup wizard has the following limitations:

- The Existing Edit mode might not work as expected if you previously configured the device manually, without using the wizard.
- Edit mode might overwrite outside configurations such as Custom Application, Policy Name, and zone inbound services.
- In create new mode, when you commit your configuration changes, your changes will overwrite the existing configuration.
- VPN and NAT wizards are not compatible with the New Setup wizard; therefore the VPN or NAT wizard configuration will not be reflected in the New Setup wizard or vice versa.
- By default, 2 minutes are required to commit a configuration using the New Setup wizard.
- On SRX650 devices, the default mode configures only the ge-0/0/1 interface under the internal zone.
- You might encounter usability issues if you use Microsoft Internet Explorer version 8 to launch the New Setup wizard.
- If you refresh your browser after you download the license, the factory mode wizard is not available.
- When you commit the configuration, the underlying Web management interface changes, and you do not receive a response about the commit status.
- Webserver ports 80 (HTTP) and 443 (HTTPS) on the DMZ or internal zone are overshadowed if Web management is enabled on the Internet zone not configured for destination NAT. As a workaround, change the webserver port numbers for HTTP and HTTPS by editing the recommended policies on the Security policies page.
- Images, buttons, and spinner (indicating that the configuration is being applied) on the wizard screen do not initially appear when the browser cache is cleared.

PPPoE

PPPoE connects multiple hosts on an Ethernet LAN to a remote site through a single customer premises equipment (CPE) device (Juniper Networks device).

Use the configure PPPoE tasks to configure the PPPoE connection. The PPPoE wizard guides you to set up a PPPoE client over the Ethernet connection.

**NOTE:**

On all branch SRX Series devices, the PPPoE wizard has the following limitations:

- While you use the load and save functionality, the port details are not saved in the client file.
- The Non Wizard connection option cannot be edited or deleted through the wizard. Use the CLI to edit or delete the connections.
- The PPPoE wizard cannot be launched if the backend file is corrupted.
- The PPPoE wizard cannot be loaded from the client file if non-wizard connections share the same units.
- The PPPoE wizard cannot load the saved file from one platform to another platform.
- There is no backward compatibility between PPPoE wizard Phase 2 to PPPoE wizard Phase 1. As a result, the PPPoE connection from Phase 2 will not be shown in Phase 1 when you downgrade to an earlier release.

VPN Wizard

A virtual private network (VPN) provides a means for secure communication among remote computers across a public WAN, such as the Internet.

This wizard leads you through the basic required steps to configure basic settings for a router-based VPN. To configure a VPN with a complete set of options, use either the J-Web interface or the command-line interface (CLI).

As you use this wizard, refer to the upper left area of the page to see where you are in the configuration process. Refer to the lower left area of the page for help related to the current page and its contents.

When you click a link under the Resources heading in the lower left area, the document opens in your browser. If it is in a new tab, be sure to close only the tab (not the browser window) when you close the document.

NAT Wizard

Network Address Translation (NAT) is a method for modifying or translating network address information in packet headers. Either one or both of the source and destination addresses in a packet may be translated. NAT can also include the translation of port numbers.

The NAT type determines the order in which NAT rules are processed. During the first packet processing for a flow, NAT rules are applied in the following order:

1. Static NAT rules
2. Destination NAT rules

3. Route lookup
4. Security policy lookup
5. Reverse mapping of static NAT rules
6. Source NAT rules

This wizard leads you through the basic required steps to configure NAT for the SRX Series security device. To configure more detailed settings, use either the J-Web interface or the command-line interface (CLI).

As you use this wizard, refer to the upper left area of the page to see where you are in the configuration process. Refer to the lower left area of the page for help related to the current page and its contents.

When you click a link under the Resources heading in the lower left area, the document opens in your browser. If it is in a new tab, be sure to close only the tab (not the browser window) when you close the document.

Interfaces

- [Viewing Interfaces Configuration Page Options on page 203](#)
- [Interconnecting Interface Ports Configuration Page Options on page 207](#)
- [VLAN Configuration Page Options on page 210](#)
- [Link Aggregation Configuration Page Options on page 213](#)

Viewing Interfaces Configuration Page Options

1. Select **Configure>Interfaces>Ports** in the J-Web user interface.

The Interfaces configuration page appears. [Table 121 on page 204](#) explains the contents of this page.

2. Click one:
 - **Add** or **+**—Add a new or duplicate interface configuration. See [Table 122 on page 204](#).
 - **Edit** or **/**—Edit the selected interface configuration.
 - **Delete** or **X**—Delete the selected interface configuration.
3. Click one:
 - **OK**—Saves the configuration and returns to the main configuration page.
 - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.

- **Cancel**—Cancels your entries and returns to the main configuration page.
4. Click **Switch to L2 mode** to switch between L2 and L3 mode and vice versa. [Table 123 on page 206](#) explains the contents of this page.



NOTE: This feature is not supported on SRX1500 devices.

This feature is not supported in Junos OS Release 15.1 and later.

Table 121: Interfaces Configuration Page

Field	Function
Interface	Displays the interface name. Logical interfaces configured under this interface appear in a collapsible list under the physical interface.
Admin status	Displays the administrative status of the interface. Status can be either Up or Down.
Link Status	Displays the operational status of the link. Status can be either Up or Down.
IP Address	Displays the configured IP addresses. Multiple IP addresses configured on one logical interface are displayed in a collapsible list under the logical interface.
Zone	Displays the security zone with which this interface is associated.
MTU	Displays the maximum transmission unit value for this physical interface.
Speed	Displays the Interface speed (10 Mbps, 100 Mbps, 1 Gbps, or Auto).
Link Mode	Displays the link mode status for this interface. Status can be Active, Passive, or None.
Auto Negotiation	Displays the auto negotiation status of the interface. Status can be either Enabled or Disabled.

Table 122: Viewing Interfaces Configuration Details

Field	Function	Action
Filter		
Interface Type	Displays the list of interfaces available on the device. NOTE: By default, only interfaces ge and fe are displayed. Others are hidden.	Select an option.

Table 122: Viewing Interfaces Configuration Details (continued)

Field	Function	Action
Interface State	Displays the state options. The options available are: <ul style="list-style-type: none"> • Admin Up • Link Up • Admin Up and Link Down • Admin Down 	Select an option.
Zone Association	Displays the list of security zones available.	Select an option.
Go	Displays the list of interfaces based on the interface type, interface state, or zone association that you have used to filter the interface information.	
Clear	Clears the filter options that you have selected and displays all the interfaces.	
Expand All	Expands the tree under the interfaces.	
Global Settings	Opens a window, where you can configure all the interfaces on the device with respect to MAC table size, MAC limit, and packet action.	<p>MAC Table size—Specify the size of MAC address forwarding table.</p> <p>MAC Limit—Specify the maximum number of MAC addresses learned per interface. The range is between 1 and 65,535.</p> <p>Packet Action—Specify the action when MAC limit is reached. The options available are: drop, drop-and-log, log, none, and shutdown.</p>
Add	Adds a new or duplicate logical interface configuration.	Select any of the listed Interface and select Add>Logical Interface .
Edit	Edits the selected interface configuration.	Select any of the listed Interface and select Edit .
Disable	Disables the selected interface.	
Delete	Deletes the selected interface.	

To edit an interface:

1. Select the Interface that you want to edit from the listed rows, and click **Edit**.

The Edit interface *<interface name>* page appears.

2. Enter the description for the interface in the Description field.

3. Enter the MTU in bytes.
4. Select the speed from the listed options: 10 Mbps, 100 Mbps, 1 Gbps, 10 Gbps, or None.



NOTE: Starting Junos OS 18.1R1, in an SRX4600 device if you have inserted an SFP module, then you can configure the speed of XE (1 Gbps or 10 Gbps) ports in the SFP module.

5. Select the Link Mode from the listed options: Half Duplex, Full Duplex, and None.
6. Select Loopback, if you want the interface to loop back.
7. Select or deselect Flow Control, Enable Auto Negotiation, Enable Per Unit Scheduler, and Enable VLAN Tagging based on your preference.
8. Click **Add** if you want to assign a MAC Address to the interface.
9. Enter the MAC limit. The range is from 1 through 65535.
10. Select the action to be taken on the packet from the options: **drop**, **drop-and-log**, **log**, **none**, and **shutdown**.
11. Click **OK** to save the interface settings.

Table 123: L2/L3 Switching Mode

Field	Function	Action
Switch to L2 mode		
Management IP	<p>Specifies the management IP address.</p> <p>CAUTION: When you click Switch to L2 mode, the following confirm message appears: "Transitioning to L2 Transparent mode might fail due to some security configurations like (NAT, IPSEC, VPN). Are you sure you want to proceed?"</p> <p>NOTE: This confirm message appears only when the security configurations like (NAT, IPSEC, VPN) were available in L3 mode.</p>	<p>Enter a valid IP address for the management interface.</p> <p>CAUTION: When you enter the management IP address and click OK, the following confirm message appears: "During this action, the device will be rebooted and J-Web connectivity will be lost. Are you sure you want to continue?"</p>
Switch to L3 mode		
Management IP	Specifies the management IP address.	Enter a valid IP address for the management interface.

Table 123: L2/L3 Switching Mode (continued)

Field	Function	Action
Management Interface	Displays the list of interfaces available on the device.	Select an option. CAUTION: When you select the interface and click OK , the following confirm message appears: "During this action, the device will be rebooted and J-Web connectivity will be lost. Are you sure you want to continue?"

- See Also**
- [Link Aggregation Configuration Page Options on page 213](#)
 - [Fast Ethernet Interfaces Configuration Page Options](#)
 - [Gigabit Ethernet Interfaces Configuration Page Options](#)
 - [Logical Ethernet Interfaces Configuration Page Options](#)

Interconnecting Interface Ports Configuration Page Options

On SRX Series Services Gateways, the logical tunnel interface is used to interconnect logical systems. Use this page to interconnect logical system that serves as an internal virtual private LAN service (VPLS) switch connecting one logical system on the device to another.

1. Select **Configure>Interfaces>Interconnect Ports** in the J-Web user interface.

The Interfaces configuration page appears. [Table 124 on page 208](#) explains the contents of this page.

2. Click one:
 - **Add** or **+**—Add a new or duplicate interface configuration. See, [Table 125 on page 208](#).
 - **Edit** or **/**—Edit the selected interface configuration.
 - **Delete** or **X**—Delete the selected interface configuration.
3. Click Commit icon at the top of the J-Web page. The following commit options are displayed.
 - **Commit**—Commits the configuration and returns to the main configuration page.
 - **Compare**—Enables you to compare the current configuration with the previous configuration.
 - **Discard**—Discards the configuration changes you performed in the J-Web.
 - **Preferences**—There are two tab:
 - **Commit preferences**—You can choose to just validate or validate and commit the changes.
 - **Confirm commit timeout (in min)** —You can select the commit timeout interval.

Table 124: Interconnect Ports Configuration Page

Field	Function
Interface	Displays the interface name. Logical interfaces configured under this interface appear in a collapsible list under the physical interface.
Link Status	Displays the operational status of the link. Status can be either Up or Down.
IP Addresses	Displays the configured IP addresses. Multiple IP addresses configured on one logical interface are displayed in a collapsible list under the logical interface.
Encapsulation	<p>Displays the mode of encapsulation. Encapsulation is the process of taking data from one protocol and translating it into another protocol, so the data can continue across a network. It can from the following points:</p> <ul style="list-style-type: none"> • Ethernet • Frame Relay • Ethernet VPLS <p>Ethernet and Frame Relay are used if logical tunnel interfaces connected between two logical systems. Ethernet VPLS will be used on logical tunnel interface which is connecting VPLS switch to logical system.</p>
LSYS/Tenant/VPLS Switch	Displays the name of the logical system or the name of VPLS Switch.
Peer Interface	Displays the peer details.
Type	Displays the type for logical interface—Logical System, Tenant, or VPLS Switch.
Peer Encapsulation	Displays the peer encapsulation mode.
Peer LSYS/VPLS Switch	Displays the name of the peer logical system and VPLS Switch.

Table 125: Creating and Editing LT Logical Interface - Configuration Details

Field	Function	Action
Local Details		
Unit	Specify the unit for logical interface.	Enter the Logical unit number
Type	Specify the type for logical interface.	Select a type from the drop down list. The options available are Logical System, Tenant, and VPLS Switch.
Logical System	Specify the logical system created.	<p>Select a logical system from the list. If not present in the list, then we need to create a logical system.</p> <p>NOTE: Starting from Junos OS 19.1R1, the user interface will autocomplete the logical system names when you type the partial name.</p>

Table 125: Creating and Editing LT Logical Interface - Configuration Details (continued)

Field	Function	Action
Tenant	Specify the tenant created.	Select a tenant from the list. NOTE: Starting from Junos OS 19.1R1, the user interface will autocomplete the tenant names when you type the partial name.
VPLS Switch	Specify the VPLS switch created.	Select a VPLS switch from the list.
Description	Specify the interface description.	Enter description for the interface.
IPv4 Address	Specify the IPv4 address.	Click + and enter the following: <ul style="list-style-type: none"> • IPv4 address—IP Addresses added here would be used as interconnect IP. • Prefix Length—Enter the prefix length. This specifies the number of bits set in the subnet mask.
IPv6 Address	Specify the IPv6 address.	Click + and enter the following: <ul style="list-style-type: none"> • IPv6 address—IP Addresses added here would be used as interconnect IP. • Prefix Length—Enter the prefix length. This specifies the number of bits set in the subnet mask.
Peer Details		
Type	Specify the type of connection.	Select any one of the connection type from the following: <ul style="list-style-type: none"> • Logical system • Tenant • VPLS Switch
Logical System	Displays the name of the logical system.	Select a logical system from the list. If not present in the list, then we need to create a logical system.
Tenant	Specify the tenant created.	Select a tenant from the list.
Unit	Specify the peering logical system unit number.	Enter the logical system unit number
Description	Specify the interface description.	Enter description for the interface.

Table 125: Creating and Editing LT Logical Interface - Configuration Details (continued)

Field	Function	Action
IPv4 Address	Specify the IPv4 address.	Click + and enter the following: <ul style="list-style-type: none"> • IPv4 address—IP Addresses added here would be used as interconnect IP. • Prefix Length—Enter the prefix length. This specifies the number of bits set in the subnet mask.
IPv6 Address	Specify the IPv6 address.	Click + and enter the following: <ul style="list-style-type: none"> • IPv6 address—IP Addresses added here would be used as interconnect IP. • Prefix Length—Enter the prefix length. This specifies the number of bits set in the subnet mask.

VLAN Configuration Page Options

1. Select **Configure>Switching>VLAN** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Configure>Interfaces>VLAN** in the J-Web user interface.

The VLAN configuration page appears. [Table 126 on page 211](#) explains the contents of this page.



NOTE: Starting in Junos OS Release 19.2R1, now bridge domain is the new name for the VLANs in the Layer 2 transparent mode. You can now assign an interface for the created VLANs. You can view all the available VLANs with its ID, interfaces assigned, and the status.

2. Click one:
 - **Add** or **+**—Adds a new or duplicate VLAN configuration. Enter information as specified in [Table 127 on page 211](#).
 - **Edit** or **/**—Edits a selected VLAN configuration.
 - **Delete** or **X**—Deletes the selected VLAN configuration.
3. Click one:
 - **OK**—Saves the configuration and returns to the main configuration page.
 - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
 - **Cancel**—Cancels your entries and returns to the main configuration page.

Table 126: VLAN Configuration Page

Field	Function
General	
VLAN Name	Displays the name for the VLAN.
VLAN ID/List	Displays the identifier or list for the VLAN.
Interface Assigned	Displays the interfaces assigned for the VLAN.
Description	Displays a brief description for the VLAN.

Table 127: Add VLAN Configuration Details

Field	Function	Action
VLAN Details		
VLAN Name	Specifies a unique name for the VLAN.	Enter a name. NOTE: The VLAN text field is disabled when vlan-tagging is not enabled.
VLAN ID Type	Specifies the type of VLAN ID. The available options are: <ul style="list-style-type: none"> • Single • Range 	Select an option.
VLAN ID	Specifies the identifier for the VLAN.	Type an unique identification number from 1 through 4094. If no value is specified, the default is 1.
Description	Provides a description of the VLAN.	Enter a brief description for the VLAN.
Advanced Settings (optional)		
L2 Interfaces	Specifies the interfaces to be associated with the VLAN.	The available options are as follows: <ul style="list-style-type: none"> • Add—Click + to add the MAC address and L2 interface details. • Edit—Click the pencil icon to edit the selected interface. • Remove—Select the interface or interfaces that you do not want associated with the VLAN.
Filter		
Input Filter	Specifies the VLAN interface firewall filter that is applied to incoming packets.	To apply an input firewall filter to an interface, select the firewall filter from the list.
Output Filter	Specifies the VLAN interface firewall filter that is applied to outgoing packets.	To apply an output firewall filter to an interface, select the firewall filter from the list.

Table 127: Add VLAN Configuration Details (continued)

Field	Function	Action
IPv4 Address		
IPv4 Address	Specifies the IPv4 address of the VLAN.	Enter the IP address.
Subnet Mask	Specifies the range of logical addresses within the address space that is assigned to an organization.	Enter the address, for example, 255.255.255.0. You can also specify the address prefix.
IP Address	Specifies the IP address of the VLAN.	<p>The available options are as follows:</p> <ul style="list-style-type: none"> • Add—Click + to add the IP address, MAC address, and L2 interface details. • Edit—Click the pencil icon to edit the selected IPv4 address. • Remove—Select the IPv4 address or addresses that you do not want associated with the VLAN.
IPv6 Address		
NOTE: This option is available only for SRX5000 line of devices.		
IPv6 Address	Specifies the IPv6 address of the VLAN.	Enter the IP address.
Prefix	Specifies the destination prefix of the VLAN.	Select the address prefix.

Table 128: Assign Interface

Field	Function	Action
VLAN Name	Displays the name of the VLAN for which you want to assign the interface.	-
VLAN ID	Displays the ID of the selected VLAN.	-
Description	Displays the description of the selected VLAN.	-
Interfaces	Displays the available interfaces.	Select the interfaces in the Available column and use the right arrow to move them to the Selected column.
VoIP Interfaces	Displays the available VoIP interfaces.	Select the VoIP interfaces in the Available column and use the right arrow to move them to the Selected column.

- See Also**
- *Spanning Tree Configuration Page Options*
 - *IGMP Snooping Configuration Page Options*
 - *GVRP Configuration Page Options*

Link Aggregation Configuration Page Options

1. Select **Configure > Interfaces > Link Aggregation** in the J-Web user interface.

The Link Aggregation configuration page appears. [Table 129 on page 213](#) explains the contents of this page.



NOTE: Link Aggregation menu to configure aggregated Ethernet (ae) interfaces is not available when the device is in cluster (HA) mode. To configure redundant Ethernet (reth) interfaces in the HA mode, navigate to **Configure > Device Settings > Cluster Configuration**.

2. Click one:

- **Global Setting**—Creates an Link Aggregated Ethernet interface, or LAG. You can choose the number of device that you want to create. Enter information as specified in [Table 130 on page 214](#).
- **Add Logical Interface**—Adds logical interfaces to the configured port. See [Table 131 on page 214](#).



NOTE: Logical Interface is supported only for Layer 3 inet or inet6 family.

- **Enable/Disable**—Enables or disables the configured aggregated interface. A message appears to confirm if you want to enable or disable the aggregated interface.
 - **Add or +**—Adds a new link aggregation configuration. Enter information as specified in [Table 132 on page 215](#).
 - **Edit or /**—Edits a selected link aggregation configuration.
 - **Delete or X**—Deletes a selected link aggregation configuration.
3. Click one:
 - **OK**—Saves the configuration and returns to the main configuration page.
 - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
 - **Cancel**—Cancels your entries and returns to the main configuration page.

Table 129: Link Aggregation Configuration Page

Field	Function
Name	Displays the name of the select LAG.
Link Status	Displays whether the interface is linked (Up) or not linked (Down).
Admin Status	Displays whether the interface is up or down.

Table 129: Link Aggregation Configuration Page (continued)

Field	Function
Interfaces	Displays the name of the aggregated interface.
VLAN ID	Displays the Virtual LAN identifier value for IEEE 802.1Q VLAN tags (0.4094).
IP Address	Displays the IP address associated with the interface.
VLAN Tagging	Displays whether the interface is VLAN-tagged (enabled) or untagged (disabled).
Enabled/Disabled	Displays whether the LACP link-protection is enabled or disabled.
Description	Provides a description of the LAG.

Table 130: Global Setting Link Aggregation Configuration Page

Field	Function	Action
Global Settings		
Device Count	Specifies the device count.	Enter the device count by clicking the arrow button.
Advanced Settings		
NOTE: This option is not available for SRX5000 line of devices.		
LACP Configuration	Specifies global Link Aggregation Control Protocol configuration.	-
System Priority	Specifies the priority level that you associate with the LAG.	Select the priority level that you want to associate with the LAG by clicking the arrow button.
Link Protection	Specifies the option to protect the link. NOTE: You can configure only two member links for an aggregated Ethernet interface, that is, one active and one standby.	Select the option.
Non-Revertive	Specifies not to choose even if a higher priority link is available.	Enable or disable the option.

Table 131: Add Logical Interface

Field	Function	Action
Aggregated Interface Name	Displays the name of the aggregated Interface.	Select an aggregated interface name from the grid.

Table 131: Add Logical Interface (continued)

Field	Function	Action
Logical Interface Unit	Displays the logical interface unit.	Enter the logical interface unit.
Description	Displays the description.	Enter the description.
VLAN ID	Displays the VLAN ID.	Enter the VLAN ID. VLAN ID is mandatory.
IPv4 Address		
IPv4 Address	Displays the IPv4 address.	Click + and enter a valid IP address.
Subnet Mask	Displays the subnet mask for IPv4 address.	Enter a valid subnet mask.
IPv6 Address		
IPv6 Address	Displays the IPv6 address.	Enter a valid IP address.
Subnet Mask	Displays the subnet mask for IPv6 address.	Enter a valid subnet mask.

Table 132: Add Link Aggregation Configuration Details

Field	Function	Action
General Settings		
AE Name	Specifies the name of the aggregated interface. If an aggregated interface already exists, then the field is displayed as read-only.	Enter the aggregated interface name.
Interfaces	Displays the interfaces available for aggregation. NOTE: Only interfaces that are configured with the same speed can be selected together for a LAG.	Select the interface and move to Selected column using right arrow.
Advanced Settings		
LACP Configuration	Specifies global Link Aggregation Control Protocol configuration.	-
LACP Mode	Specifies the mode in which Link Aggregation Control Protocol packets are exchanged between the interfaces. The modes are: <ul style="list-style-type: none"> • Active—Indicates that the interface initiates transmission of LACP packets • Passive—Indicates that the interface only responds to LACP packets. 	Select an option.

Table 132: Add Link Aggregation Configuration Details (continued)

Field	Function	Action
General Settings		
Periodic	Specifies periodic transmissions of link aggregation control PDUs occur at different transmission rate. The options available are: <ul style="list-style-type: none"> fast—Transmit link aggregation control PDUs every second. slow—Transmit link aggregation control PDUs every 30 seconds. 	Select an option.
System Priority	Specifies the priority level that you associate with the LAG.	Select the priority level that you want to associate with the LAG by clicking the arrow button.
Link Protection	Specifies the option to protect the link. <i>NOTE:</i> You can configure only two member links for an aggregated Ethernet interface, that is, one active and one standby.	Enable or disable the option.
Non-Revertive	Specifies not to choose even if a higher priority link is available.	Enable or disable the option.
Description	Provides a description of the LAG.	Enter a description for the LAG.
VLAN Tagging	Specifies whether or not to enable VLAN tagging for a LAG.	Select to enable VLAN tagging.

- See Also**
- [Viewing Interfaces Configuration Page Options on page 203](#)
 - [Firewall Authentication Configuration Page Options on page 226](#)

Users

- [User Management Configuration Page Options on page 216](#)
- [Access Profiles Configuration Page Options on page 221](#)
- [Firewall Authentication Configuration Page Options on page 226](#)
- [UAC Settings Configuration Page Options on page 228](#)

User Management Configuration Page Options

1. Select **Configure>System Properties>User Management** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platform.

Or

Select **Configure>Device Setup>Basic Settings>User Management** in the J-Web user interface.

The User Management configuration page appears.

2. (Junos OS Release 19.1R1 and later releases) Select **Configure>Users>User Management** in the J-Web user interface.

The User Management configuration page appears. [Table 133 on page 217](#) explains the contents of this page.

3. Click one:
 - **Save**—Saves all the user management configuration and returns to the main configuration page.
 - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
 - **Cancel**—Cancels all your entries and returns to the main configuration page.

Table 133: User Management Configuration Details

Field	Function	Action
User Details		

Table 133: User Management Configuration Details (continued)

Field	Function	Action
User Details	<p>Provides the users details to the device's local database. The options available are:</p> <ul style="list-style-type: none"> • Add • Edit • Delete • Search • Filter 	<p>Select an option:</p> <p>To add a new user, click Add. Then enter the details specified below and click OK.</p> <ul style="list-style-type: none"> • User name—Enter a unique name for the user. Do not include spaces, colons, or commas in the username. • Login ID—Enter a unique ID for the user. • Full Name—Enter the user's full name. If the full name contains spaces, enclose it in quotation marks. Do not include colons or commas. • Password—Enter a login password for the user. The login password must meet the following criteria: <ul style="list-style-type: none"> • The password must be at least 6 characters long. • You can include most character classes in a password (alphabetic, numeric, and special characters), except control characters. • The password must contain at least one change of case or character class. • Confirm password—Re-enter the login password for the user. • Role—Select the user's access privilege from the following options: <ul style="list-style-type: none"> • super-user • operator • read-only • unauthorized • To edit the information of a user, select it and click Edit. Then edit the user details in the Edit User dialog box and click OK. • To delete an existing user, select it and click Delete.

Authentication Methods

Table 133: User Management Configuration Details (continued)

Field	Function	Action
Authentication Method And Order	<p>Specifies the authentication method the device should use to authenticate users. The options available are:</p> <ul style="list-style-type: none"> • Password • RADIUS Servers • TACACS+ Servers 	Enable authentication methods and drag and drop to change the authentication order.
RADIUS Servers		
RADIUS Servers	Specifies the details of RADIUS servers.	<p>Click Configure.</p> <p>To add a new RADIUS server, click +. Then enter the details specified below and click OK.</p> <ul style="list-style-type: none"> • IP Address—Enter the server's 32-bit IP address. • Password—Enter the secret password for the server. • Confirm Password—Re-enter the secret password for the server. • Server Port—Enter an appropriate port. • Source Address—Enter the source IP address of the server. • Time out—Specify the amount of time (in seconds) the device should wait for a response from the server. • Retry Attempts—Specify the number of times that the server should try to verify the user's credentials. • To delete an existing RADIUS server, select it and click Delete.
TACACS		

Table 133: User Management Configuration Details (continued)

Field	Function	Action
TACACS Servers	Specifies the details of TACACS servers.	<p>Click Configure.</p> <p>To add a new TACACS server, click +. Then enter the details specified below and click OK.</p> <ul style="list-style-type: none"> • IP Address—Enter the server's 32-bit IP address. • Password—Enter the secret password for the server. • Confirm Password—Re-enter the secret password for the server. • Server Port—Enter an appropriate port. • Source Address—Enter the source IP address of the server. • Time out—Specify the amount of time (in seconds) the device should wait for a response from the server. • To delete an existing TACACS server, select it and click Delete.

Password Settings

NOTE:

- Starting in Junos OS Release 19.1R1, the User Management configuration supports the password settings range.
- J-Web interface does not support configuring the number of characters by which the new password should be different from the existing password.

Minimum Reuse	Specifies the minimum number of old passwords which should not be same as the new password.	<p>Starting in Junos OS Release 19.1R1, this Minimum Reuse option is supported.</p> <p>Click top or bottom arrow to specify the minimum number of old passwords that you want to use. Range: 1-20.</p>
Maximum Lifetime	Specifies the maximum password lifetime.	<p>Starting in Junos OS Release 19.1R1, this Maximum Lifetime option is supported.</p> <p>Click top or bottom arrow to specify the maximum lifetime of your password in days. Range: 30-365.</p>
Minimum Lifetime	Specifies the minimum password lifetime.	<p>Starting in Junos OS Release 19.1R1, this Minimum Lifetime option is supported.</p> <p>Click top or bottom arrow to specify the minimum lifetime of your password in days. Range: 1-30.</p>

- See Also**
- [System Identity Configuration Page Options on page 175](#)
 - [Management Access Configuration Page Options on page 179](#)
 - [Date and Time Configuration Page Options on page 177](#)

Access Profiles Configuration Page Options

1. Select **Configure>Access>Access Profiles** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Configure>Authentication>Access Profiles** in the J-Web user interface.

The Access Profiles configuration page appears.

2. (Junos OS Release 19.1R1 and later releases) Select **Configure>Users>Access Profile** in the J-Web user interface.

The Access Profiles configuration page appears.

3. Click one:

- **Add** or **+**—Adds a new or duplicate access profile configuration. Enter information as specified in [Table 134 on page 221](#).
- **Edit** or **/**—Edits a selected access profile configuration.
- **Delete** or **X**—Deletes the selected access profile configuration.
- **Search Icon**—Enables you to search a firewall policy or rule from the grid.

Table 134: Add Access Profile Configuration Details

Field	Function	Action
General Settings		
Access Profile Name	Specifies the name of the access profile.	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. Maximum length is 64 characters.
Authentication Order		

Table 134: Add Access Profile Configuration Details (continued)

Field	Function	Action
General Settings		
Order 1	Configures the order in which the user tries different authentication methods during login. For each login attempt, the method for authentication starts with the first one, until the password matches.	

Table 134: Add Access Profile Configuration Details (continued)

Field	Function	Action
General Settings		<p>Select one or more of the following authentication method:</p> <ul style="list-style-type: none"> NONE—No authentication for the specified user. LDAP—Use LDAP. The SRX Series device uses this protocol to get user and group information necessary to implement the integrated user firewall feature. Password—Use a locally configured password in the access profile. You can set the password to none or configure for the following authentication orders: <ul style="list-style-type: none"> LDAP Radius servers Secure ID Radius—Use RADIUS authentication services. If RADIUS servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order. Secure ID—Configure the RSA SecurID authentication. Users can enter either static or dynamic passwords as their credentials. A dynamic password is a combination of a user's PIN and a randomly generated token that is valid for a short period of time, approximately one minute. A static password is configured for the user on the SecurID server. For example, the SecurID

Table 134: Add Access Profile Configuration Details (continued)

Field	Function	Action
General Settings		
		server administrator might set a temporary static password for a user who has lost SecurID token.
Order 2	Configures the next authentication method if the authentication method included in the authentication order option is not available, or if the authentication is available but returns a reject response.	Select the authentication method from the list and click Next .
Password		
Address Assignment	Specifies the address pool used by the access profile.	<p>Select an address pool from the list.</p> <p>Click + to create the password using the address pool and enter the following details:</p> <ul style="list-style-type: none"> • User Name—Enter the user name. • Password—Enter the password. • XAUTH IP Address—Enter the IPv4 address of the external authentication server to verify the authentication user account. • Groups—Enter the group name to store several user accounts together on the external authentication servers.
LDAP		

Table 134: Add Access Profile Configuration Details (continued)

Field	Function	Action
General Settings		
LDAP	Configures the LDAP server for authentication.	<p>Click + to add LDAP server, enter the following details, and click OK:</p> <ul style="list-style-type: none"> • Address—Enter the IPv4 address or hostname of the LDAP authentication server. • Port—Configure the port number on which to contact the LDAP server. Range is 1-65535. • Retry—Specify the number of retries that a device can attempt to contact an LDAP server. Range is 1-10 seconds. • Routing Instance—Configure the routing instance used to send LDAP packets to the LDAP server. • Source Address—Configure a source IP address for each configured LDAP server. • Timeout—Configure the amount of time that the local device waits to receive a response from an LDAP server. Range is 3-90.
LDAP Options		
Base Distinguished Name	Specifies the base distinguished name that defines the user.	Enter the base distinguished name.
Revert Interval	Specifies the amount of time that elapses before the primary server is contacted if a backup server is being used.	<p>Use top/bottom arrows to provide the revert interval.</p> <p>Range is 60-4294967295.</p>
Additional Details		
Assemble	Specifies that a user's LDAP distinguished name (DN) is assembled through the use of a common name identifier, the username, and base distinguished name.	Enable the assemble option.

Table 134: Add Access Profile Configuration Details (continued)

Field	Function	Action
General Settings		
Common Name	Specifies the common name identifier used as a prefix for the username during the assembly of the users distinguished name.	Enter a common name identifier.
Search	Specifies that a user's LDAP distinguished name is assembled through the use of a common name identifier, a username, and a base distinguished name.	Enable the search option.

See Also • [Firewall Authentication Configuration Page Options on page 226](#)

Firewall Authentication Configuration Page Options

1. Select **Configure>Access>FW Authentication** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Configure>Authentication>FW Authentication** in the J-Web user interface.

The Firewall Authentication configuration page appears. [Table 135 on page 226](#) explains the contents of this page.

2. (Junos OS Release 19.1R1 and later releases) Select **Configure>Users>FW Authentication** in the J-Web user interface.

The Firewall Authentication configuration page appears. [Table 135 on page 226](#) explains the contents of this page.

3. Click one:

- **OK/Save**—Saves the configuration and returns to the main configuration page.
- **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
- **Reset**—Resets your entries and returns to the main configuration page.
- **Cancel**—Cancels your entries and returns to the main configuration page.

Table 135: Add Firewall Authentication Configuration Details

Field	Function	Action
Pass-through Settings		

Table 135: Add Firewall Authentication Configuration Details (continued)

Field	Function	Action
Default Profile	Specifies the profile that the policies use to authenticate users. The options available are: <ul style="list-style-type: none"> • None • stu-access-profile • juniper-access-profile 	Select an option.
HTTP Banner		
Login	Displays the login prompt for users logging in using HTTP.	–
Failed	Displays failed login prompt for users logging in using HTTP.	–
Success	Displays a successful login prompt for users logging in using HTTP.	–
FTP Banners		
Login	Displays the login prompt for users logging in using FTP.	–
Failed	Displays failed login prompt for users logging in using FTP.	–
Success	Displays a successful login prompt for users logging in using FTP.	–
Telnet Banners		
Login	Displays the login prompt for users logging in using telnet.	–
Failed	Displays failed login prompt for users logging in using telnet.	–
Success	Displays a successful login prompt for users logging in using telnet.	–
Web-auth-settings		
Default Profile	Specifies the profile that the policies use to authenticate users. The options available are: <ul style="list-style-type: none"> • None • stu-access-profile • juniper-access-profile 	Select an option.
Banner Success	Displays a successful login prompt for users logging in using Web authentication banner.	–

Table 135: Add Firewall Authentication Configuration Details (continued)

Web-auth logo upload		
Logo image	Indicates an image to be chosen for the Web authentication logo. NOTE: For the good logo image, the image format must be in .gif and the resolution must be 172x65.	—
Browse	Navigates to the available logo image on the user's local disk.	Navigate to the logo image.
Upload File	Uploads the image.	Click the button to upload the image.
Restore Juniper logo	Restores the default Juniper Networks logo.	Click the button to restore the Juniper Networks logo.

- See Also**
- [Link Aggregation Configuration Page Options on page 213](#)
 - [Source NAT Configuration Page Options on page 301](#)

UAC Settings Configuration Page Options

1. Select **Configure>Authentication>UAC Settings** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Configure>Authentication>UAC Settings** in the J-Web user interface.

The UAC Settings configuration page appears.
2. (Junos OS Release 19.1R1 and later releases) Select **Configure>Users>UAC Settings** in the J-Web user interface.

The UAC Settings configuration page appears. [Table 136 on page 229](#) explains the contents of this page.
3. Click one:
 - **Add or +**—Adds a new Infranet Controller. Enter information as specified in [Table 136 on page 229](#).
 - **Edit or /**—Edits the selected Infranet Controller configuration.
 - **Delete or X**—Deletes the selected Infranet Controller configuration.
4. Click one:
 - **OK/Save**—Saves the configuration and returns to the main configuration page.
 - **Actions>Commit**—Commits the configuration and returns to the main configuration page.

- **Cancel**—Cancels your entries and returns to the main configuration page.

Table 136: Infranet Controller Configuration Details

Field	Function	Action
Global Settings		
Certificate Verification	Determines whether server certificate verification is required when initiating a connection between a device and an Access Control Service in a UAC configuration.	<p>Select the following options from the list:</p> <ul style="list-style-type: none"> • None—Certificate verification is not required. • Optional—Certificate verification is not required. If the CA certificate is not specified in the ca-profile option, the commit check passes and no warning is issued. • Required—Certificate verification is required. If the CA certificate is not specified in the ca-profile option, an error message is displayed, and the commit check fails. Use this option to ensure strict security. • Warning—Certificate verification is not required. A warning message is displayed during commit check if the CA certificate is not specified in the ca-profile option.
Interval	Specifies the value in seconds that the device should expect to receive a heartbeat signal from the IC Series device.	Enter the heartbeat interval in seconds. Range: 1 through 9999.
Test Only Mode	Allows all traffic and log enforcement result.	Enable the Test Only Mode option.
Timeout	Specifies (in seconds) that the device should wait to get a heartbeat response from an IC Series UAC Appliance.	Enter the timeout in seconds. Range: 2 through 10000.
Timeout Action	Specifies the action to be performed when a timeout occurs and the device cannot connect to an Infranet Enforcer.	Select the timeout action.
Infranet Controller		
Name	Specifies the name of the Infranet Controller.	Enter a name for the Infranet Controller.
IP address	Specifies an IP address for the Infranet Controller.	Enter an IP address for the Infranet Controller.
Interface	Specifies the interface used for the Infranet Controller.	Select an interface.
Password	Specifies the password to use for the Infranet Controller.	Enter the password.

Table 136: Infranet Controller Configuration Details (continued)

Field	Function	Action
CA Profiles	Specifies the preferred CA to use for the Infranet Controller. If no value is specified, then no certificate request is sent (although incoming certificates are still accepted).	Select a CA from the list in the CA Profiles column and then click the right arrow to move them to the Selected column. NOTE: To deselect a CA, select the CA in the Selected column and then click the left arrow to move them to the CA Profiles column.
Port	Specifies the port number to be associated with this Infranet Controller for data traffic.	Enter a value from 1 through 65,535.
Server Certificate Subject	Specifies the subject name of the Infranet Controller certificate to match.	Enter the server certificate subject name.
Captive Portal		
Captive Portal	Specifies the preconfigured security policy for captive portal on the Junos OS Enforcer.	Click + to add a captive portal.
Name	Specifies the name of the captive portal.	Enter a name for the captive portal.
Redirect Traffic	Specifies a traffic type to be redirected.	Select a traffic type.
Redirect URL	Specifies a URL to which the traffic should be redirected.	Enter the URL to which the captive portal should be directed.

See Also • [Firewall Authentication Configuration Page Options on page 226](#)

Network

- [DHCP on page 230](#)
- [Routing Instances Configuration Page Options on page 238](#)
- [Static Routing Configuration Page Options on page 239](#)
- [RIP Configuration Page Options on page 241](#)
- [OSPF Configuration Page Options on page 246](#)
- [BGP Configuration Page Options on page 252](#)
- [Policies Configuration Page Options on page 258](#)
- [Class of Service on page 264](#)
- [Forwarding Mode on page 280](#)

DHCP

- [DHCP Client Configuration Page Options on page 231](#)
- [DHCP Services Configuration Page Options on page 232](#)

DHCP Client Configuration Page Options

1. Select **Configuration>DHCP>DHCP client** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Configure>Network>DHCP>DHCP client** in the J-Web user interface.

The DHCP client configuration page appears.

2. Click one:
 - **Add**—Adds a new DHCP client configuration. Enter information as specified in [Table 137 on page 231](#).
3. Click one:
 - **OK**—Saves the configuration and returns to the main configuration page.
 - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
 - **Cancel**—Cancels your entries and returns to the main configuration page.

Table 137: Add DHCP Client Configuration Details

Field	Function	Action
DHCP Client Information		
Interface	Specifies the interface on which to configure the DHCP client.	Enter the name of the interface.
Client Identifier	Specifies the name of the client used by the DHCP server to index its database of address bindings. The options available are: <ul style="list-style-type: none"> • ASCII—ASCII client. • Hexadecimal—Hexadecimal client. 	Select an option.
Lease Time	Specifies the time in seconds, to negotiate and exchange DHCP messages.	Enter a value from 60 through 2,147,483,647.
Retransmission Attempt	Specifies the number of attempts the router is allowed to retransmit a DHCP packet fallback.	Enter a value from 0 through 6. The default value is 4.
DHCP Server Address	Specifies the preferred DHCP server that the DHCP clients contact with DHCP queries.	Enter the IPv4 address of the DHCP server.
Vendor Class ID	Specifies the vendor class identity number for the DHCP client.	Enter the vendor class ID numbers.

Table 137: Add DHCP Client Configuration Details (continued)

Field	Function	Action
Update Server	Specifies whether the propagation of TCP/IP settings is enabled on the specified interface (if it is acting as a DHCP client) to the DHCP server that is configured on the router.	Select the check box.

- See Also**
- [DHCP Services Configuration Page Options on page 232](#)
 - [Boot DHCP Relay Configuration Page Options](#)

DHCP Services Configuration Page Options

1. Select **Configure>DHCP>DHCP Services** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Configure>Network>DHCP>DHCP Server** in the J-Web user interface.

The DHCP services configuration page appears. Enter information as specified in [Table 138 on page 232](#) to configure DHCP services.

2. Click:
 - **Apply**—Applies the configuration and returns to the main configuration page.

Table 138: Add DHCP Services Configuration Details

Field	Function	Action
Global Settings		
Server Information		
Server Identifier	Specifies the IP address of the DHCP server.	Enter the IP address of the Services Router. If you do not specify a server identifier, the primary address of the interface on which the DHCP exchange occurs is used.
Domain Name	Specifies the domain name that the clients must use to resolve hostnames.	Enter the domain name.
Next Server	Specifies the IP address of the next DHCP server that the clients need to contact.	Enter the IP address of the next DHCP server.
Propagate Interface	Specifies the name of the interface on the router through which the resolved DHCP queries are propagated to the DHCP pool.	Enter the name of the interface.

Table 138: Add DHCP Services Configuration Details (continued)

Field	Function	Action
Domain Search	Specifies the order, from top to bottom, in which clients must append domain names when resolving hostnames using DNS. The options available are: <ul style="list-style-type: none"> • Add—Adds a domain name. • Delete—Deletes a domain name. 	Select an option.
Name Servers	Specifies a list of DNS servers that the client can use, in order of preference from top to bottom. The options available are: <ul style="list-style-type: none"> • Add—Adds a DNS server. • Delete—Deletes a DNS server. 	Click an option.
Gateway Routers	Specifies a list of routers on the subnet that are configured as DHCP relay agents, in order of preference from top to bottom. The options available are: <ul style="list-style-type: none"> • Add—Adds a relay agent. • Delete—Deletes a relay agent. 	Click an option.
WINS Servers	Specifies the name of the SNMP trap group being configured. The options available are: <ul style="list-style-type: none"> • Add—Adds a NetBIOS name server. • Delete—Deletes a NetBIOS name server. 	Select an option.
Lease Time and Boot Options		
Maximum Lease Time	Specifies the maximum length of time in seconds, a client can hold a lease. (Dynamic BOOTP lease lengths can exceed this maximum time.)	Enter a from value 60 through 1,209,600.
Default Lease Time	Specifies the length of time in seconds, a client can hold a lease, for clients that do not request a specific lease length.	Enter a value from 60 through 2,419,200.
Boot File	Specifies the path and filename of the initial boot file to be used by the client.	Enter the path and filename.
Boot Server	Specifies the TFTP server that provides the initial boot file to the client.	Enter the IP address or hostname of the TFTP server.
Option Table		
Option Table		

Table 138: Add DHCP Services Configuration Details (continued)

Field	Function	Action
Code / Type / Value	<p>Defines a list of option codes, types, and values, in order of preference from top to bottom. It is mandatory to define all the options</p> <ul style="list-style-type: none"> Option Code—Type a number. Option Type—Select a type from the list that corresponds to the code. Option Value—Type a valid option value based on the type. <p>The options available are</p> <ul style="list-style-type: none"> Add—Adds the code/type/value. Delete—Deletes the code/type/value. 	Select an option.
DHCP Pool Information		
Address Pool Subnet	Specifies the pool subnet on which DHCP is configured.	Enter an IP address prefix.
Address Range Low	Specifies the lowest address in the IP address pool range.	Enter an IP address that is part of the subnet specified in Address Pool Subnet.
Address Range High	Specifies the highest address in the IP address pool range.	Enter an IP address that is part of the subnet specified in Address Pool Subnet. This address must be greater than the address specified in Address Range Low.
Exclude Addresses	<p>Specifies addresses to exclude from the IP address pool. The options available are:</p> <ul style="list-style-type: none"> Add—Adds an excluded address. Delete—Deletes an excluded address. 	Select an option.
Server Information		
Server Identifier	Specifies the server identifier to assign to the DHCP client in the address pool.	Enter the name of the server identifier.
Domain Name	Specifies the domain name to be assigned to the address pool.	Enter the domain name.
Next Server	Specifies the next sever that the client needs to contact.	Enter the server name.
Propagate Interface	Specifies the interface name to propagate TCP/IP settings to the pool	Enter the interface name.

Table 138: Add DHCP Services Configuration Details (continued)

Field	Function	Action
Domain Search	<p>Specifies the domain name to be searched. The options available are:</p> <ul style="list-style-type: none"> • Add—Adds the DHCP client in the address pool. • Delete—Deletes the DHCP client from the address pool. 	Click an option.
DNS Name Servers	<p>Specifies the DNS name to assign to the DHCP client in the address pool. The options available are:</p> <ul style="list-style-type: none"> • Add—Adds the DNS name in the address pool. • Delete—Deletes the DNS name in the address pool. 	Select an option.
Gateway Routers	<p>Specifies the gateway router to assign DHCP client in the address pool. The options available are:</p> <ul style="list-style-type: none"> • Add—Adds the gateway router to the address pool. • Delete—Deletes the gateway router to the address pool. 	Select an option.
WINS Servers	<p>Specifies the WINS servers to assign to the DHCP client in the address pool. The options available are:</p> <ul style="list-style-type: none"> • Add—Adds WINS servers to the address pool. • Delete—Deletes WINS servers from the address pool. 	Select an option.
Lease Time		
Maximum Lease Time	Specifies the maximum amount of time in seconds, that DHCP should lease an address.	Enter a value.
Default Lease Time	Specifies the default amount of time in seconds, that DHCP should lease an address.	Enter a value.
Boot File	Specifies the boot file to be assigned to any DHCP client in the pool address.	Enter the boot file name.
Boot Server	Specifies the boot server to be assigned to any DHCP client in the pool address.	Enter the boot server name.
Option Table		

Table 138: Add DHCP Services Configuration Details (continued)

Field	Function	Action
Code / Type / Value	<p>Defines a list of option codes, types, and values, in order of preference from top to bottom. It is mandatory to define all the options.</p> <ul style="list-style-type: none"> Option Code—Type a number. Option Type—Select a type from the list that corresponds to the code. Option Value—Type a valid option value based on the type. <p>The options available are</p> <ul style="list-style-type: none"> Add—Adds the code, type, and value. Delete—Deletes the code, type, and value. 	Select an option.
Static Bindings		
DHCP Static Binding Information		
DHCP MAC Address	Specifies the hardware MAC address to statically assign DHCP information.	Enter the MAC address.
Host Name	Specifies the hostname to assign the DHCP client to the MAC address.	Enter the hostname.
Fixed Address	<p>Specifies the fixed address to assign the DHCP client to the MAC address. The options available are:</p> <ul style="list-style-type: none"> Add—Adds the fixed address. Delete—Deletes the fixed address. 	Select an option.
Client Identifier	Specifies the client identifier option.	Select the ASCII/hexadecimal value from the vale box, and enter the corresponding value in the edit box.
Server Information		
Server Identifier	Specifies the server identifier for assigning the DHCP client to the MAC address.	Enter the server identifier name.
Domain Name	Specifies the domain name to assign the DHCP client to the MAC address.	Enter the domain name.
Next Server	Specifies the next server the client must contact to assign the DHCP client to the MAC address.	Enter the next server address.
Domain Search	<p>Specifies the domain name to be serached. The options available are:</p> <ul style="list-style-type: none"> Add—Adds a domain name to be searched. Delete—Deletes a domain name to be searched. 	Enter the domain name to be searched.

Table 138: Add DHCP Services Configuration Details (continued)

Field	Function	Action
Gateway Routers	<p>Specifies the gateway router to assign to the specific MAC address. The options available are:</p> <ul style="list-style-type: none"> • Add—Adds the gateway router to the address pool. • Delete—Deletes the gateway router from the address pool. 	Select an option.
Name Servers	<p>Specifies the name servers to assign to the specific MAC address. The options available are:</p> <ul style="list-style-type: none"> • Add—Adds name servers in the address pool. • Delete—Deletes name servers in the address pool. 	Select an option.
WINS Servers	<p>Specifies the WINS servers to assign to the specific MAC address. The options available are:</p> <ul style="list-style-type: none"> • Add—Adds WINS servers in the address pool. • Delete—Deletes WINS servers in the address pool. 	Select an option.
Boot Options		
Boot File	Specifies a boot file to be assigned to the specific MAC address.	Enter the boot filename.
Boot Server	Specifies a boot server to be assigned to the specific MAC address.	Enter the boot server name.
Option Table		
Code / Type / Value	<p>Defines a list of option codes, types, and values, in order of preference from top to bottom. It is mandatory to define all the options.</p> <ul style="list-style-type: none"> • Option Code—Type a number. • Option Type—Select a type from the list corresponding to the code. • Option Value—Type a valid option value based on the type. <p>The options available are:</p> <ul style="list-style-type: none"> • Add—Adds an option code, type and value. • Delete—Deletes an option code, type and value. 	Select an option.

- See Also**
- [DHCP Client Configuration Page Options on page 231](#)
 - [Boot DHCP Relay Configuration Page Options](#)

Routing Instances Configuration Page Options

A routing instance is a collection of routing tables, interfaces, and routing protocol parameters. The set of interfaces belongs to the routing tables, and the routing protocol parameters control the information in the routing tables. There can be multiple routing tables for a single routing instance—for example, unicast IPv4, unicast IPv6, and multicast IPv4 routing tables can exist in a single routing instance. Routing protocol parameters and options control the information in the routing tables.

1. Select **Configure>Network>Routing Instance** in the J-Web user interface.

The Routing Instance page appears. [Table 139 on page 239](#) explains the contents of this page.



NOTE: If you log in as a tenant user, Routing Instance page is not displayed.

This is applicable for routing instance of root and LSYS users. Routing instances of root will be shown in root context and routing instances of the LSYS will be shown in LSYS context.

2. Click one:
 - **Add** or **+**—Adds a new routing instances. Enter information as specified in [Table 140 on page 239](#).
 - **Edit** or **/**—Edits the selected routing configuration [Table 140 on page 239](#).
 - **Delete** or **X**—Deletes the selected routing configuration.
3. Click Commit icon at the top of the J-Web page. The following commit options are displayed.
 - **Commit**—Commits the configuration and returns to the main configuration page.
 - **Compare**—Enables you to compare the current configuration with the previous configuration.
 - **Discard**—Discards the configuration changes you performed in the J-Web.
 - **Preferences**—There are two tab:
 - **Commit preferences**—You can choose to just validate or validate and commit the changes.
 - **Confirm commit timeout (in min)**—You can select the commit timeout interval.

Table 139: Routing Instance Configuration Page

Field	Function
Name	Name of the routing instance.
Type	Identifies the routing instance type.
Assigned Interfaces	Displays the selected interfaces assigned to the routing instance.
Description	Displays the description of the routing instances.

Table 140: Add-Edit Routing Instance Details

Field	Function	Action
General Settings		
Name	Specify the name of the routing instances.	Enter a unique name for the routing instance that contains a corresponding IP unicast table; no special characters are allowed and the keyword default cannot be used.
Description	Specify the description for the routing instance.	Enter a description for the routing instance. We recommend that you enter a maximum of 255 characters.
Instance Type	Specify the type of routing instance.	Select the type of routing instance from the drop down list: <ul style="list-style-type: none"> Virtual Router- Used for non-VPN related applications. VPLS- This instance is applicable only for root or super admin. This option will not be applicable for LSYS admin. Interfaces with Encapsulation Ethernet-VPLS will be listed when VPLS instance type is selected.
Interfaces		
Name	Displays the interface name.	Select interfaces from the available interfaces.
Zone	Displays the zone name corresponding to the interface name.	This is used to validate that all the interfaces of the selected zone(s) must belong to the same routing instance.

Static Routing Configuration Page Options

1. Select **Configure>Network>Routing>Static Routing** in the J-Web user interface.

The Static Routing configuration page appears. [Table 141 on page 240](#) explains the contents of this page.

2. Click one:

- **Add** or **+**—Adds a new or duplicate static routing configuration. Enter information as specified in [Table 142 on page 240](#).
- **Edit** or **/**—Edits the selected static routing configuration.
- **Delete** or **X**—Deletes the selected static routing configuration.

3. Click one:

- **OK**—Saves the configuration and returns to the main configuration page.
- **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
- **Cancel**—Cancels your entries and returns to the main configuration page.

Table 141: Static Routing Configuration Page

Field	Function
Static Routing	
Route	Displays the static route selected.
Next-hop	Displays the selected next-hop address selected.
Routing Instance	Displays the routing instance selected for this route.

Table 142: Add Static Routing Configuration Details

Field	Function	Action
Static Route		
Routing Instance	Specify the destination routing instance that points to the routing table containing the tunnel destination address. NOTE: If you log in as a tenant user, routing instance is not displayed as tenant context supports only one routing instance.	Select the routing instance from the list.
IPv4	Specifies an IPv4 address.	Click the IPv4 radio button.
IPv6	Specifies an IPv6 address.	Click the IPv6 radio button.
IP address	Specifies the IP address of the static route.	Enter the static route IP address.
Subnet mask	Specifies the subnet mask.	Enter the subnet mask or address prefix. For example, 24 bits represents the 255.255.255.0 address.

Table 142: Add Static Routing Configuration Details (continued)

Field	Function	Action
Nexthop	Displays the nex-thop address created. The options available are: <ul style="list-style-type: none"> • Delete—Adds the nexthop. • Delete—Deletes the nexthop. 	Select an option.

- See Also**
- [RIP Configuration Page Options on page 241](#)
 - [OSPF Configuration Page Options on page 246](#)
 - [BGP Configuration Page Options on page 252](#)
 - [Policies Configuration Page Options on page 258](#)

RIP Configuration Page Options

1. Select **Configure>Network>Routing>RIP** in the J-Web user interface.
The RIP configuration page appears. [Table 143 on page 241](#) explains the contents of this page.
2. Click one:
 - **Routing Instance**:—Displays the master routing instance or all routing instances.
 - **Add** or **+**—Adds a new or duplicate RIP configuration. Enter information as specified in [Table 144 on page 242](#).
 - **Edit** or **/**—Edits the selected RIP configuration.
 - **Delete** or **X**—Deletes the selected RIP configuration.
3. Click one:
 - **OK**—Saves the configuration and returns to the main configuration page.
 - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
 - **Cancel**—Cancels your entries and returns to the main configuration page.

Table 143: RIP Configuration Page

Field	Function
RIP Instance	Displays the RIP instance selected.
Neighbors	Displays the neighbors selected.
Routing Instance	Displays the routing instance.
Export Policies	Displays the export policies selected.

Table 143: RIP Configuration Page (continued)

Field	Function
Import Policies	Displays the import policies selected.
Preference	Displays the preference selected.
Update Interval	Displays the update interval selected.
Metric-out	Displays the metric-out value selected.

Table 144: Add RIP Configuration Details

Field	Function	Action
Routing Information Protocol Configuration		
General		
Routing Instance	Specifies whether you want to display only the master routing instance or all routing instances	Select from the list.
Routing Instance Name	Specifies a name for the routing instance.	Enter the routing instance name.
Preference	Specifies the preference order of external routes learned by RIP as compared to those learned from other routing protocols.	Enter the preference of the external routes.
Metric-out	Specifies the metric value to add to routes transmitted to the neighbor.	Enter the metric value.
Update Interval	Specifies an update time interval to periodically send out routes learned by RIP to neighbors.	Enter the update time.
Route Timeout	Specifies the route timeout interval for RIP.	Enter the route timeout interval.
Policy		

Table 144: Add RIP Configuration Details (continued)

Field	Function	Action
Import Policy	<p>Specifies one or more policies to control which routes learned from an area are used to generate summary link-state advertisements (LSAs) into other areas. The options available are:</p> <ul style="list-style-type: none"> • Add—Adds an import policy. • Move up—Moves the selected policy up the list of policies. • Move down—Moves the selected policy down the list of policies. • Remove—Removes an import policy. 	Select an option.
Export Policy	<p>Specifies one or more policies to control which summary LSAs are flooded into an area. The options available are:</p> <ul style="list-style-type: none"> • Add—Adds an export policy. • Move up—Moves the selected policy up the list of policies. • Move down—Moves the selected policy down the list of policies. • Remove—Removes an export policy. 	Select an option.
Neighbor		
Displays the RIP-enabled interfaces, its port, metric-in, and update interval.		
Associate	Selects interface(s) to associate with the instance.	<p>Select the box next to the interface name to enable RIP on an interface.</p> <p>Click the edit icon / to modify the selected interface's settings.</p> <p>NOTE: Only logical interfaces for RIP are displayed.</p>

Table 145: Edit RIP Global Setting Configuration Details

Field	Function	Action
General		
Send	<p>Specifies RIP send options. The options available are:</p> <ul style="list-style-type: none"> • Broadcast • Multicast • None • Version-1 	Select an option.

Table 145: Edit RIP Global Setting Configuration Details (continued)

Field	Function	Action
Receive	Configures RIP receive options. The options available are: <ul style="list-style-type: none"> Both None Version-1 Version-2 	Select an option.
Route timeout (sec)	Specifies the route timeout interval for RIP.	Enter the route timeout interval value.
Update interval (sec)	Specifies the update time interval to periodically send out routes learned by RIP to neighbors.	Enter the update time interval value.
Hold timeout (sec)	Specifies period for which the expired route is retained in the routing table before being removed.	Enter the hold timeout interval period.
Metric in	Specifies the metric to add to incoming routes when advertising into RIP routes that were learned from other protocols.	Enter the metric-in value.
RIB Group	Specifies a routing table group to install RIP routes into multiple routing tables.	Select the routing table group.
Message size	Specifies the number of route entries to be included in every RIP update message.	Enter the number of route entries.
Check Zero	Specifies whether the reserved fields in a RIP packet are set to zero. The options available are: <ul style="list-style-type: none"> check-zero—Discards version 1 packets that have nonzero values in the reserved fields and version 2 packets that have nonzero values in the fields that must be zero. This default behavior implements check-zerothe RIP version 1 and version 2 specifications. no-check-zero—Receives RIP version 1 packets with nonzero values in the reserved fields or RIP version 2 packets with nonzero values in the fields that must be zero. This behavior violates the specifications in RFC 1058 and RFC 2453. 	Select an option.
Graceful switchover	Specifies graceful switchover for RIP.	Select Disable .
Restart time (sec)	Specifies the estimated time for the restart to complete.	Enter the time in seconds.

Table 145: Edit RIP Global Setting Configuration Details (continued)

Field	Function	Action
Authentication Type	Specifies the type of authentication for RIP route queries received on an interface. The options available are: <ul style="list-style-type: none"> • None • MD5 • Simple 	Select the authentication type. Enter the authentication key for MD5.
Policy tab		
Import Policy	Specifies one or more policies to routes being imported into the local routing device from the neighbors. The options available are: <ul style="list-style-type: none"> • Add—Adds an export policy. • Move up—Moves the selected policy up the list of policies. • Move down—Moves the selected policy down the list of policies. • Remove—Removes an export policy. 	Click one:
Trace Options tab		
File Name	Specifies the name of the file to receive the output of the trace operation.	Enter the filename.
Number of Files	Specifies the maximum number of trace files.	Enter the filename.
File Size	Specifies the maximum size for each trace file.	Enter the file size.
World Readable	Specifies whether or not the trace file can be read by any user or not. The options available are: <ul style="list-style-type: none"> • True—Allows any user to read the file. • False up—Restricts all users being able to read the file. 	Select an option.
Flags		
Available Flags	Specifies the available trace operation to perform.	—
Configured Flags	Specifies the configured trace operation to perform.	—

- See Also**
- [Static Routing Configuration Page Options on page 239](#)
 - [OSPF Configuration Page Options on page 246](#)
 - [BGP Configuration Page Options on page 252](#)
 - [Policies Configuration Page Options on page 258](#)

OSPF Configuration Page Options

1. Select **Configure > Network > Routing > OSPF** in the J-Web user interface.

The OSPF configuration page appears. [Table 146 on page 246](#) explains the contents of this page.



NOTE:

- By default, All is selected in routing instance filter. For root users, this displays the OSPF areas configured under all routing instances including master (default).
- Logical system users and tenant users supports only SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, and SRX5800 devices.

2. Click one:

- **Add** or **+**—Adds a new or duplicate OSPF configuration. Enter information as specified in [Table 147 on page 247](#).



NOTE: Common fields, such as Router ID, Traffic Engineering, and Trace options are auto populated based on routing instance or OSPF version.

- **Edit** or **/**—Edits the selected OSPF configuration.
- **Delete** or **X**—Deletes the selected OSPF configuration.



NOTE: During the deleting process, only OSPF area specific configuration is deleted and not the common configurations, such as router-id, traffic-engineering, and trace-options.

3. Click one:

- **OK**—Saves the configuration and returns to the main configuration page.
- **Commit Options > Commit**—Commits the configuration and returns to the main configuration page.
- **Cancel**—Cancels your entries and returns to the main configuration page.

Table 146: OSPF Configuration Page

Field	Function
Area ID	Displays the area ID selected.
Area Type	Displays the area type selected.
Member Interfaces	Displays the member interface selected.

Table 146: OSPF Configuration Page (continued)

Field	Function
Version	Displays the version of the interface selected (OSPF for IPv4 and OSPFv3 for IPv6).
Routing Instance	Displays the routing instance of the interface selected. NOTE: This option is not available for tenant users.
Import Policy	Displays the import policy selected. NOTE: This option is not available for tenant users.
Export Policy	Displays the export policy selected. NOTE: This option is not available for tenant users.

Table 147: Add OSPF Configuration Details

Field	Function	Action
Basic Settings		
Routing Instance	Specifies the name of the routing instance. NOTE: This option is not available for tenant users.	Select the routing instance from the list or select Add to create a new routing instance. For more information on routing instance, see <i>Routing Instances Configuration Page Options</i> section.
Routing Options		
Router ID	Specifies the ID of the routing device.	Enter the ID of the routing device.
Traffic Engineering NOTE: This option is not available for OSPFv3.	Specifies whether traffic engineering is set to on or off.	Enable if you want the traffic to be managed or engineered.
Area Details		
Area Id	Specifies the uniquely identified area within its AS.	Type a 32-bit numeric identifier for the area. Type an integer or select and edit the value. If you enter an integer, the value is converted to a 32-bit equivalent. For example, if you enter 3, the value assigned to the area is 0.0.0.3 .

Table 147: Add OSPF Configuration Details (continued)

Field	Function	Action
Area Range	Displays a range of IP addresses for the summary link state advertisements (LSAs) to be sent within an area.	<p>Select an option:</p> <ol style="list-style-type: none"> To add an area range form: <ol style="list-style-type: none"> Click +. The Create Area Range form page appears. Enter the area range address. NOTE: For OSPF, enter an IPv4 address and for OSPFv3 enter an IPv6 address. Enter the subnet mask area address. NOTE: This option is available only for IPv4 address. Select a value to override the metric for the IP address range. Range: 1025 - 65534. Select Restrict Advertisements of this area range to specify that the routes contained within a summary must not be displayed. Select Enforce exact match for advertisements of this area range to specify that the summary of a route must be advertised only when an exact match is made within the configured summary range. Click OK. To edit the selected are range: <ol style="list-style-type: none"> Select the existing area range. Click the pencil icon to edit the selected area range. Click OK. To delete the area range: <ol style="list-style-type: none"> Select the area range that you want to delete. Click the delete icon. A message appears to confirm if you want to proceed with the deletion of the selected area range. Click Yes to delete the selected area range.
Area Type	<p>Specifies the type of OSPF area.</p> <ul style="list-style-type: none"> None—A regular OSPF area, including the backbone area. stub—A stub area. nssa—A not-so-stubby area (NSSA). 	Select an options.

NOTE: This option is not applicable for area zero.

Table 147: Add OSPF Configuration Details (continued)

Field	Function	Action
No Summaries (Totally Stubby area) NOTE: This option is applicable for non-zero area and it is not applicable for area zero.	Specifies whether summaries is enabled or disabled.	Enable or disable the summaries. NOTE: This option can be configured when area-type is nssa or stub.
Virtual Link NOTE: This option is applicable for area zero and it is not applicable for non-zero area.	Specifies the logical link using the least cost path between the ABR of the non-backbone connected area and the backbone ABR of the transit area.	Select whether you want the virtual link to be established. If you select virtual link to be created, then enter the Neighbor ID and Transit area. Transit area is the area that has virtual link connecting two or more ABRs attached to this area.
Interface Details		
Select Interface	Select one or more interfaces to associate with the routing instance from the interfaces displayed in the Available column.	Select the interface from the Available table and by using the arrow move it to the Selected table.
Interface type	Specifies the interfaces to be associated with the OSPF configuration. Options available are: <ul style="list-style-type: none"> • None—No interface. • nbma—Nonbroadcast multiaccess (NBMA) interface. NOTE: This option is not available for OSPFv3. <ul style="list-style-type: none"> • p2mp—Point-to-multipoint interface. • p2p—Point-to-point interface. • p2mp-over-lan—Point-to-multipoint over LAN mode. NOTE: This option is not available for OSPF.	Select the interface from the list.
Interface Metric	Displays the interface metric.	Type the metric that you want for measuring the interface.
Passive mode	Specifies the passive mode.	Enable if you want the passive mode. NOTE: You can enable this option only if Secondary option is disabled and vice-versa.
Advanced		

Table 147: Add OSPF Configuration Details (continued)

Field	Function	Action
Bidirectional Forward Detection	Specifies the bidirectional forwarding detection (BFD) protocol version that you want to detect.	<p>Enable or disable the bidirectional forward detection.</p> <p>If you enable, enter the following details:</p> <ul style="list-style-type: none"> BFD Version—Select the bidirectional forward detection version from the list: <ul style="list-style-type: none"> None—No BFD version is used. automatic—Autodetects the BFD protocol version. BFD Version 0—Uses BFD protocol version 0. BFD Version 1—Uses BFD protocol version 1. Minimum Interval—Enter the minimum interval value for BFD in milliseconds. Range: 1 through 255,000. Minimum Receive Interval—Enter the minimum receive interval value. Range: 1 through 255,000.
IPSec security association	Specifies the number of one of the security associations.	<p>Select an option from the list.</p> <p>By default, no security keys are configured.</p> <p>NOTE: You can configure this option only if Secondary option is disabled and vice-versa.</p>
Link protection	Creates a backup loop-free alternate path to the primary next hop for all destination routes that traverse the protected interface.	<p>Enable or disable this option.</p> <p>NOTE: You can either enable Link protection or Node Link protection at a time. For example, if you enable Link protection, then Node Link protection is automatically disabled.</p>
Node Link protection	Creates an alternate loop-free path to the primary next hop for all destination routes that traverse a protected interface.	<p>Enable or disable this option.</p>
Secondary	Specifies an interface to belong to another OSPF area.	<p>Enable or disable this option.</p> <p>NOTE: You can enable this option only if Passive Mode is disabled and IPSec security association is not configured and vice-versa.</p>
Authentication	Specifies an authentication key (password).	<p>Select an option from the list:</p> <ul style="list-style-type: none"> None md5 simplepassword

NOTE: This option is not available for OSPFv3.

Table 147: Add OSPF Configuration Details (continued)

Field	Function	Action
MD5 Authentication Key NOTE: This option is not available for OSPFv3.	Specifies an MD5 authentication key (password).	Click + and enter the following details: <ul style="list-style-type: none"> MD5 ID—MD5 key identifier. Range: 0 through 255. Key—One or more MD5 key strings. The MD5 key values can be from 1 through 16 characters long. Characters can include ASCII strings. If you include spaces, enclose all characters in quotation marks (" "). Start Time—MD5 start time.
Simple Password NOTE: This option is not available for OSPFv3.	Specifies a simple authentication key (password).	Enter a password string.
Advanced Settings		
Policy		
NOTE: This option is not available for tenant users.		
Import Policy	Specifies one or more policies to control which routes learned from an area are used to generate summary link-state advertisements (LSAs) into other areas. The options available are: <ul style="list-style-type: none"> Add—Adds an import policy. Move up—Moves the selected policy up the list of policies. Move down—Moves the selected policy up the list of policies down. Remove— Removes the import policy. 	Select an option.
Export Policy	Specifies one or more policies to control which summary LSAs are flooded into an area. <ul style="list-style-type: none"> Add—Adds an export policy. Move up—Moves the selected policy up the list of policies. Move down—Moves the selected policy up the list of policies down. Remove— Removes the export policy. 	Select an option.
Trace Options		
File Name	Specifies the name of the file to receive the output of the trace operation.	Enter the filename.

Table 147: Add OSPF Configuration Details (continued)

Field	Function	Action
Number of files	Specifies the maximum number of trace files.	Enter the filename.
File Size	Specifies the maximum size for each trace file.	Enter the file size.
World Readable	Specifies whether the trace file can be read by any user or not.	Enable this option to allow any user to read the file. Disable this option to prevent all users from reading the file.
Flags		
Available Flags	Specifies the available trace operation to be performed.	Select available flags and move to Selected column using the right arrow.
Selected Flags	Specifies the configured trace operation to be performed.	Select selected flags and move to available column using the back arrow.

- See Also**
- [Static Routing Configuration Page Options on page 239](#)
 - [RIP Configuration Page Options on page 241](#)
 - [BGP Configuration Page Options on page 252](#)
 - [Policies Configuration Page Options on page 258](#)

BGP Configuration Page Options

1. Select **Configure>Network>Routing>BGP** in the J-Web user interface.
The BGP configuration page appears. [Table 148 on page 253](#) explains the contents of this page.
2. Click one:
 - **Add** or **+**—Adds a new or duplicate BGP configuration. Enter information as specified in [Table 149 on page 254](#).
 - **Edit** or **/**—Edits the selected BGP configuration.
 - **Delete** or **X**—Deletes the selected BGP configuration.
 - **Disable**—Disables selected BGP configuration.
3. Click one:
 - **OK**—Saves the configuration and returns to the main configuration page.
 - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.

- **Cancel**—Cancels your entries and returns to the main configuration page.

Table 148: BGP Configuration Page

Field	Function
Group Information	
Routing Instance NOTE: If you log in as a tenant user, the Routing Instance is not displayed as tenant context supports only one routing instance.	Displays the selected routing instances. Example: Master or All routing instances. The global information values corresponding to the the routing instance that you selected will be displayed in the Global Information section. Based on the routing instance that you select, the values in the Global information
Group Name	Displays the name of the group.
Status	Displays the status of the group.
Peer ASN	Displays the peer ASN.
Type	Displays the group type.
Dynamic Peers	Displays the dynamic peers selected.
Static Peers	Displays the static peers selected.
Routing Instance	Displays the routing instance selected.
Import Policy	Displays the import policy selected.
Export Policy	Displays the export policy selected.
NOTE: If you log in as a tenant user, Routing Instance, Import Policy, and Export Policy are not displayed.	
Global Information	
Edit or /	Edits the Global settings which lists the following fields. See Table 149 on page 254 for more details.
Name	Value
Router Identifier	Specifies the routing device's IP address.
BGP Status	Enables or disables BGP.
Router ASN	Specifies the routing device's AS number.
Preference	Specifies the route preference.
Confederation	Specifies the routing device's confederation AS number.
NOTE: If you log in as a tenant user, Confederation is not displayed.	

Table 148: BGP Configuration Page (continued)

Field	Function
Group Information	
Confederation Members	Specifies the AS numbers for the confederation members.
NOTE: If you log in as a tenant user, Confederation Members is not displayed.	
Description	Specifies the text description of the global, group, or neighbor configuration.
Import Policy	Specifies one or more routing policies for routes being imported into the routing table from BGP. The options available are:
NOTE: If you log in as a tenant user, Import Policy is not displayed.	
Export Policy	Specifies one or more policies to routes being exported from the routing table into BGP. The options available are:
NOTE: If you log in as a tenant user, Export Policy is not displayed.	

Table 149: Add/Edit BGP Configuration Details

Field	Function	Action
General Tab		
Routing Instance	Specifies whether the routing instance is a master instance or not.	Select an option from the list.
NOTE: If you log in as a tenant user, the Routing Instance is not displayed as tenant context supports only one routing instance.		
Group Name	Specifies the name for the group.	Enter a new group name.
Status	Specifies the status of the group.	-
ASN	Specifies the unique numeric identifier of the AS in which the routing device is configured.	Enter the routing device's 32-bit AS number, in dotted decimal notation. If you enter an integer, the value is converted to a 32-bit equivalent. For example, if you enter 3 , the value assigned to the AS is 0.0.0.3 .
Preference	Specifies the degree of preference for an external route. The route with the highest local preference value is preferred.	Enter the preface value.
Cluster Id	Specifies the cluster identifier to be used by the route reflector cluster in an internal BGP group.	Enter the IPv6 or IPv4 address to be used as the identifier.

Table 149: Add/Edit BGP Configuration Details (continued)

Field	Function	Action
Description	Specifies the text description of the global, group, or neighbor configuration.	Enter the description.
Damping	Specifies whether or not route flap damping is enabled.	<p>Select the check box to enable route flap damping.</p> <p>Do not select the check box to disable route flap damping .</p>
Advertise Inactive Routes	Specifies whether or not BGP advertises the best route even if the routing table did not select it to be an active route.	<p>Select the check box to enable advertising of inactive routes.</p> <p>Clear the check box to disable advertising of inactive routes.</p>
Advertise Peer AS Routes	Specifies whether or not to disable the default behavior of suppressing AS routes.	<p>Select the check box to advertising of peer AS routes, select the check box.</p> <p>Clear the check to disable advertising of peer AS routes.</p>
Neighbors Tab		
Dynamic Neighbors	<p>Configures a dynamic neighbor (peer). The options available are:</p> <ul style="list-style-type: none"> • Add—Adds the selected dynamic neighbor. • Edit—Edits the selected dynamic neighbor. • Delete—Deletes the selected dynamic neighbor. 	Select an option.
Static Neighbors	<p>Configures a static neighbor (peer). The options available are:</p> <ul style="list-style-type: none"> • Add—Adds the selected static neighbor. • Edit—Edits the selected static neighbor. • Delete—Deletes the selected static neighbor. 	Select an option.
Add neighbor		
All address/IPAddress	Specifies whether to select all address or IP address.	Select an option.
IP Address	Specifies the IP address.	Enter the IP address.
Subnet Mask	Specifies the subnet mask for the neighbor.	Enter the subnet mask.
Policies Tab		

Table 149: Add/Edit BGP Configuration Details (continued)

Field	Function	Action
Import Policy	<p>Specifies one or more routing policies for routes being imported into the routing table from BGP. The options available are:</p> <ul style="list-style-type: none"> • Add—Adds an import policy. • Move up—Moves the selected policy up the list of policies. • Move down—Moves the selected policy down. • Remove — Removes an import policy. 	Select an option.
Export Policy	<p>Specifies one or more policies to routes being exported from the routing table into BGP. The options available are:</p> <ul style="list-style-type: none"> • Add—Adds an export policy. • Move up—Moves the selected policy up the list of policies. • Move down—Moves the selected policy down • Remove — Removes an export policy. 	Select an option.

Table 150: Edit BGP Global Setting Configuration Details

Field	Function	Action
General		
Router ASN	Specifies the routing device's AS number.	Enter the router ASN value.
Router Identifier	Specifies the routing device's IP address.	Enter the router identification IP address.
BGP Status	Enables or disables BGP.	<p>To enable BGP, select Enabled.</p> <p>To disable BGP, select Disabled.</p>
Description	Describes the global, group, or neighbor configuration.	Enter the description.
Confederation Number	Specifies the routing device's confederation AS number.	Enter the value.
Confederation Members	Specifies the AS numbers for the confederation members.	To add a member AS number, click Add and enter the number in the Member ASN box. Click OK .
Advance Options		

Table 150: Edit BGP Global Setting Configuration Details (continued)

Field	Function	Action
Keep Route	Specifies whether routes learned from a BGP peer must be retained in the routing table even if they contain an AS number that was exported from the local AS. The options available are: <ul style="list-style-type: none"> • All • None 	Select All or None to configure Keep Routes.
MTU Discovery	Specifies the option for configure MTU discovery.	Enable MTU discovery.
Remove Private ASN	Specifies the local system strip private AS numbers from the AS path when advertising AS paths to remote systems.	Enable removal of private ASNs.
Graceful Restart	Specifies the period of time after which a restart is expected to be complete. Specifies the maximum time that stale routes are kept during restart.	Enter the time period for a graceful restart and the maximum time that stale routes must be kept.
Multihop	Specifies the maximum time-to-live (TTL) value for the TTL in the IP header of BGP packets.	Select NextHop Change to allow unconnected third-party next hops. Enter a TTL value.
Authentication Type	Specifies the authentication algorithm: None, MD5, or SHA1.	Select the authentication algorithm. If you select MD5, specify an MD5 authentication key (password).

Policies Tab

NOTE: If you log in as a tenant user, Policy tab is not displayed.

Import Policy	Applies one or more policies to routes being imported into the local routing device from the neighbors. The options available are: <ul style="list-style-type: none"> • Add—Adds an import policy. • Move up—Moves the selected policy up the list of policies. • Move down—Moves the selected policy down • Remove—Removes an export policy. 	Select an option.
Export Policy	Specifies one or more policies to control which summary LSAs are flooded into an area. The options available are: <ul style="list-style-type: none"> • Add—Adds an export policy. • Move up—Move the selected policy up the list of policies. • Move down—Move the selected policy up the list of policies. • Remove—Removes an export policy. 	Select an option.

Trace Options Tab

Table 150: Edit BGP Global Setting Configuration Details (continued)

Field	Function	Action
File Name	Specifies the name of the file to receive the output of the trace operation.	Type or select and edit the name.
Number of Files	Specifies the maximum number of trace files.	Type or select and edit the number.
File Size	Specifies the maximum size for each trace file.	Type or select and edit the size.
World Readable	Specifies whether the trace file can be read by any user.	True —allows any user to read the file. False —prevents all users from reading
Flags		
Available Flags	Specifies the available trace operation to perform.	—
Configured Flags	Specifies the configured trace operation to perform.	—

- See Also**
- [Static Routing Configuration Page Options on page 239](#)
 - [RIP Configuration Page Options on page 241](#)
 - [OSPF Configuration Page Options on page 246](#)
 - [Policies Configuration Page Options on page 258](#)

Policies Configuration Page Options

1. Select **Configure>Network>Policies** in the J-Web user interface.

The Policies configuration page appears. [Table 151 on page 259](#) explains the contents of this page.



NOTE: If you log in as a tenant user, the Policies page is not displayed.

2. Click one:
 - **Global Settings**—Defines general specifications for routing policies. Enter information as specified in [Table 152 on page 259](#).
 - **Add or +**—Adds a new or duplicate term policies configuration. Enter information as specified in [Table 153 on page 260](#).
 - **Term Up**— Moves a term up in a selected list policies configuration.
 - **Term Down**— Moves a term down in a selected list policies configuration.
 - **Edit or /**—Edits the selected policies configuration.

- **Delete** or **X**—Deletes the selected policies configuration.
 - **Test Policy**— Verifies that a policy to check if the policy produces the expected results for the selected policies configuration.
3. Click one:
- **OK**—Saves the configuration and returns to the main configuration page.
 - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
 - **Cancel**—Cancels your entries and returns to the main configuration page.

Table 151: Policies Configuration Page

Field	Function
Name	Displays the name of the policy.
From: Prefix	Displays the policy prefix.
From: Protocol	Displays the selected protocol.
From: Interface or Address	Need Input
To: Protocol	Need Input
To: Interface or Address	Displays the selected interface or address.
Action	Displays the selected action.
Move To	Need Input

Table 152: Edit Global Setting Configuration Details

Field	Function	Action
Add Prefix List		
Name	Displays the name of the prefix list. The options available are: <ul style="list-style-type: none"> • Add—Adds the prefix list. • Edit—Edits the prefix list. • Removes—Removes the prefix list. 	Select an option.
Members		
IP Address	Specifies the member IP address.	Enter the member IP address.
Add Prefix List Members		
IP Address	Specifies the prefix list IP address.	Enter the prefix list IP address.
Subnet Mask	Specifies the subnet mask IP address.	Enter the subnet mask IP address.

Table 152: Edit Global Setting Configuration Details (continued)

Field	Function	Action
BGP Community		
Name	Displays the BGP community name.	—
Add BGP Community		
Name	Specifies the BGP community name.	Enter the BGP community name.
Members		
Community	Displays the BGP community.	—
Add BGP Community Members		
Community ID	Specifies the BGP community ID.	Enter the BGP community ID.
As Path		
Name	Displays the path name.	—
Add As Path		
As Path Name	Specifies the AS path name.	Enter the name of the as path.
Regular Expression	Specifies the regular expression of the As path.	Enter the regular expression.

Table 153: Add Terms Configuration Parameters

Field	Function	Your Action
Term Name	Specifies a term name.	Enter the term name.
Source tab		
Family	Specifies an address family protocol.	Enter the family protocol address.
Routing Instance	Specifies a routing instance.	Select a value from the list.
RIB	Specifies the name of a routing table.	Select a value from the list.
Preference	Specifies the individual preference value for the route.	Enter a preference value.
Metric	Specifies a metric value. You can specify up to four metric values.	Enter the metric value.
Interface	Specifies the name or IP address of one or more routing device interfaces. Do not use this qualifier with protocols that are not interface-specific, such as internal BGP (IBGP).	<p>To add an interface, select Add > Interface. Select the interface from the list.</p> <p>To add an address, select Add > Address. Select the address from the list.</p> <p>To remove an interface, select it and click Remove.</p>

Table 153: Add Terms Configuration Parameters (continued)

Field	Function	Your Action
Prefix List	Specifies a named list of IP addresses. You can specify an exact match with incoming routes.	Click Add . Select the prefix list from the list and click OK . To remove a prefix list, select it and click Remove .
Protocol	Specifies the name of the protocol from which the route was learned or to which the route is being advertised.	Click Add and select the protocol from the list. To remove a protocol, select it and click Remove .
Policy	Specifies the name of a policy to evaluate as a subroutine.	Click Add . Select the policy from the list. To remove a policy, select it and click Remove .
More		
More	Specifies advanced configuration options for policies.	Click More for advanced configuration.
OSPF Area ID	Specifies the area identifier.	Enter the IP address.
BGP Origin	Specifies the origin of the AS path information.	Select a value from the list.
Local Preference	Specifies the BGP local preference.	Type a local preference value.
Route		
External	Specifies the type of route.	Select an option from the list.
OSPF type	Specifies the OSPF type.	Select the OSPF type.
AS Path		
Name	Specifies the name of an AS path regular expression.	Click Add . Select the AS path from the list.
Community		
Name	Specifies the name of one or more communities.	Click Add . Select the community from the list.
Destination tab		
Family	Specifies an address family protocol.	Select a value from the list.
Routing Instance	Specifies a routing instance.	Select a value from the list.
RIB	Specifies the name of a routing table.	Select a value from the list.
Preference	Specifies the individual preference value for the route.	Type a preference value.

Table 153: Add Terms Configuration Parameters (continued)

Field	Function	Your Action
Metric	Specifies a metric value.	Type a metric value.
Interface		
Name	Specifies the name or IP address of one or more routing device interfaces. Do not use this qualifier with protocols that are not interface-specific, such as internal BGP (IBGP).	<p>To add an interface, select Add > Interface. Select the interface from the list.</p> <p>To add an address, select Add > Address. Select the address from the list.</p> <p>To delete an interface, select it and click Remove.</p>
Policy		
Name	Displays the name of the policy.	—
Protocol		
Name	Specifies the name of the protocol from which the route was learned or to which the route is being advertised.	<p>Click Add and select the protocol from the list.</p> <p>To delete a protocol, select it and click Remove.</p>
Action		
Action	Specifies the action to take if the conditions match.	Select a value from the list.
Default Action	Specifies that any action that is intrinsic to the protocol is overridden. This action is also nonterminating so that various policy terms can be evaluated before the policy is terminated.	Select a value from the list.
Next	Specifies the default control action if a match occurs, and there are no further terms in the current routing policy.	Select a value from the list.
Priority	Specifies a priority for prefixes included in an OSPF import policy. Prefixes learned through OSPF are installed in the routing table based on the priority assigned to the prefixes.	Select a value from the list.
BGP Origin	Specifies the BGP origin attribute.	Select a value from the list.
AS Path Prepend	Affixes an AS number at the beginning of the AS path. AS numbers are added after the local AS number has been added to the path. This action adds an AS number to AS sequences only, not to AS sets. If the existing AS path begins with a confederation sequence or set, the affixed AS number is placed within a confederation sequence. Otherwise, the affixed AS number is placed with a nonconfederation sequence.	Enter AS path prepend value.
AS Path Expand		

Table 153: Add Terms Configuration Parameters (continued)

Field	Function	Your Action
Type	Extracts the last AS number in the existing AS path and affixes that AS number to the beginning of the AS path n times, where n is a number from 1 through 32. The AS number is added before the local AS number has been added to the path. This action adds AS numbers to AS sequences only, not to AS sets. If the existing AS path begins with a confederation sequence or set, the affixed AS numbers are placed within a confederation sequence. Otherwise, the affixed AS numbers are placed within a nonconfederation sequence. This option is typically used in non-IBGP export policies.	Select the type and type a value.
Value	Specifies the As path value.	Enter the As path value.
Preference		
Action	Specifies the preference action.	Select the preference action and type a value.
Value	Specifies the preference value.	Enter the preference value.
Local Preference		
Action	Specifies the BGP local preference action.	Select the action and type a value.
Value	Specifies the local preference value.	Enter the local preference value.
Load Balance Per Packet	Specifies that all next-hop addresses in the forwarding table must be installed and have the forwarding table perform per-packet load balancing. This policy action allows you to optimize VPLS traffic flows across multiple paths.	Select the check box to enable the option.
Tag		
Action	Specifies the tag value. The tag action sets the 32-bit tag field in OSPF external link-state advertisement (LSA) packets.	Select the action and type a value.
Value	Specifies the tag value.	Enter the tag value.
Metric		
Action	Changes the metric (MED) value by the specified negative or positive offset. This action is useful only in an external BGP (EBGP) export policy.	Select the action and type a value.
Value	Specifies the metric value.	Enter the metric value.
Route		
External	Specifies whether or not the route is external.	Select the External check box to enable the option, and select the OSPF type.
OSPF Type	Specifies the route value.	Enter the route value.
Class of Service		

Table 153: Add Terms Configuration Parameters (continued)

Field	Function	Your Action
Class	Specifies the class-of-service parameters to be applied to routes installed into the routing table.	Select none .
Source Class	Specifies that the value entered here maintains the packet counts for a route passing through your network, based on the source address.	Enter the source class.
Destination Class	Specifies the value entered here maintains packet counts for a route passing through your network, based on the destination address in the packet.	Enter the destination class.
Forwarding Class	Specifies that the value of queue number entered here maintains packet counts for a route passing through your network, based on the internal queue number assigned in the packet.	Enter the forwarding class.

- See Also**
- [Static Routing Configuration Page Options on page 239](#)
 - [RIP Configuration Page Options on page 241](#)
 - [OSPF Configuration Page Options on page 246](#)
 - [BGP Configuration Page Options on page 252](#)

Class of Service

- [Value Alias Configuration Page Options on page 264](#)
- [Forwarding Classes Configuration Page Options on page 266](#)
- [Classifiers Configuration Page Options on page 267](#)
- [Rewrite Rules Configuration Page Options on page 270](#)
- [Schedulers Configuration Page Options on page 272](#)
- [Scheduler Maps Configuration Page Options on page 274](#)
- [Drop Profile Configuration Page Options on page 275](#)
- [Virtual Channel Groups Configuration Page Options on page 276](#)
- [Assign To Interface Configuration Page Options on page 278](#)

Value Alias Configuration Page Options

1. Select **Configure>Class of Service>Value Aliases** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Configure>Network>Class of Service>Value Aliases** in the J-Web user interface.

The Code Point Alias configuration page appears. [Table 154 on page 265](#) explains the contents of this page.

2. Click one:

- **Add** or **+**—Adds a new or duplicate code point alias configuration. Enter information as specified in [Table 155 on page 265](#).
- **Edit** or **/**—Edits the selected code point alias configuration.
- **Delete** or **X**—Deletes the selected code point alias configuration.

3. Click one:

- **OK**—Saves the configuration and returns to the main configuration page.
- **Commit Options > Commit**—Commits the configuration and returns to the main configuration page.
- **Cancel**—Cancels your entries and returns to the main configuration page.

Table 154: Code Point Alias Configuration Page

Field	Function
Alias name	Displays the name given to CoS values. For example, af11 or be .
Alias type	<p>Displays the code point type.</p> <p>The following types of code points are supported:</p> <ul style="list-style-type: none"> • DSCP—Defines aliases for Differentiated Services code point (DSCP) for IPv4 values. You can refer to these aliases when you configure classes and define classifiers. • DSCP-IPv6—Defines aliases for DSCP IPv6 values. You can refer to these aliases when you configure classes and define classifiers. • EXP—Defines aliases for MPLS experimental (EXP) bits. You can map MPLS EXP bits to the device forwarding classes. • inet-precedence—Defines aliases for IPv4 precedence values. Precedence values are modified in the IPv4 TOS field and mapped to values that correspond to levels of service.
CoS Value bits	<p>Displays the CoS value for which an alias is defined.</p> <p>NOTE: Changing this value alters the behavior of all classifiers that refer to this alias.</p>

Table 155: Add Code Point Alias Configuration Details

Field	Function	Action
Code point name	Specifies a name for the CoS point alias.	Enter a name for the CoS point alias.
Code point type	Specifies a code point type.	Select a code point type from the list.
Code point value bits	Specifies a CoS value for which an alias is defined.	Select a COS value from the list.

- See Also**
- [Forwarding Classes Configuration Page Options on page 266](#)
 - [Classifiers Configuration Page Options on page 267](#)
 - [Rewrite Rules Configuration Page Options on page 270](#)

Forwarding Classes Configuration Page Options

1. Select **Configure>Class of Service>Forwarding Classes** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Configure>Network>Class of Service>Forwarding Classes** in the J-Web user interface.

The Forwarding Class configuration page appears. [Table 156 on page 266](#) explains the contents of this page.

2. Click one:
 - **Add** or **+**—Adds a new or duplicate forwarding class configuration. Enter information as specified in [Table 157 on page 267](#).
 - **Edit** or **/**—Edits the selected forwarding class configuration.
 - **Delete** or **X**—Deletes the selected forwarding class configuration.
3. Click one:
 - **OK**—Saves the configuration and returns to the main configuration page.
 - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
 - **Cancel**—Cancels your entries and returns to the main configuration page.

Table 156: Forwarding Class Configuration Page

Field	Function
Forwarding class name	<p>Displays the forwarding class name assigned to the internal queue number.</p> <p>By default, four forwarding classes are assigned to queue numbers: 0 (best-effort), 1 (assured-forwarding), 5 (expedited-forwarding), and 7 (network-connect).</p>
Queue number	<p>Displays the internal queue numbers to which forwarding classes are assigned.</p> <p>By default, if a packet is not classified, it is assigned to the class associated with queue 0. You can have more than one forwarding class assigned to a queue number.</p>
Queue characteristics	Displays the queue characteristics, for example, video or voice.

Table 157: Add Forwarding Class Configuration Details

Field	Function	Action
Queue number	Specifies the internal queue number to which a forwarding class is assigned.	Select a queue number from the list.
Forwarding class name	Specifies the forwarding class name assigned to the internal queue number.	Enter a forwarding class name.

- See Also**
- [Value Alias Configuration Page Options on page 264](#)
 - [Classifiers Configuration Page Options on page 267](#)
 - [Rewrite Rules Configuration Page Options on page 270](#)

Classifiers Configuration Page Options

1. Select **Configure>Class of Service>Classifiers** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.
 Or
 Select **Configure>Network>Class of Service>Classifiers** in the J-Web user interface.
 The Classifier configuration page appears. [Table 158 on page 267](#) explains the contents of this page.
2. Click one:
 - **Add** or **+**—Adds a new or duplicate classifier configuration. Enter information as specified in [Table 159 on page 268](#).
 - **Edit** or **/**—Edits the selected classifier configuration.
 - **Delete** or **X**—Deletes the selected classifier configuration.
3. Click one:
 - **OK**—Saves the configuration and returns to the main configuration page.
 - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
 - **Cancel**—Cancels your entries and returns to the main configuration page.

Table 158: Classifiers Configuration Page

Field	Function
Classifier name	Displays the name of a classifier.

Table 158: Classifiers Configuration Page (continued)

Field	Function
Classifier type	<p>Displays the classifier type.</p> <p>The following type of classifiers are supported on :</p> <ul style="list-style-type: none"> J Series (J6350), SRX210, SRX240, SRX650: <ul style="list-style-type: none"> dscp—Differentiated Services code point classifier for IPv4 dscp-ipv6—Differentiated Services code point classifier for IPv6 (default and compatibility) exp—MPLS experimental (EXP) bits classifier ieee-802.1—IEEE-802.1 classifier ieee-802.1ad—IEEE-802.1ad classifier inet-precedence—IPv4 precedence classifier (default and compatibility) SRX3400, SRX3600, SRX5600, SRX5800: <ul style="list-style-type: none"> dscp—Differentiated Services code point classifier for IPv4 dscp-ipv6—Differentiated Services code point classifier for IPv6 ieee-802.1—IEEE-802.1 classifier ieee-802.1ad—IEEE-802.1ad classifier inet-precedence—Precedence classifier for IPv4
Details of classifiers	
Incoming code point	Displays CoS values and the aliases to which the forwarding class and loss priority are mapped.
Forwarding class name	Displays forwarding class names that are assigned to specific CoS values and aliases of a classifier.
Loss priority	Displays loss priorities that are assigned to specific CoS values and aliases of a classifier.

Table 159: Add Classifiers Configuration Details

Field	Function	Action
Classifier name	Specifies the name of a classifier.	Enter the classifier name.

Table 159: Add Classifiers Configuration Details (continued)

Field	Function	Action
Classifier type	Specifies a classifier type.	Select a classifier type from the list. <ul style="list-style-type: none"> • J Series (J6350), SRX210, SRX240, SRX650: <ul style="list-style-type: none"> • dscp—Differentiated Services code point classifier for IPv4. • dscp-ipv6—Differentiated Services code point classifier for IPv6. • exp—MPLS experimental bits classifier. • ieee-802.1—IEEE-802.1 classifier. • ieee-802.1ad—IEEE-802.1ad classifier. • inet-precedence—Precedence classifier for IPv4. • SRX3400, SRX3600, SRX5600, SRX5800: <ul style="list-style-type: none"> • dscp—Differentiated Services code point classifier for IPv4. • dscp-ipv6—Differentiated Services code point classifier for IPv6. • ieee-802.1—IEEE-802.1 classifier. • ieee-802.1ad—IEEE-802.1ad classifier. • inet-precedence—Precedence classifier for IPv4.
Code point mapping	Specifies the code point mapping created.	Click one: <ul style="list-style-type: none"> • Add—Adds a code point mapping. • Edit—Edits the selected code point mapping. • Delete—Deletes a record.
Code point	Specifies the CoS value in bits and the alias of a classifier.	Select the CoS value in bits and the alias of a classifier from the list.
Forwarding class	Specifies the forwarding class to the specified CoS value and alias.	Select the forwarding class for the specified CoS value and alias from the list.
Loss priority	Specifies a loss priority for the specified CoS value and alias.	Select the loss priority for the specified CoS value and alias from the list.

See Also

- [Rewrite Rules Configuration Page Options on page 270](#)
- [Forwarding Classes Configuration Page Options on page 266](#)

- [Value Alias Configuration Page Options on page 264](#)

Rewrite Rules Configuration Page Options

1. Select **Configure>Class of Service>Rewrite Rules** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Configure>Network>Class of Service>Rewrite Rules** in the J-Web user interface.

The Configure Rewrite Rule configuration page appears. [Table 160 on page 270](#) explains the contents of this page.

2. Click one:
 - **Add** or **+**—Adds a new or duplicate rewrite rule configuration. Enter information as specified in [Table 161 on page 270](#).
 - **Edit** or **/**—Edits the selected rewrite rule configuration.
 - **Delete** or **X**—Deletes the selected rewrite rule configuration.
3. Click one:
 - **OK**—Saves the configuration and returns to the main configuration page.
 - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
 - **Cancel**—Cancels your entries and returns to the main configuration page.

Table 160: Rewrite Rule Configuration Page

Field	Function
Rewrite rule name	Displays the names of defined rewrite rules.
Rewrite rule type	Displays the rewrite rule type.
Code Point Details	
Egress/Outgoing Code point	Displays the CoS values and aliases that a specific rewrite rule has set for a specific forwarding class and loss priority.
Forwarding class name	Displays the forwarding classes associated with a specific rewrite rule.
Loss priority	Displays the loss priority values associated with a specific rewrite rule.

Table 161: Add Rewrite Rule Configuration Details

Field	Function	Action
Rewrite rule name	Displays the name of a defined rewrite rule.	

Table 161: Add Rewrite Rule Configuration Details (continued)

Field	Function	Action
Rewrite rule type	Specifies a rewrite rule type.	<p>Select a rewrite rule type from the list.</p> <p>The following rule types are supported for J6350 and all SRX Series devices:</p> <ul style="list-style-type: none"> • dscp—Defines the Differentiated Services code point rewrite rule. • ieee-802.1—Defines the IEEE-802.1 rewrite rule. • inet-precedence—Defines the precedence rewrite rule for IPv4. • exp—Defines the MPLS EXP rewrite rule (not supported for SRX3400, SRX3600, SRX5600, and SRX5800 devices). • dscp-ipv6—Defines the Differentiated Services code point rewrite rule for IPv6. • ieee-802.1ad—Defines the IEEE-802.1ad rewrite rule. • frame-relay-de—Defines the frame relay discard eligible bit rewrite rule (not supported for SRX3400, SRX3600, SRX5600, and SRX5800 devices).
Code point mapping	Specifies the code point mapping created.	<p>Click one:</p> <ul style="list-style-type: none"> • Add or +—Adds a code point mapping. • Edit or /—Edits the selected code point mapping. • Delete or X—Deletes a record.
Code point	Specifies the CoS value in bits and the alias of a classifier.	Select a CoS value and alias from the list.
Forwarding class	Specifies that it assigns the forwarding class to the rewrite rule.	Select the forwarding class of the rewrite rule from the list.
Loss priority	Specifies that it assigns a loss priority to the specified rewrite rule.	Select the loss priority of the rewrite rule from the list.

- See Also**
- [Schedulers Configuration Page Options on page 272](#)
 - [Classifiers Configuration Page Options on page 267](#)
 - [Forwarding Classes Configuration Page Options on page 266](#)

Schedulers Configuration Page Options

1. Select **Configure>Class of Service>Schedulers** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Configure>Network>Class of Service>Schedulers** in the J-Web user interface.

The Configure Schedulers configuration page appears. [Table 163 on page 272](#) explains the contents of this page.

2. Click one:
 - **Global Setting**—Enable or disable non-strict priority to all the schedulers globally. Enter information as specified in [Table 162 on page 272](#).
 - **Add or +**—Adds a new or duplicate configuration of schedulers. Enter information as specified in [Table 164 on page 273](#).
 - **Edit or /**—Edits the configuration of selected schedulers.
 - **Delete or X**—Deletes the configuration of selected schedulers.
3. Click one:
 - **OK**—Saves the configuration and returns to the main configuration page.
 - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
 - **Cancel**—Cancels your entries and returns to the main configuration page.

Table 162: Schedulers Global Setting

Field	Function
Enable Non Strict Priority	Applies non-strict priority policy to all the schedulers.

Table 163: Schedulers Configuration Page

Field	Function
Scheduler name	Displays the names of defined schedulers.
Scheduler priority	Displays the scheduler transmission priority, which determines the order in which an output interface transmits traffic from the queues.
Details of scheduler	
Name	Displays the scheduler name.
Value	Displays the CoS value.

Table 164: Add Schedulers Configuration Details

Field	Function	Action
Scheduler name	Specifies the name of a scheduler.	Enter the scheduler name.
Scheduler priority	Specifies scheduler transmission priority, which determines the order in which an output interface transmits traffic from the queues.	<p>Select the scheduler priority from the list.</p> <ul style="list-style-type: none"> • high—Packets in this queue have high priority. • low—Packets in this queue are transmitted last. • medium-low—Packets in this queue have medium-low priority. • medium-high—Packets in this queue have medium-high priority. • strict-high—Packets in this queue are transmitted first.
Buffer size	Specifies the size of the delay buffer.	<p>Select one of the options from the list.</p> <ul style="list-style-type: none"> • exact—Exact buffer size. • percent—Percentage of the total buffer. Select and type an integer from 1 through 100. • remainder—Remaining available buffer size. • temporal—Temporal value in microseconds.
Shaping rate	Specifies the minimum bandwidth allocated to a queue.	<p>Select one of the options from the list.</p> <ul style="list-style-type: none"> • rate—Shaping rate as an absolute number of bits per second. Select and type an integer from 3200 through 160,000,000,000 bits per second. • percent—Shaping rate as a percentage. Select and type an integer from 0 through 100.
Transmit rate	Specifies the transmission rate of a scheduler.	<p>Select one of the options from the list.</p> <ul style="list-style-type: none"> • rate—Transmit rate. Select and type an integer from 3200 through 160,000,000,000 bits per second. • exact—Exact transmit rate. • percent—Percentage of transmission capacity. Select and type an integer from 1 through 100. • remainder—Remaining transmission capacity.

See Also • [Scheduler Maps Configuration Page Options on page 274](#)

- [Rewrite Rules Configuration Page Options on page 270](#)
- [Classifiers Configuration Page Options on page 267](#)

Scheduler Maps Configuration Page Options

1. Select **Configure>Class of Service>Scheduler Maps** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platform.
Or
Select **Configure>Network>Class of Service>Scheduler Maps** in the J-Web user interface.
The Configure Schedulers maps configuration page appears. [Table 165 on page 274](#) explains the contents of this page.
2. Click one:
 - **Add** or **+**—Adds a new or duplicate schedulers maps configuration. Enter information as specified in [Table 166 on page 274](#).
 - **Edit** or **/**—Edits the selected schedulers maps configuration.
 - **Delete** or **X**—Deletes the selected schedulers maps configuration.
3. Click one:
 - **OK**—Saves the configuration and returns to the main configuration page.
 - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
 - **Cancel**—Cancels your entries and returns to the main configuration page.

Table 165: Schedulers Maps Configuration Page

Field	Function
Scheduler map name	Displays the names of defined scheduler maps. Scheduler maps link schedulers to forwarding classes.
Schedulers	Displays the schedulers assigned for each map.
Forwarding classes	Displays the forwarding classes assigned for each map.
Details of Schedulers	
Name	Displays the scheduler assigned to the selected scheduler map.
Value	Displays the CoS values.

Table 166: Add Schedulers Maps Configuration Details

Field	Function	Action
Scheduler map name	Specifies the name of a scheduler map.	Enter a name for the scheduler map.

Table 166: Add Schedulers Maps Configuration Details (continued)

Field	Function	Action
best-effort	Specifies no service profile. Loss priority is typically not carried in a CoS value.	Select an option from the list.
expedited-forwarding	Specifies end-to-end service with low loss, low latency, low jitter, and assured bandwidth.	Select an option from the list.
assured-forwarding	Specifies the group of defined values.	Select an option from the list.
network-control	Specifies CoS packet forwarding class of high priority.	Select an option from the list.

- See Also**
- [Drop Profile Configuration Page Options on page 275](#)
 - [Schedulers Configuration Page Options on page 272](#)
 - [Rewrite Rules Configuration Page Options on page 270](#)

Drop Profile Configuration Page Options

1. Select **Configure>Class of Service>Drop Profile** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Configure>Network>Class of Service>Drop Profile** in the J-Web user interface.

The Red Drop Profiles configuration page appears. [Table 167 on page 276](#) explains the contents of this page.
2. Click one:
 - **Add** or **+**—Adds a new or duplicate drop profile configuration. Enter information as specified in [Table 168 on page 276](#).
 - **Edit** or **/**—Edits the selected drop profile configuration.
 - **Delete** or **X**—Deletes the selected drop profile configuration.
3. Click one:
 - **OK**—Saves the configuration and returns to the main configuration page.
 - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
 - **Cancel**—Cancels your entries and returns to the main configuration page.

Table 167: Drop Profile Configuration Page

Field	Function
Drop profile name	Displays the configured random early detection (RED) drop profile names.
Profile type	Displays whether a RED drop profile type is interpolated or segmented.
Data points	Displays information about the data point types.

Table 168: Add Drop Profile Configuration Details

Field	Function	Action
Drop Profile Name	Specifies a name for a drop profile.	Enter a drop profile name.
Interpolated	Specifies whether the value pairs are interpolated to produce a smooth profile.	Select Interpolated .
Segmented	Specifies whether the value pairs are represented by line fragments, which connect each data point on the graph to produce a segmented profile.	Select Segmented .
Add Data Point	Specifies the data point created. The options available are: <ul style="list-style-type: none"> • Add—Adds a data point. • Edit—Edits the selected data point. • Delete—Deletes a record. 	Select an option.
Fill Level	Specifies the percentage value of queue buffer fullness for the X-coordinate.	Enter a percentage value for fill level, for example, 95.
Drop Probability	Specifies the percentage value of drop probability for the Y-coordinate.	Enter a percentage value for drop probability, for example, 85.

- See Also**
- [Virtual Channel Groups Configuration Page Options on page 276](#)
 - [Scheduler Maps Configuration Page Options on page 274](#)
 - [Schedulers Configuration Page Options on page 272](#)

Virtual Channel Groups Configuration Page Options

1. Select **Configure>Class of Service>Virtual Channel Groups** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Configure>Network>Class of Service>Virtual Channel Groups** in the J-Web user interface.

The Virtual Channel Group Information configuration page appears.

[Table 169 on page 277](#) explains the contents of this page.

2. Click one:

- **Add**—Adds a new or duplicate virtual group channel configuration. Enter information as specified in [Table 170 on page 277](#).
- **Edit**—Edits the selected virtual group channel configuration.
- **Delete**—Deletes the selected virtual group channel configuration.

3. Click one:

- **OK**—Saves the configuration and returns to the main configuration page.
- **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
- **Cancel**—Cancels your entries and returns to the main configuration page.

Table 169: Virtual Channel Group Information Configuration Page

Field	Function
Virtual Channel Group Name	Displays the name of defined virtual channel groups.
Virtual Channel Name	Displays the name of defined virtual channels.
Default	Displays the default virtual channel of a group marking.
Scheduler Map	Displays the scheduler map assigned to a particular virtual channel.
Shaping Rate	Displays the shaping rate configured for a virtual channel.

Table 170: Add Virtual Channel Group Information Configuration Details

Field	Function	Action
Virtual Channel Name	Specifies the name of a virtual channel to be assigned to a virtual channel group.	Select a predefined name from the list or enter a new virtual channel name.
Scheduler Map	Specifies a predefined scheduler map to assign to a virtual channel. Scheduler maps associate schedulers with forwarding classes.	Select a scheduler map from the list.
Unconfigured	Specifies no shaping rate.	Select the option.

Table 170: Add Virtual Channel Group Information Configuration Details (continued)

Field	Function	Action
Shaping Rate	<p>Specifies the shaping rate for a virtual channel.</p> <p>Configuring a shaping rate is optional. If no shaping rate is configured, a virtual channel without a shaper can use the full logical interface bandwidth. The options available are:</p> <ul style="list-style-type: none"> • Absolute Rate—Configures a shaping rate as an absolute number of bits per second. The range is 3200 through 320000000000. • Percent—Configures a shaping rate as a percentage. The range is 0 through 100. 	Select an option.

- See Also**
- [Assign To Interface Configuration Page Options on page 278](#)
 - [Drop Profile Configuration Page Options on page 275](#)
 - [Scheduler Maps Configuration Page Options on page 274](#)

Assign To Interface Configuration Page Options

1. Select **Configure>Class of Service>Assign To Interface** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.
 Or
 Select **Configure>Network>Class of Service>Assign To Interface** in the J-Web user interface.
 The Configure Interface Association configuration page appears. [Table 171 on page 279](#) explains the contents of this page.
2. Click the following:
 - **Edit** or **/**—Edits the selected interface. Edit information as specified in [Table 172 on page 279](#).
3. Click one:
 - **Add** or **+**—Adds a new or duplicate assign to interface configuration. Enter information as specified in [Table 173 on page 279](#).
 - **Edit** or **/**—Edits the selected assign to interface configuration.
 - **Delete** or **X**—Deletes the selected assign to interface configuration.
4. Click one:
 - **OK**—Saves the configuration and returns to the main configuration page.

- **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
- **Cancel**—Cancels your entries and returns to the main configuration page.

Table 171: Assign To Interface Configuration Page

Field	Function
Port	Displays the port and interface name.
Scheduler map	Displays the predefined scheduler maps for the physical interface.
Details of Logical Interfaces	
Unit	Displays the name of a logical interface.
Forwarding class	Displays the forwarding classes assigned to a particular interface.
Scheduler map	Displays the scheduler maps assigned to a particular interface.
Virtual channel group	Displays the virtual channel groups assigned to a particular interface.
Classifier[dscp,dscp6,exp,inet]	Displays the classifiers assigned to a particular interface—for example, information about DSCP and DSCPv6, EXP, and IPv4 (inet precedence) classifiers.
Rewrite rule[dscp,dscp6,exp,inet]	Displays the rewrite rules assigned to a particular interface—for example, information about Differentiated Services Code Point (DSCP and DSCPv6), EXP, and IPv4 (inet precedence) rewrite rules.

Table 172: Edit Interface Page

Field	Function	Action
Interface Name	Displays the selected interface name.	None.
Associate system default scheduler map	Specifies that you can associate the system default scheduler map with the selected interface.	Select Associate system default scheduler map .
Select the scheduler map	Specifies the scheduler map to the selected interface.	Select Select the scheduler map and select a value from the list.

Table 173: Add Assign To Interface Configuration Details

Field	Function	Action
Unit	Specifies the name of a logical interface.	Enter a logical interface name.
Scheduler map	Specifies a predefined scheduler map for this interface.	Select a scheduler map from the list.

Table 173: Add Assign To Interface Configuration Details (continued)

Field	Function	Action
Forwarding class	Assigns a predefined forwarding class to incoming packets on a logical interface.	Select a forwarding class from the list.
Virtual channel group	Applies a virtual channel group to a logical interface.	Select a virtual channel group from the list.
Classifiers		
dscp	Specifies the Differentiated Services Code Point of the classifier type assigned to a particular interface.	Select a classifier DSCP value from the list.
dscp v6	Specifies the Differentiated Services Code Point version 6 of the classifier type assigned to a particular interface.	Select a classifier DSCPv6 value from the list.
exp	Specifies the EXP classifier type assigned to a particular interface.	Select an EXP classifier value from the list.
inet precedence	Specifies the IPv4 precedence classifier type assigned to a particular interface.	Select an IPv4 precedence classifier value from the list.
Rewrite rules		
dscp	Specifies the Differentiated Services Code Point of the rewrite rule type assigned to a particular interface.	Select a rewrite rule DSCP value from the list.
dscp v6	Specifies the Differentiated Services Code Point version 6 of the rewrite rule type assigned to a particular interface.	Select a rewrite rule DSCPv6 value from the list.
exp	Specifies the EXP rewrite rule type assigned to a particular interface.	Select an EXP rewrite rule value from the list.
inet precedence	Specifies the IPv4 precedence rewrite rule type assigned to a particular interface.	Select an IPv4 precedence rewrite rule value from the list.

- See Also**
- [Virtual Channel Groups Configuration Page Options on page 276](#)
 - [Scheduler Maps Configuration Page Options on page 274](#)
 - [Schedulers Configuration Page Options on page 272](#)

Forwarding Mode

- [Forwarding Configuration Page Options on page 280](#)

Forwarding Configuration Page Options

1. Select **Configure>Security>Forwarding** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Configure>Network>Forwarding Mode** in the J-Web user interface.

The Forwarding configuration page appears. [Table 174 on page 281](#) explains the contents of this page.



NOTE: Starting in Junos OS Release 19.2R1, flow mode is the default mode for processing traffic. You can now configure an SRX Series devices as a border router by changing the flow-based processing to packet-based processing.

2. Click one:

- **OK**—Saves the configuration and returns to the main configuration page.
- **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
- **Reset**—Resets your entries and returns to the main configuration page.

3. (Junos OS Release 19.2R1 and later) Click one:

- **Save**—Saves the configuration.
- **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
- **Cancel**—Cancels the configuration made.

Table 174: Forwarding Configuration Options

Field	Function	Action
Forwarding Options		
Family IPv6	<p>Supports IPv6 protocol traffic, including Routing Information Protocol for IPv6 (RIPng).</p> <p>The available options are:</p> <ul style="list-style-type: none"> • None • drop—Drop IPv6 packets. • flow-based—Perform flow-based packet forwarding. • packet-based—Perform simple packet forwarding. <p>NOTE: For SRX5000 line of devices, only drop and flow based options are available.</p>	Select an option from the list.
Family ISO	<p>Supports IS-IS traffic.</p> <p>The available options are:</p> <ul style="list-style-type: none"> • None • packet-based 	Select an option from the list.
<p>NOTE: This option is not available for SRX5000 line of devices.</p>		

Table 174: Forwarding Configuration Options (continued)

Field	Function	Action
Family MPLS	Supports MPLS traffic.	Select an option from the list.
NOTE: This option is not available for SRX5000 line of devices.	The available options are: <ul style="list-style-type: none"> • None • flow-based • packet-based 	

- See Also**
- [Signature Update Configuration Page Options on page 373](#)
 - [ALG Configuration Page Options on page 429](#)

Security

- [Security Policy on page 282](#)
- [NAT on page 301](#)
- [Objects on page 313](#)
- [Security Objects on page 330](#)
- [AppSecure on page 332](#)
- [UTM on page 336](#)
- [IPS on page 373](#)
- [skyATP or Threat Prevention on page 386](#)
- [IPSec VPN on page 386](#)
- [User Firewall on page 409](#)
- [SSL Profiles on page 419](#)
- [ALG on page 429](#)
- [Firewall Filters on page 437](#)
- [ICAP Redirect on page 462](#)
- [DS-Lite on page 465](#)

Security Policy

- [Configuring Firewall Security Policy Rules on page 282](#)
- [Configuring Firewall Policy Schedules on page 299](#)

Configuring Firewall Security Policy Rules

1. Select **Configure>Security Services>Security Policy>Rules**.

The Rules configuration page appears displaying all the rules based on grouping of rules as zone pairs or zone contexts. Each row displays the from and to zones (zone

pairs) and the number of rules present in that zone pair. [Table 175 on page 283](#) explains the contents of this page.

2. Click one:

- **Global Options**—Configures global options for the firewall security policy. Enter information as specified in [Table 176 on page 284](#).
- **Add icon (+)**—Adds a new firewall or global security policy configuration. Enter information as specified in [Table 177 on page 287](#).
- **Edit icon (/)**—Edits the selected firewall policy configuration. Enter information as specified in [Table 177 on page 287](#).
- **Delete icon (X)**—Deletes the selected firewall security policy configuration.
- **Save**—Saves the rule that you edited or cloned. This is enabled if you edit or clone a rule.
- **Discard**—Discards the rule that you selected from the grid.
- **More**—Enables you to add rule before or after, copy, cut, paste, clone a rule, and so on. For more information see [Table 178 on page 298](#).
- **Search icon**—Enables you to search a firewall policy or rule from the grid.
- **Show Hide Column Filter icon**—Enables you to show or hide a column in the grid.

3. Click Commit icon at the top of the J-Web page. The following commit options are displayed.

- **Commit**—Commits the configuration and returns to the main configuration page.
- **Compare**—Enables you to compare the current configuration with the previous configuration.
- **Discard**—Discards the configuration changes you performed in the J-Web.
- **Preferences**—There are two tab:

Commit preferences—You can choose to just validate or validate and commit the changes.

Startup page upon login—You can choose what page should be displayed as soon as you login to J-Web. The options are: Configuration, Monitoring, Dashboard, and Last accessed.

Table 175: Rules Configuration Page

Field	Function
Seq.	Displays the sequence number of rules in a zone pair.
Hit Count	Displays the number of hits the rule has encountered.
Rule Name	Displays the rule name.

Table 175: Rules Configuration Page (continued)

Field	Function
Source Zone	Displays the source zone that is specified in the zone pair for the rule.
Source Address	Displays the name of the source address or address set for the rule.
Source Identity	Displays the user identity of the rule.
Destination Zone	Displays the destination zone that is specified in the zone pair for the rule.
Destination Address	Displays the name of the destination address or address set for the rule.
Dynamic Application	<p>Displays the dynamic application names for match criteria in application firewall rule set.</p> <p>An application firewall configuration permits, rejects, or denies traffic based on the application of the traffic.</p>
Service	Displays the type of service for the destination of the rule.
URL Category	Displays the URL category that you want to match criteria for web filtering category.
Action	Displays the actions that need to take place on the traffic as it passes through the firewall.
Rule Options	Displays the rule option while permitting the traffic.
Advanced Security	Displays the security option that apply for this rule.
Description	Displays the description of the rule.

Table 176: Global Options Firewall Policy Configuration Details

Field	Function	Action
Policy Options		
Default policy action	<p>Specifies that specific protocol actions are overridden. This action is also nonterminating. The options available are:</p> <ul style="list-style-type: none"> • permit-all • deny-all 	Select a value from the list.

Table 176: Global Options Firewall Policy Configuration Details (continued)

Field	Function	Action
Policy rematch	Specifies that a policy is added that has just been modified to a deferred action list for reevaluation. For every session associated with the policy, the device reevaluates the policy lookup. If the policy is different from the one associated with the session, the device drops the session. If the policy matches, the session continues.	Select the check box.
Flow - Main		
Early ageout	Specifies the amount of time before the device aggressively ages out a session from its session table.	Enter a value from 1 through 65,535 seconds. The default value is 20 seconds.
High watermark	Specifies the percentage of session table capacity at which the aggressive aging-out process begins.	Enter a value from 0 through 100 percent. The default value is 100 percent.
Low watermark	Specifies the percentage of session table capacity at which the aggressive aging-out process ends.	Enter a value from 0 through 100 percent. The default value is 100 percent.
Enable SYN cookie protection	Enables SYN cookie defenses against SYN attacks.	Select the check box.
Enable SYN proxy protection	Enables SYN proxy defenses against SYN attacks.	Select the check box.
Allow DNS reply	Specifies that an incoming DNS reply packet without a matched request is allowed.	Select the check box.
Force IP reassembly	Specifies reassemble all IP fragmented packets before forwarding.	
Enable Routing Mode	Enables routing mode on uPIM and ePIM ports that correspond to the interfaces that will carry the VPLS traffic.	
Route change to nonexistent route timeout	Specifies the session timeout value on a route change to a nonexistent route.	Enter a value from 6 through 1800 seconds.
Flow - TCP MSS		
Enable MSS override for all packets	Enables maximum segment size override for all TCP packets for network traffic.	Select the check box. Enter an maximum segment size value from 64 through 65,535.
Enable MSS override for all GRE packets coming out of an IPsec tunnel	Enables maximum segment size override for all generic routing encapsulation packets exiting an IPsec tunnel.	Select the check box. Enter a maximum segment size value from 64 through 65,535 bytes. The default value is 1320 bytes.

Table 176: Global Options Firewall Policy Configuration Details (continued)

Field	Function	Action
Enable MSS override for all GRE packets entering an IPsec tunnel	Enables maximum segment size override for all generic routing encapsulation packets entering an IPsec tunnel.	Select the check box. Enter a maximum segment size value from 64 through 65,535 bytes. The default value is 1320 bytes.
Enable MSS override for all packets entering IPsec tunnel	Enables maximum segment size override for all packets entering an IPsec tunnel.	Select the check box. Enter a maximum segment size value from 64 through 65,535 bytes. The default value is 1320 bytes.
Flow - TCP Session		
Disable sequence-number checking	Disables checking of sequence numbers in TCP segments during stateful inspections. By default, the device monitors the sequence numbers in TCP segments.	Select the check box.
Strict SYN-flag check	Enables the strict three-way handshake check for the TCP session. This check enhances security by dropping data packets before the three-way handshake is done. By default, this check is disabled.	Select the check box.
Disable SYN-flag check	Disables the checking of the TCP SYN bit before creating a session. By default, the device checks that the SYN bit is set in the first packet of a session. If it is not set, the device drops the packet.	Select the check box.
Disable SYN-flag check (tunnel packets)	Disables the first packet check for the SYN flag when forming a TCP flow session.	Select the check box.
RST invalidate session	Specifies that a session is marked for immediate termination when it receives a TCP RST segment. By default, this statement is unset. When unset, the device applies the normal session timeout interval—for TCP, session timeout is 30 minutes; for HTTP, it is 5 minutes; and for UDP, it is 1 minute.	Select the check box.
RST sequence check	Specifies that the TCP sequence number in a TCP segment can be checked, with the RST bit enabled. This matches the previous sequence number for a packet in that session or is the next higher number incrementally.	Select the check box.
TCP Initial Timeout	Specifies the length of time (in seconds) that the device keeps an initial TCP session in the session table before dropping it, or until the device receives a FIN or RST packet.	Select the check box.

Table 177: Add Firewall Policy Rule Configuration Details

Field	Function	Action
General		
Rule Name	Specifies the name of the security policy.	Enter a name for the new rule or policy.
Rule Description	Specifies a description for the security policy.	Enter a description for the security policy.
Global Policy	Specifies that the policy defined is a global policy and zones are not required.	
Source		
Zone	Specifies the source zone.	Identify and select the source zone to which you want the rule to be associated with from the dropdown menu.
Address(es)	Specifies the source address of the rule.	<p>Select the Address(es) for the policy by clicking Select. The Source Address page appears.</p> <p>Select the Address for this policy. The options available are:</p> <ul style="list-style-type: none"> • Include Any Address—Selecting this will include any address as the source address. • Include Specific—Selects an address book entry from the available list or you can make a new address book entry by selecting Add New Source Address and creating a new source address in the Create Address page. • Exclude Specific—Selects an address book entry from the available list or you can make a new address book entry by selecting Add New Source Address and creating a new source address in the Create Address page.
Identity	Select the user identity that you want to permit or deny in the rule.	<p>Select the user identity to permit or deny.</p> <p>Click Select to choose a user identity from the available list or you can make a new user identity by selecting Add New Identity and creating a new user name or identity in the Create Identity page.</p> <p>NOTE: Starting in Junos OS Release 19.1R1, list of local authentication users are available in the source identity list for logical system and tenant users.</p>

Table 177: Add Firewall Policy Rule Configuration Details (continued)

Field	Function	Action
Destination		
Zone	Specifies the destination zone.	Identify and select the destination zone to which you want the rule to be associated with from the dropdown menu.
Address(es)	Specifies the source address of the rule.	<p>Select the Address(es) for the policy by clicking Select. The Destination Address page appears.</p> <p>Select the Address for this policy. The options available are:</p> <ul style="list-style-type: none"> • Include Any Address—Selecting this will include any address as the destination address. • Include Specific—Selects an address book entry from the available list or you can make a new address book entry by selecting Add New Source Address and creating a new source address in the Create Address page. • Exclude Specific—Selects an address book entry from the available list or you can make a new address book entry by selecting Add New Source Address and creating a new source address in the Create Address page.

Table 177: Add Firewall Policy Rule Configuration Details (continued)

Field	Function	Action
Dynamic Application	Select the dynamic application names for match criteria in application firewall rule set.	

Table 177: Add Firewall Policy Rule Configuration Details (continued)

Field	Function	Action
		<p>Select the application from the Available list and move it to Selected list.</p> <p>Starting in Junos OS Release 19.2R1, you can add an application or application group for a dynamic application using the Add New Application or Add New Application Group button.</p> <ol style="list-style-type: none"> Click Select to select a dynamic application. Enter the following details in the Dynamic Application page: The Dynamic Application page appears. Application/Group—Select an option from the list. To add a new application: <ol style="list-style-type: none"> Select Application from the list. Click Add New Application. The Create Application Signature page appears. Follow the steps mentioned in the <i>Application Signature Configuration Page Options</i> section to create application signature. Click OK. The Dynamic Application page appears. To add a new application group: <ol style="list-style-type: none"> Select Group from the list. Click Add New Application Group. The Create Application Signature Group page appears. Enter name of the application group in the Name field. Select the group members or click + to add application signatures to the group member. Click OK. The Dynamic Application page appears. <p>NOTE: After adding an application or group, it should be auto-selected in Dynamic Application. The values None or any should be moved to</p>

Table 177: Add Firewall Policy Rule Configuration Details (continued)

Field	Function	Action
		available list. By default, None value is auto-populated when the Selected list is empty.
		3. Predefined/Custom—Select an option from the list: Predefined, Custom, or All.
		4. Category—Select an option from the list.
		5. Dynamic Application—Select the application from the Available list and move it to Selected list.
		6. Click OK .

Table 177: Add Firewall Policy Rule Configuration Details (continued)

Field	Function	Action
Service(s)	Select the services that you want to permit or deny in the rule.	<p>Click Select to select the services to permit or deny. You can choose a service from the available list.</p> <p>Starting in Junos OS Release 19.2R1, you can add a new service using the Add New Service button.</p> <p>To add a new service:</p> <ol style="list-style-type: none"> 1. Click Add New Service on the Service page. The Create Service page appears. 2. Enter the following details for global settings: <ul style="list-style-type: none"> • Name—Enter a unique name for application. • Description—Enter description of application. • Application Protocol—Select an option from the list for application protocol. • Match IP protocol—Select an option from the list to match IP protocol. • Source Port—Select an option from the list for source port. • Destination Port—Select an option from the list for destination port. • ICMP Type—Select an option from the list for ICMP message type. • ICMP Code—Select an option from the list for ICMP message code. • RPC program numbers—Enter a value for RPC program numbers. <p>NOTE: The format of the value must be W or X-Y. Where, W, X, and Y are integers between 0 and 65535.</p>

Table 177: Add Firewall Policy Rule Configuration Details (continued)

Field	Function	Action
		<ul style="list-style-type: none"> Inactivity Timeout—Select an option from the list for application specific inactivity timeout. UUID—Enter a value for DCE RPC objects. <p>NOTE: The format of the value must be 12345678-1234-1234-1234-123456789012</p>
		<p>3. Enter the following details for terms if you want to define individual application protocols:</p> <ol style="list-style-type: none"> Click + to create a term. Name—Enter the name for term. ALG—Select an option from the list for ALG. Match IP protocol—Select an option from the list to match IP protocol. Source Port—Select an option from the list for source port. Destination Port—Select an option from the list for destination port. ICMP Type—Select an option from the list for ICMP message type. ICMP Code—Select an option from the list for ICMP message code. RPC program numbers—Enter a value for RPC program numbers. <p>NOTE: The format of the value must be W or X-Y. Where, W, X, and Y are integers between 0 and 65535.</p> <ol style="list-style-type: none"> Inactivity Timeout—Select an option from the list for application specific inactivity timeout. UUID—Enter a value for DCE RPC objects. <p>NOTE: The format of the value must be 12345678-1234-1234-1234-123456789012</p>
		<p>4. Click Create to create a service.</p>

Table 177: Add Firewall Policy Rule Configuration Details (continued)

Field	Function	Action
		5. Click OK . NOTE: After adding a service, it should be auto-selected in Service(s). The values None or any should be moved to available list.
URL Category	Select the URL category that you want to match criteria for web filtering category.	Select the URL category by clicking Select . URL Category page appears. <ul style="list-style-type: none">• Predefined/Custom—Select an option from the list: Predefined, Custom, or All.• URL Category—Select an option from the list.

Advanced Security

Table 177: Add Firewall Policy Rule Configuration Details (continued)

Field	Function	Action
Rule Action	Specifies the action taken when traffic matches the criteria. Available options are: <ul style="list-style-type: none">• Permit• Deny• Reject	

Table 177: Add Firewall Policy Rule Configuration Details (continued)

Field	Function	Action
		<p>Select an option.</p> <p>Permit—Allow packet to pass through the firewall. It enables the following Permit options:</p> <ol style="list-style-type: none"> 1. App Firewall—Select the application firewall from the list. 2. IPS—Select Off or On from the list. If you select On, the IPS Policy field will be disabled. If you select Off, you may select the IPS Policy from the list. 3. UTM—Select the UTM policy to associate with this rule from the list, which shows all the UTM policies available. If you want to create a new UTM policy, click Add New, which enables you to create a new UTM policy in the Create UTM Policies Wizard. To know more about this wizard refer Configure>Security>UTM page in J-Web. 4. SSL Proxy—Select the SSL proxy policy to associate with this rule from the list, which shows all the SSL proxy profiles that are created using the Configure>Security>SSL Proxy page in J-Web. After you associate, the SSL proxy policy will be applied to the traffic. 5. IPsec VPN—Select the IPsec VPN tunnel from the list. 6. Pair Policy Name—Select the name of the policy with the same IPsec VPN in the opposite direction to create a pair policy. 7. Threat Prevention Policy—Select the configured threat prevention policy from the list. To create a threat prevention policy go to Configure>Security>SkyATP or Threat Prevention>Policies.

Table 177: Add Firewall Policy Rule Configuration Details (continued)

Field	Function	Action
		<p>8. ICAP Redirect Profile—Select the configured ICAP Redirect profile name from the list.</p> <p>Deny—Block and drop the packet, but do not send notification back to the source.</p> <p>Reject—Block and drop the packet and send a notice to the source host.</p> <ul style="list-style-type: none"> For TCP traffic—Sends TCP RST. For UDP traffic—Sends ICMP destination unreachable, port unreachable message (type 3, code 3). For TCP and UDP traffic—Specifies action denied.
Rule Options		
Logging/Count		
Log at Session Close Time	Specifies that an event is logged when the session closes.	Select the check box.
Log at Session Init Time	Specifies that an event is logged when the session is created.	Select the check box.
Enable Count	Specifies statistical counts and triggers alarms whenever traffic exceeds specified packet and byte thresholds. When this count is enabled, statistics are collected for the number of packets, bytes, and sessions that pass through the firewall with this policy.	Select the check box. NOTE: Alarm threshold fields are disabled if Enable Count is not enabled.
Authentication		
Push Auth Entry to JIMS	Pushes authentication entries from firewall authentication, that are in auth-success state, to Juniper Identity Management Server (JIMS). This will enable the SRX device to query JIMS to get IP/user mapping and device information.	Select the check box.
Type	Specify the type of firewall authentication for this rule.	Select the type of firewall authentication from the list. The options available are: None, Pass-through, User-firewall, and Web-authentication.
Advanced Settings		

Table 177: Add Firewall Policy Rule Configuration Details (continued)

Field	Function	Action
Destination Address Translation	Specifies the action to be taken on a destination address translation.	Select the action to be taken on a destination address translation. The options available are: None, Drop Translated, Drop Untranslated.
Redirect Options	Specifies the action to be taken if redirect is needed.	Select the action to redirect. The options available are: None, Redirect Wx, and Reverse Redirect Wx.
Enable TCP-SYN	Disables or enables the checking of the TCP SYN bit before creating a session. By default, the device checks that the SYN bit is set in the first packet of a session. If it is not set, the device drops the packet.	Select if you want enable TCP-SYN.
Log TCP Sequence	Disables or enables checking of sequence numbers in TCP segments during stateful inspections. By default, the device monitors the sequence numbers in TCP segments.	Select if you want to log TCP sequencing.

Table 178: More options on Rules

Field	Function
Add Rule Before	Adds a new rule before the selected rule.
Add Rule After	Adds a new rule after the selected rule.
Copy	Copies a selected rule and enables you to paste it before or after the selected rule.
Cut	Removes the selected rule from its row and enables you to paste it before or after the selected rule.
Paste	Pastes the copied or cut rule before or after the rule selected for copy.
Clone	Clones or copies the selected firewall policy configuration and enables you to update the details of the rule.
Move Rule	Organizes records. Select a rule and choose Move up , Move down , Move to top , or Move to bottom to reposition the rule.
Disable	Disables the selected rule.
Enable	Enables the selected rule if it was disabled.
Clear Selection	Clears the selection of those rules that are selected.

- See Also**
- [Zones and Screens Configuration Page Options on page 313](#)
 - [UTM Policies Configuration Page Options on page 371](#)
 - [IDP Policies Configuration Page Options on page 381](#)
 - *Chassis Configuration Page Options*

Configuring Firewall Policy Schedules

1. Select **Configure>Security>Firewall Policy>Schedules**.

The Scheduler Information configuration page appears. [Table 179 on page 299](#) explains the contents of this page.

2. Click one:

- **Add icon (+)**—Adds a new or duplicate scheduler configuration. Enter information as specified in [Table 180 on page 300](#).
- **Edit icon (/)**—Edits the selected scheduler configuration.
- **Delete(X)**—Deletes the selected scheduler configuration.
- **More**— Enables you to clone a schedule from the selected schedule, display a detailed view of the selected schedule, and clear all selections in the grid.
- **Search icon**—Enables you to search a schedule in the grid.
- **Show Hide Column Filter icon**—Enables you to show or hide a column in the grid.

3. Click Commit icon at the top of the J-Web page. The following commit options are displayed.

- **Commit**—Commits the configuration and returns to the main configuration page.
- **Compare**—Enables you to compare the current configuration with the previous configuration.
- **Discard**—Discards the configuration changes you performed in the J-Web.
- **Preferences**—There are two tab:

Commit preferences—You can choose to just validate or validate and commit the changes.

Startup page upon login—You can choose what page should be displayed as soon as you login to J-Web. The options are: Configuration, Monitoring, Dashboard, and Last accessed.

Table 179: Scheduler Configuration Page

Field	Function
Details icon in blue color	Displays the Schedules Details, on clicking the icon.
Name	Displays the name of the scheduler.

Table 179: Scheduler Configuration Page (continued)

Field	Function
Description	Displays a description of the scheduler.
Start Date	Displays the start date for the first day.
End Date	Displays the stop date for the first day.
Second Start Date	Displays the start date for the second day.
Second End Date	Displays the stop date for the second day.
Schedules	On expanding, displays the days of the schedule, exclusion days if any, and the start and end time of the schedule.

Table 180: Add Scheduler Configuration Details

Field	Function	Action
Name	Specifies the scheduler name.	Enter the name of the scheduler.
Description	Specifies a description for the scheduler.	Enter a description for the scheduler.
Start Date	Specifies the start date of the first day.	Select the start date for the first day from the calendar.
Stop Date	Specifies the stop date of the first day.	Select the stop date for the first day from the calendar.
Second Start Date	Specifies the start date of the second day.	Select the start date for the second day from the calendar.
Second End Date	Specifies the stop date of the second day.	Select the stop date for the second day from the calendar.

Time Ranges

Specify a day/time range to edit

Specify the same time for all days	Specifies the same time for all days	<p>Click Specify the same time for all days. The Apply Options for All Days page appears.</p> <p>Select the Time Options from All Day, Exclude Day, or Time Ranges.</p> <p>If you select Time Ranges enter the Start Time and End Time. You can also a Second Start Time and Second End Time by clicking Add Another Range.</p>
------------------------------------	--------------------------------------	--

Table 180: Add Scheduler Configuration Details (continued)

Field	Function	Action
Daily option	Specifies that you can set the scheduler to run at regular and recurring intervals.	<p>Select an day from the list. The Speicify Time for <selected day> appears.</p> <p>Select the Time Options from All Day, Exclude Day, or Time Ranges.</p> <p>If you select Time Ranges enter the Start Time and End Time. You can also a Second Start Time and Second End Time by clicking Add Another Range.</p>
Time Start1	Specifies the start time for the first day.	Enter the start time in HH:MM:SS format.
Time Stop1	Specifies the stop time for the first day.	Enter the stop time in HH:MM:SS format.
Time Start2	Specifies the start time for the second day.	Enter the start time in HH:MM:SS format.
Time Stop2	Specifies the stop time for the second day.	Enter the stop time in HH:MM:SS format.

- See Also**
- [Applications Configuration Page Options](#)
 - [IDP Policies Configuration Page Options on page 381](#)
 - [Address Book Configuration Page Options on page 326](#)

NAT

- [Source NAT Configuration Page Options on page 301](#)
- [Destination NAT Configuration Page Options on page 306](#)
- [Static NAT Configuration Page Options on page 309](#)
- [Proxy Configuration Page Options on page 311](#)

Source NAT Configuration Page Options

1. Select **Configure>NAT>Source NAT** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Configure>>Security>NAT>Source** in the J-Web user interface.

The Source NAT configuration page appears. [Table 181 on page 302](#) explains the contents of this page.

2. Click one:

- **Global Settings**—Defines general specifications for source NAT. Enter information as specified in [Table 182 on page 303](#).
 - **Add** or **+**—Adds a new or duplicate Source NAT configuration. Enter information as specified in [Table 183 on page 304](#).
 - **Edit** or **/**—Edits the selected source NAT configuration.
 - **Delete** or **X**—Deletes the selected source NAT configuration.
3. Click one:
- **OK**—Saves the configuration and returns to the main configuration page.
 - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
 - **Cancel**—Cancels your entries and returns to the main configuration page.

Table 181: Source NAT Configuration Page

Field	Function
Source NAT Rule Set	
From	Displays the source NAT sort options from which the packets flow. The options available are: <ul style="list-style-type: none"> • Routing Instance • Zone • Interface
To	Displays the source NAT sort options to which the packets flow. The options available are: <ul style="list-style-type: none"> • Routing Instance • Zone • Interface
Filter	Displays the filter option.
Name	Displays the name of the source NAT rule set.
From	Displays the name of the routing instance/zone/interface from which the packets flow.
To	Displays the name of the routing instance/zone/interface to which the packets flow.
Rule	Displays the name of the rule in the selected source NAT rule set.
Description	Displays a description of the source NAT rule set.
Rules in Selected Rule-Set	

Table 181: Source NAT Configuration Page (continued)

Field	Function
Rule Name	Displays the name of the rule in the selected source NAT rule set.
Match Source	Displays the match source address.
Match Destination	Displays the match destination address.
Match IP Protocol	Displays the match IP protocol.
Match Destination Port	Displays the match destination port.
Action	Displays the action of the rule.
Persistent	Displays the persistent NAT address in the source NAT pool
Description	Displays a description of the rule.
Source NAT Pool	
Name	Displays the name of the source NAT pool.
Address	Displays the IP address of the source NAT pool.
Port	Displays the port address of the source NAT pool.
Description	Displays a description of the source NAT pool.

Table 182: Source NAT Global Setting Configuration Page

Field	Function	
Global Settings		
Address Persistent	Provides source address to maintain same translation.	Select check box to the enable address persistence.
Interface Port-Overloading	Specifies interface port overloading for persistent NAT.	Select check box to the enable interface port-overloading.
Port randomization	Specifies source NAT port randomization.	Select check box to the enable port randomization.
Pool Utilization Alarm		
Clear Threshold	Specifies clear to clear the threshold for pool utilization.	The default option is 40-100.
Raise Threshold	Specifies raise to raise the threshold for pool utilization.	The default option is 50-100.

Table 183: Add Source NAT Configuration Details

Field	Function	Action
Add Rule Set		
Rule Set Name	Specifies the name of the rule set.	Enter the rule set name.
Rule Set Description	Specifies a description for the rule set.	Enter a description for the rule set.
From/To	Specifies the filter option. The options available are: <ul style="list-style-type: none"> • Routing Instance • Zone • Interface 	Select an option. Select the source routing instances/zones/interfaces in the Available column and the use the right arrow to move them to the Selected column. Select the destination routing instances/zones/interfaces in the Available column and the use the right arrow to move them to the Selected column.
Add Rule		
Rule Name	Specifies the name of the rule.	Enter the rule name.
Rule Description	Specifies a description for the rule.	Enter a description for the rule.
Match		
Source Address	Specifies the source IP address. The options available are: <ul style="list-style-type: none"> • Available—Specifies the available source addresses. • Selected—Specifies the selected source addresses. 	Search and select the source addresses in the Available column and the use the right arrow to move them to the Selected column. You can also enter a source address in the New text box in the Selected and click Add to add the source address to the lower pane of the Selected column.
Destination Address	Specifies the destination IP address. The options available are: <ul style="list-style-type: none"> • Available—Specifies the available destination addresses. • Selected—Specifies the selected destination addresses. 	Select the destination addresses in the Available column and the use the right arrow to move them to the Selected column. You can also enter a destination address in the New text box in the Selected column and click Add to add the destination address to the lower pane of the Selected column.
IP Protocol	Specifies the IP protocol.	Enter the protocol name in the New text box and click Add to add the protocol to the lower pane of the IP Protocol column.

Table 183: Add Source NAT Configuration Details (continued)

Field	Function	Action
Destination Port	Specifies the destination port options. The options available are: <ul style="list-style-type: none"> Any Port Port Range 	Select an option.
Action	Specifies the action to be taken. The options available are: <ul style="list-style-type: none"> No Source NAT Do Source NAT with Egress Interface Address Do Source NAT with Pool 	Select an option.
Persistent	Specifies the persistent NAT address in the source NAT pool.	Select the check box to enable the following fields: <ul style="list-style-type: none"> Permit—Select an option. Inactivity Timeout—Enter a value. Max Session Number—Enter a value.
Add Source NAT Pool		
Pool Name	Specifies the name of the source NAT pool.	Enter the source NAT pool name.
Pool Description	Specifies a description for the source NAT pool.	Enter a description for the source NAT pool.
Routing Instance	Specifies the routing instances available.	Select an option.
Pool Address Family	Specifies the source NAT pool address family.	Select an option.
Pool Addresses	Specifies the source NAT pool addresses.	Enter the address range in the Address/Range text boxes. Click Add to add the address range to the Addresses column.
Port Translation	Specifies the port translation options. The options available are: <ul style="list-style-type: none"> No Translation Translation with Default Port Range (1024–65535) Translation with Specified Port Range Translation with Port Overloading Factor 	Select an option.

See Also

- [Destination NAT Configuration Page Options on page 306](#)
- [Static NAT Configuration Page Options on page 309](#)

- [Proxy Configuration Page Options on page 311](#)

Destination NAT Configuration Page Options

1. Select **Configure>NAT>Destination NAT** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Configure>Security>NAT>Destination** in the J-Web user interface.

The Destination NAT configuration page appears. [Table 184 on page 306](#) explains the contents of this page.

2. Click one:
 - **Add** or **+**—Adds a new or duplicate destination NAT configuration. Enter information as specified in [Table 185 on page 307](#).
 - **Edit** or **/**—Edits the selected destination NAT configuration.
 - **Delete** or **X**—Deletes the selected destination NAT configuration.
3. Click one:
 - **OK**—Saves the configuration and returns to the main configuration page.
 - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
 - **Cancel**—Cancels your entries and returns to the main configuration page.

Table 184: Destination NAT Configuration Page

Field	Function
Destination NAT Rule Set	
From	<p>Displays the destination NAT sort options from which the packets flow.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Routing Instance • Zone • Interface
To	<p>Displays the destination NAT sort options to which the packets flow.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Routing Instance • Zone • Interface
Filter	Displays the filter option.
Name	Displays the name of the destination NAT rule set.

Table 184: Destination NAT Configuration Page (continued)

Field	Function
From	Displays the name of the routing instance/zone/interface from which the packets flow.
Rule	Displays the name of the rule in the selected destination NAT rule set.
Description	Displays a description of the destination NAT rule set.
Rules in Selected Rule-Set	
Rule Name	Displays the name of the rule in the selected destination NAT rule set.
Match Source	Displays the match source address.
Match Destination	Displays the match destination address.
Match IP Protocol	Displays the match IP protocol.
Match Destination Port	Displays the match destination port.
Action	Displays the action of the rule in the selected rule set.
Description	Displays a description of the rule in the selected destination NAT rule set.
Destination NAT Pool	
Name	Displays the name of the destination NAT pool.
Address	Displays the IP address of the destination NAT pool.
Port	Displays the port address of the destination NAT pool.
Description	Displays a description of the destination NAT pool.

Table 185: Add Destination NAT Rule Set Configuration Details

Field	Function	Action
Destination Rule Set		
Add Rule Set		
Rule Set Name	Specifies the name of the rule set.	Enter the rule set name.
Rule Set Description	Specifies a description for the rule set.	Enter a description for the rule set.

Table 185: Add Destination NAT Rule Set Configuration Details (continued)

Field	Function	Action
From	Specifies the filter options. The options available are: <ul style="list-style-type: none"> Routing Instance Zone Interface 	Select an option. Select the routing instances/zones/interfaces in the Available column and the use the right arrow to move them to the Selected column.
Add Rule		
Rule Name	Specifies the name of the rule.	Enter the rule name.
Rule Description	Specifies a description for the rule.	Enter a description for the rule.
Match		
Source Address	Specifies the source IP address. The options available are: <ul style="list-style-type: none"> Available—Specifies the available source addresses. Selected—Specifies the selected source addresses. 	Search and select the source addresses in the Available column and the use the right arrow to move them to the Selected column. You can also enter a source address in the New text box in the Selected column and click Add to add the source address to the lower pane of the Selected column.
Destination Address	Specifies the destination IP address.	Enter the destination IP address.
Port	Specifies the destination port number.	Enter the destination port number.
IP Protocol	Specifies the IP protocol for the destination NAT rule.	Enter the protocol name in the text box and click Add to add the protocol to the IP Protocol column.
Actions	Specifies the actions for the destination NAT pool. The options available are: <ul style="list-style-type: none"> No Destination NAT. Do Destination NAT With Pool. 	Select an option.
Do Destination NAT With Pool		
Add New Pool	Specifies the add option for the Do Destination NAT With Pool option.	Click Add New Pool .
Add Destination Pool		
Pool Name	Specifies the name of the destination pool.	Enter the destination pool name.
Pool Description	Specifies a description for the destination pool.	Enter a description for the destination pool.

Table 185: Add Destination NAT Rule Set Configuration Details (continued)

Field	Function	Action
Routing Instance	Specifies the routing instance available.	Select an option.
Pool Addresses and Port		
Address/Port	Specifies the destination pool address.	Enter the destination pool address.
Port	Specifies the destination pool port number.	Enter the destination pool port number.
Address Range	Specifies the destination pool address range.	Enter the destination pool address range.
Destination NAT Pool		
Add Destination Pool		
Pool Name	Specifies the name of the destination pool.	Enter the destination pool name.
Pool Description	Specifies a description for the destination pool.	Enter a description for the destination pool.
Routing Instance	Specifies the routing instance available.	Select an option.
Pool Addresses and Port		
Address/Port	Specifies the destination pool address.	Enter the destination pool address.
Port	Specifies the destination pool port number.	Enter the destination pool port number.
Address Range	Specifies the destination pool address range.	Enter the destination pool address range.

- See Also**
- [Source NAT Configuration Page Options on page 301](#)
 - [Static NAT Configuration Page Options on page 309](#)
 - [Proxy Configuration Page Options on page 311](#)

Static NAT Configuration Page Options

1. Select **Configure > NAT > Static NAT** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.
Or
Select **Configure > Security > NAT > Static** in the J-Web user interface.

The Static NAT configuration page appears. [Table 186 on page 310](#) explains the contents of this page.

2. Click one:

- **Add** or **+**—Adds a new or duplicate static NAT configuration. Enter information as specified in [Table 187 on page 311](#).
- **Edit** or **/**—Edits the selected static NAT configuration.
- **Delete** or **X**—Deletes the selected static NAT configuration.

3. Click one:

- **OK**—Saves the configuration and returns to the main configuration page.
- **Cancel**—Cancels your entries and returns to the main configuration page.

Table 186: Static NAT Configuration Page

Field	Function
Static NAT Rule Set	
From	Displays the destination NAT sort options from which the packets flow. The options available are: <ul style="list-style-type: none"> • Routing Instance • Zone • Interface
Filter	Displays the filter option.
Name	Displays the name of the static NAT rule set.
From	Displays the name of the routing instance/zone/interface from which the packets flow.
Rule	Displays the name of the rule in the selected static NAT rule set.
Description	Displays a description of the static NAT rule set.
Rules in Selected Rule-Set	
Rule Name	Displays the name of the routing instance/zone/interface to which the packet flows.
Match Destination	Displays the match destination address.
Action	Displays the action of the rule in the selected rule set.
Description	Displays a description of the rule in the selected static NAT rule set.

Table 187: Add Static NAT Configuration Details

Field	Function	Action
Add Rule Set		
Rule Set Name	Specifies the name of the rule set.	Enter the rule set name.
Rule Set Description	Specifies a description for the rule set.	Enter a description for the rule set.
From	Specifies the filter options. The options available are: <ul style="list-style-type: none"> • Routing Instance • Zone • Interface 	Select an option. Select the routing instances/zones/interfaces in the Available column and the use the right arrow to move them to the Selected column.
Add Rule		
Rule Name	Specifies the name of the rule.	Enter the rule name.
Rule Description	Specifies a description for the rule.	Enter a description for the rule.
Match Destination Address		
IPv4	Specifies the IPv4 address.	Enter the IPv4 address.
IPv6	Specifies the IPv6 address.	Enter the IPv6 address.
Then		
Static Prefix	Specifies the static prefix.	Enter the static prefix address.
Routing Instance	Specifies the routing instance.	Select a routing instance.

- See Also**
- [Source NAT Configuration Page Options on page 301](#)
 - [Destination NAT Configuration Page Options on page 306](#)
 - [Proxy Configuration Page Options on page 311](#)

Proxy Configuration Page Options

1. Select **Configure>NAT>Proxy** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Configure>Security>NAT>Proxy ARP/ND** in the J-Web user interface.

The Proxy ARP configuration page appears. [Table 188 on page 312](#) explains the contents of this page.

2. Click one:

- **Add** or **+**—Adds a new or duplicate proxy configuration. Enter information as specified in [Table 190 on page 312](#).
 - **Edit** or **/**—Edits the selected proxy ARP or Proxy ND configuration.
 - **Delete** or **X**—Deletes the selected proxy ARP or proxy ND configuration.
3. Click one:
- **OK**—Saves the configuration and returns to the main configuration page.
 - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
 - **Cancel**—Cancels your entries and returns to the main configuration page.

Table 188: Proxy Configuration Page

Field	Function
Proxy	
Interface	Displays the interface type.
Address	Displays the IPv4 or IPv6 address.

Table 189: Add Proxy ARP Configuration Details

Field	Function	Action
Add Proxy ARP		
Interface	Specifies the interface type. The options available are: <ul style="list-style-type: none"> • ge-0/0/0.0 • ge-0/0/2.0 • lo0.0 • vlan0.0 	Select an option.
Address	Specifies the proxy ARP IP address.	Click Delete to deleted the proxy ARP address.
Address/Range	Specifies the source IP address range.	Click Add to add the range address.
To	Specifies the end IP address that the device can be assigned to.	Click Add to add the port address.

Table 190: Add Proxy ND Configuration Details

Field	Function	Action
Add Proxy ND		

Table 190: Add Proxy ND Configuration Details (continued)

Field	Function	Action
Interface	Specifies the interface type. The options available are: <ul style="list-style-type: none"> • ge-0/0/0.0 • ge-0/0/1.0 • ge-0/0/3.0 • lo0.0 	Select an option.
Address	Specifies the proxy ND IP address.	Click Delete to delete the proxy ND address.
Address/Range	Specifies the source IPv6 address range.	Click Add to add the range address.
To	Specifies the end IPv6 address that the device can be assigned to.	Click Add to add the port address.

- See Also**
- [Source NAT Configuration Page Options on page 301](#)
 - [Destination NAT Configuration Page Options on page 306](#)
 - [Static NAT Configuration Page Options on page 309](#)

Objects

- [Zones and Screens Configuration Page Options on page 313](#)
- [Configuring Applications on page 322](#)
- [Zone Address Book Configuration Page Options on page 325](#)
- [Address Book Configuration Page Options on page 326](#)
- [Proxy Profiles Configuration Page Options on page 328](#)

Zones and Screens Configuration Page Options

1. Select **Configure>Security>Zones/Screens** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Configure>Security>Objects>Zones/Screens** in the J-Web user interface.

The Zones/Screens configuration page appears. [Table 191 on page 314](#) explains the contents of this page.

2. Click one:
 - **Add** or **+**—Adds a new or duplicate zone configuration. Enter information as specified in [Table 192 on page 314](#).
 - **Edit** or **/**—Edits the selected zone configuration.

- **Delete** or **X**—Deletes the selected zone configuration.
3. Click one:
- **Add** or **+**—Adds a new or duplicate screen configuration. Enter information as specified in [Table 193 on page 316](#).
 - **Edit** or **/**—Edits the selected screen configuration.
 - **Delete** or **X**—Deletes the selected screen configuration.
4. Click one:
- **OK**—Saves the configuration and returns to the main configuration page.
 - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
 - **Cancel**—Cancels your entries and returns to the main configuration page.

Table 191: Zones/Screens Configuration Page

Field	Function
Zones list	
Zone name	Displays the name of the zone.
Type	Displays the type of zone.
Services	Displays the type of service.
Protocols	Displays the protocol type of incoming traffic.
Interfaces	Displays the interfaces that are part of this zone.
Screen	Displays name of the option objects applied to the zone.
Description	Displays a description of the zone.
Screen list	
Screen name	Displays the name of the screen object.
Type	Displays the type of screen.
Description	Displays a description of the screen.

Table 192: Add Zone Configuration Details

Field	Function	Action
Main		
Zone name	Specifies the name of the zone.	Enter a name for the zone.
Zone description	Specifies a description for the zone.	Enter a description for the zone.

Table 192: Add Zone Configuration Details (continued)

Field	Function	Action
Zone type	Specifies the type of the zone.	Select either security or functional . Only one functional zone can be configured.
Send RST for non matching session	Specifies that when the reset feature is enabled, the system sends a TCP segment with the RESET flag set when traffic arrives. This does not match an existing session and does not have the Synchronize flag set.	Select the Send RST for non matching session check box to enable this feature.
Binding screen	Specifies that you can assign screens to a zone. NOTE: If you have already configured screens, the list shows the screen names and allows you to select or delete a screen.	Select a binding screen from the list.
Interfaces in this zone	Specifies the available interfaces that you can select for the security zone.	Select or deselect the interfaces that you want to include in the security zone using either the left or the right arrow. NOTE: The selected interfaces are displayed in the Selected grid.
Host inbound traffic - Zone		
Protocols	Specifies the protocols that permit inbound traffic of the selected type to be transmitted to hosts within the zone.	Select the protocols in the Available column and then use the right arrow to move them to the Selected column. Select all to permit all protocols. NOTE: To deselect protocols, select the protocols in the Selected column and then use the left arrow to move them to the Available column.
Services	Specifies the interface services that permit inbound traffic of the selected type to be transmitted to hosts within the zone.	Select the services in the Available column and then use the right arrow to move them to the Selected column. Select all to permit all services. NOTE: To deselect services, select the services in the Selected column and then use the left arrow to move them to the Available column.
Host inbound traffic - Interface		

Table 192: Add Zone Configuration Details (continued)

Field	Function	Action
Interface services	Specifies the interfaced services that permit inbound traffic from the selected interface to be transmitted to hosts within the zone.	<p>Select the interface services in the Available column and then use the right arrow to move them to the Selected column. Select all to permit all interface services.</p> <p>To deselect services, select the services in the Selected column and then use the left arrow to move them to the Available column.</p> <p>NOTE: If you select multiple interfaces, the existing interface services and protocols are cleared and are applied to the selected interfaces.</p>
Interface protocols	Specifies the interface protocols that permit inbound traffic from the selected interface to be transmitted to hosts within the zone.	<p>Select the interface protocols in the Available column and then use the right arrow to move them to the Selected column. Select all to permit all interface protocols.</p> <p>To deselect protocols, select the protocols in the Selected column and then use the left arrow to move them to the Available column.</p>

Table 193: Add Screen Configuration Details

Field	Function	Action
Main		
Screen name	Specifies the name of the screen object.	Enter a name for the screen object.
Screen description	Specifies a description for the screen object.	Enter a description for the screen object.
Generate alarms without dropping packet	Specifies that alarms are generated without dropping packets.	Select the Generate alarms without dropping packet check box to enable this feature.
IP spoofing	Specifies that you can enable IP address spoofing. IP spoofing is when a false source address is inserted in the packet header to make the packet appear to come from a trusted source.	Select the IP spoofing check box to enable this feature.
IP sweep	Specifies the number of ICMP address sweeps. An IP address sweep can occur with the intent of triggering responses from active hosts.	Select the IP sweep check box to enable this feature.

Table 193: Add Screen Configuration Details (continued)

Field	Function	Action
Threshold	Specifies the threshold value of the IP sweep.	Enter the time interval for an IP sweep. NOTE: If a remote host sends ICMP traffic to 10 addresses within this interval, an IP address sweep attack is flagged and further ICMP packets from the remote host are rejected. The range is from 1000 through 1000000 microseconds. The default value is 5000 microseconds.
Port scan	Specifies the number of TCP port scans. The purpose of this attack is to scan the available services in the hopes that at least one port will respond, thus identifying a service to target.	Select the Port scan check box to enable this feature.
Threshold	Specifies the threshold value of the TCP port scan.	Enter the time interval for a port scan. NOTE: If a remote host scans 10 ports within this interval, a port scan attack is flagged and further packets from the remote host are rejected. The range is from 1000 through 1000000 microseconds. The default value is 5000 microseconds.
WinNuke attack protection	Specifies the number of TCP WinNuke attacks. NOTE: WinNuke is a DoS attack targeting any computer on the Internet running Windows operating system.	Select the WinNuke attack protection check box to enable this feature.
Denial of Service		
Land attack protection	Specifies the number of land attacks. NOTE: Land attacks occur when an attacker sends spoofed SYN packets containing the IP address of the victim as both the destination and source IP address.	Select the Land attack protection check box to enable this feature.
Teardrop attack protection	Specifies the number of teardrop attacks. NOTE: Teardrop attacks exploit the reassembly of fragmented IP packets.	Select the Teardrop attack protection check box to enable this feature.
ICMP fragment protection	Specifies the number of ICMP fragments. NOTE: ICMP packets contain very short messages. There is no legitimate reason for ICMP packets to be fragmented.	Select the ICMP fragment protection check box to enable this feature.
Ping of death attack protection	Specifies the ICMP ping of death counter. NOTE: A ping of death occurs when IP packets are sent that exceed the maximum legal length (65,535 bytes).	Select the Ping of death attack protection check box to enable this feature.

Table 193: Add Screen Configuration Details (continued)

Field	Function	Action
Large size ICMP packet protection	Specifies the number of large ICMP packets.	Select the Large size ICMP packet protection check box to enable this feature.
Block fragment traffic	Specifies the number of IP block fragments.	Select the Block fragment traffic check box to enable this feature.
SYN-ACK-ACK proxy protection	Specifies the number of TCP flags enabled with SYN-ACK-ACK. NOTE: This is designed to prevent flooding with SYN-ACK-ACK sessions. After the number of connections from the same IP address reaches the SYN-ACK-ACK proxy threshold, Junos OS rejects further connection requests from that IP address.	Select the SYN-ACK-ACK proxy protection check box to enable this feature.
Threshold	Specifies the threshold value for SYN-ACK-ACK proxy protection.	Enter the threshold value for SYN-ACK-ACK proxy protection. NOTE: The range is from 1 through 250000 sessions. The default value is 512 sessions.
Anomalies		
Bad option	Specifies the number of bad options counter.	Select the Bad option check box to enable this feature.
Security	Specifies the method for hosts to send security.	Select the Security check box to enable this feature.
Unknown protocol	Specifies that the IP address with security option can be enabled.	Select the Unknown protocol check box to enable this feature.
Strict source route	Specifies the complete route list for a packet to take on its journey from source to destination.	Select the Strict source route check box to enable this feature.
Source route	Specifies the number of IP addresses of the devices set at the source that an IP transmission is allowed to take on its way to its destination.	Select the Source route check box to enable this feature.
Timestamp	Specifies the time recorded (in UTC) when each network device receives the packet during its trip from the point of origin to its destination.	Select the Timestamp check box to enable this feature.
Stream	Specifies a method for the 16-bit SATNET stream identifier to be carried through networks that do not support streaming.	Select the Stream check box to enable this feature.
Loose source route	Specifies a partial route list for a packet to take on its journey from source to destination.	Select the Loose source route check box to enable this feature.
Record route	Specifies that IP addresses of network devices along the path that the IP packet travels can be recorded.	Select the Record route check box to enable this feature.

Table 193: Add Screen Configuration Details (continued)

Field	Function	Action
SYN Fragment Protection	Specifies the number of TCP SYN fragments.	Select the SYN Fragment Protection check box to enable this feature.
SYN and FIN Flags Set Protection	Specifies the number of TCP SYN and FIN flags. NOTE: When you enable this option, Junos OS checks if the SYN and FIN flags are set in TCP headers. If it discovers such a header, it drops the packet.	Select the SYN and FIN Flags Set Protection check box to enable this feature.
FIN Flag Without ACK Flag Set Protection	Specifies the number of TCP FIN flags set without an ACK flag set.	Select FIN Flag Without ACK Flag Set Protection check box to enable this feature.
TCP Packet Without Flag Set Protection	Specifies the number of TCP headers without flags set. NOTE: A normal TCP segment header has at least one flag control set.	Select TCP Packet Without Flag Set Protection check box to enable this feature.
Flood Defense		
Limit sessions from the same source	Specifies that sessions are limited from the same source IP.	Enter the range within which the sessions are limited from the same source IP. NOTE: The range is from 1 through 50000 sessions.
Limit sessions from the same destination	Specifies that sessions are limited from the same destination IP.	Enter the range within which the sessions are limited from the same destination IP. The range is from 1 through 50000 sessions. NOTE: The default value is 128 sessions. For SRX Series Services Gateways, the range is from 1 through 8000000 sessions per second.
ICMP flood protection	Specifies the Internet Control Message Protocol (ICMP) flood counter. NOTE: An ICMP flood typically occurs when ICMP echo requests use all resources in responding, such that valid network traffic can no longer be processed.	Select the ICMP flood protection check box to enable this feature.
Threshold	Specifies the threshold value for ICMP flood protection.	Enter the threshold value for ICMP flood protection. NOTE: The range is from 1 through 100000 ICMP packets per second (pps). For SRX Series Services Gateways, the range is from 1 through 4000000 ICMP pps.

Table 193: Add Screen Configuration Details (continued)

Field	Function	Action
UDP flood protection	<p>Specifies the User Datagram Protocol (UDP) flood counter.</p> <p>NOTE: UDP flooding occurs when an attacker sends IP packets containing UDP datagrams to slow system resources, such that valid connections can no longer be handled.</p>	Select the UDP flood protection check box to enable this feature.
Threshold	<p>Specifies the threshold value for UDP flood protection.</p> <p>NOTE: The range is from 1 through 100000 session. The default value is 1000 sessions.</p>	Enter the threshold value for UDP flood protection.
<p>UDP white list</p> <p>Starting Junos Release 18.1R1, the option to add UDP IP addresses and white list them is available.</p>	<p>Specifies the UDP port IP addresses that can be allowed access.</p> <p>NOTE:</p> <ul style="list-style-type: none"> The UDP white list option is enabled only if you select UDP flood protection. The white list that you created in the UDP white list window will be available in the TCP white list window also for selection. 	<p>Choose Select. The UDP White List window appears. Click + to add IP addresses that you wish to white list. The Add Whitelist window appears. Enter a Name to identify the group of IP addresses. Enter IPv4 or IPv6 address. Click +. The IPv4/IPv6 Address(es) lists the address that you entered. You may add as many IP addresses to this group. When you are done click OK. The UDP White List window is presented.</p> <p>The Name you associated with the group of IP addresses that you entered in the Add Whitelist window is listed in the Selected table. You can create many such names (group of IP addresses) and choose them to be in the Available column for you to select it later for white listing. To move the groups between Available and Selected list click the < or > accordingly.</p>
SYN flood protection	<p>Specifies that SYN flooding occurs when a host becomes so overwhelmed by SYN segments initiating incomplete connection requests that it can no longer process legitimate connection requests.</p>	Select the SYN flood protection check box to enable all the threshold and age timeout options.
<p>TCP white list</p> <p>Starting Junos Release 18.1R1, the option to add TCP IP addresses and white list them is available.</p>	<p>Specifies the TCP port IP addresses that can be allowed access.</p> <p>NOTE:</p> <ul style="list-style-type: none"> The TCP white list option is enabled only if you select SYN flood protection. The white list that you created in the TCP white list window will be available in the UDP white list window also for selection. 	<p>Choose Select. The TCP White List window appears. Click + to add IP addresses that you wish to white list. The Add Whitelist window appears. Enter a Name to identify the group of IP addresses. Enter IPv4 or IPv6 address. Click +. The IPv4/IPv6 Address(es) lists the address that you entered. You may add as many IP addresses to this group. When you are done click OK. The TCP White List window is presented.</p> <p>The Name you associated with the group of IP addresses that you entered in the Add Whitelist window is listed in the Selected table. You can create many such names (group of IP addresses) and choose them to be in the Available column for you to select it later for white listing. To move the groups between Available and Selected list click the < or > accordingly.</p>

Table 193: Add Screen Configuration Details (continued)

Field	Function	Action
Attack threshold	Specifies the number of SYN packets per second required to trigger the SYN proxy mechanism.	<p>Enter a value from 1 through 100000 proxied requests per second. The default value is 200.</p> <p>NOTE: For SRX Series Services Gateways, the range is from 1 through 1000000 proxied requests per second. The default attack threshold value is 625 pps.</p>
Alarm threshold	Specifies the number of half-complete proxy connections per second at which the device makes entries in the event alarm log.	<p>Enter a value from 1 through 100000 segments received per second for SYN flood alarm. The default value is 512.</p> <p>NOTE: For SRX Series Services Gateways, the range is from 1 through 1000000 segments per second. The default alarm threshold value is 250 pps.</p>
Source threshold	Specifies the number of SYN segments received per second from a single source IP address (regardless of the destination IP address and port number), before the device begins dropping connection requests from that source.	<p>Enter a value for SYN flood from the same source from 4 through 100000 segments received per second. The default value is 4000.</p> <p>NOTE: For SRX Series Services Gateways, the range is from 4 through 1000000 segments per second. The default source threshold value is 25 pps.</p>
Destination threshold	Specifies the number of SYN segments received per second for a single destination IP address before the device begins dropping connection requests to that destination. If a protected host runs multiple services, you might want to set a threshold based only on destination IP address, regardless of the destination port number.	<p>Enter a value for SYN flood to the same destination from 4 through 100000. The default value is 4000.</p> <p>NOTE: For SRX Series Services Gateways, the range is from 4 through 1000000 segments per second. The default destination threshold value is 0 pps.</p>
Ager timeout	Specifies the maximum length of time before a half-completed connection is dropped from the queue. You can decrease the timeout value until you see any connections dropped during normal traffic conditions.	<p>Enter a value for SYN attack protection from 1 through 50 seconds. The default value is 20 seconds.</p> <p>NOTE: 20 seconds is a reasonable length of time to hold incomplete connection requests.</p>
Apply to Zones		
Apply to Zones	Specifies that you can apply values to zones from the Available column to the Selected column.	<p>Select zones in the Available column and then use the right arrow to move them to the Selected column.</p> <p>NOTE: To remove zones from the Selected column, select the zones in the Selected column and then use the left arrow to move them to the Available column.</p>

- See Also**
- [Firewall Policies Configuration Page Options](#)
 - [UTM Policies Configuration Page Options on page 371](#)
 - [IDP Policies Configuration Page Options on page 381](#)

Configuring Applications

1. Select **Configure>Security>Objects>Applications**.
The Applications configuration page appears. [Table 194 on page 322](#) explains the contents of this page.
2. (Starting from Junos OS Release 19.2R1) Select **Configure>Security Services>Security Policy>Objects>Services**.
3. Click one:
 - **Add**—Adds a new or duplicate application configuration. Enter information as specified in [Table 195 on page 323](#).
 - **Edit**—Edits the selected application configuration.
 - **Delete**—Deletes the selected application configuration.
4. Click one:
 - **OK**—Saves the configuration and returns to the main configuration page.
 - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
 - **Cancel**—Cancels your entries and returns to the main configuration page.

Table 194: Applications Configuration Page

Field	Function
Custom-Applications	
Application Name	Displays the custom application name.
Application Description	Displays a description of the custom application.
Application-Protocol	Displays the custom application protocol.
IP-Protocol	Displays the custom network protocol.
Source-Port	Displays the custom source port identifier.
Destination-Port	Displays the custom destination port identifier.
Pre-defined Applications	
Application Name	Displays the predefined application name.
Application-Protocol	Displays the predefined application protocol.
IP-Protocol	Displays the predefined network protocol.

Table 194: Applications Configuration Page (continued)

Field	Function
Source-Port	Displays the predefined source port identifier.
Destination-Port	Displays the predefined destination port identifier.
Application Sets	
Application-Set Name	Displays the application set name.
Members	Displays members in the set.
Description	Displays a description of the application set.

Table 195: Add Applications Configuration Details

Field	Function	Action
Custom-Applications		
Global		
Application Name	Specifies a custom application name.	Enter a custom application name.
Application Description	Specifies a description for the custom application.	Enter a description for the custom application.
Application-protocol	Specifies the custom application protocol.	Select a value from the list.
Match IP protocol	Specifies the custom network protocol.	Select a value from the list.
Destination Port	Specifies the custom destination port identifier.	Select a value from the list.
Source Port	Specifies the custom source port identifier.	Select a value from the list.
Inactivity-timeout	Specifies the length of time (in seconds) that the application is inactive before it times out.	Enter a value from 4 through 86400.
RPC-program-number	Specifies the remote procedure call value.	Enter a value from 0 through 65535.
Match ICMP message code	Specifies the Internet Control Message Protocol message code.	Select a value from the list.
Match ICMP message type	Specifies the Internet Control Message Protocol message type.	Select a value from the list.
UUID	Specifies a universal unique identifier (UUID).	Enter a UUID.
ApplicationSet	Specifies the set to which this application belongs.	Select an option from the list.
Terms		

Table 195: Add Applications Configuration Details (continued)

Field	Function	Action
New Term	Specifies the new term created. The options available are: <ul style="list-style-type: none"> • Add—Adds a new term. • Edit—Edits the selected term. • Delete—Deletes a record. 	Select an option.
Term Name	Specifies a name for the application term.	Enter a term name.
ALG	Specifies the Application Layer Gateway for the application protocol.	Select an option from the list.
Match IP protocol	Specifies the network protocol.	Select an option from the list.
Destination Port	Specifies the destination port identifier.	Enter the destination port identifier.
Source Port	Specifies the source port identifier.	Enter the source port identifier.
Inactivity-timeout	Specifies the length of time (in seconds) that the application is inactive before it times out.	Enter a value from 4 through 86400.
RPC-program-number	Specifies the remote procedure call value.	Enter a value from 0 through 65535.
Match ICMP message code	Specifies the Internet Control Message Protocol message code.	Select a value from the list.
Match ICMP message type	Specifies the Internet Control Message Protocol message type.	Select a value from the list.
UUID	Specifies the set to which this application belongs.	Select an option from the list.
Application Sets		
Application-set Name	Specifies the application set name.	Enter an application set name. Using the right and left arrows select values from Application out of this set and move them to Applications in this set .
Description	Specifies a description for the application set.	Enter a description for the application set.

- See Also**
- [Scheduler Configuration Page Options](#)
 - [Address Book Configuration Page Options on page 326](#)
 - [IDP Policies Configuration Page Options on page 381](#)

Zone Address Book Configuration Page Options

1. Select **Configure>Security>Policy Elements> Zone Address** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Configure>Security>Objects>Zone Addresses** in the J-Web user interface.

The Addresses/Address-sets Configuration page appears. [Table 196 on page 325](#) explains the contents of this page.

2. Click one:
 - **Add** or **+**—Adds a new or duplicate address/address-set configuration. Enter information as specified in [Table 197 on page 326](#).
 - **Edit** or **/**—Edits the selected address/address-set configuration.
 - **Delete** or **X**—Deletes the selected address/address-set configuration.
3. Click one:
 - **OK**—Saves the configuration and returns to the main configuration page.
 - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
 - **Cancel**—Cancels your entries and returns to the main configuration page.

Table 196: Addresses/Address Sets Configuration Page

Field	Function
Addresses	
Zone	Displays the zone to which the address is applied.
Zone Name	Displays the zone name of the address.
Address Name	Displays the address name.
IP(v4/v6)/Prefix	Displays the IP address of the address.
Domain Name	Displays the domain name of the address.
Address Sets	
Zone	Displays the zone to which the address set is applied.
Zone Name	Displays the zone name of the address set.
Address Set Name	Displays the address set name.
Address List	Displays the preexisting addresses that are included or excluded from the address set.

Table 197: Add Addresses/Address-sets Configuration Details

Field	Function	Action
Add Address		
Zone	Specifies the zone to which the address is applied.	Select an option from the list.
Address Name	Specifies the address name.	Enter the address name.
IP(v4/v6)/Prefix	Specifies the IP address of the address.	Select the option and enter the IP address.
Domain Name	Specifies the domain name of the address.	Select the option and enter the domain name.
Address Sets	Displays the address sets.	Displays the address set name.
Add Address Set	Specifies the address set name.	Enter the address set name and click Add . NOTE: Click Undo to delete the immediate previous action.
Add Address Set		
Zone	Specifies the zone to which the address set is applied.	Select an option from the list.
Address Set Name	Specifies the address set name.	Enter the address set name.
Address List	Specifies which of the preexisting addresses should be included or excluded from the address set.	Select the addresses and use the arrows to move them to the Out of This Set and In This Set lists.

- See Also**
- [Applications Configuration Page Options](#)
 - [IDP Policies Configuration Page Options on page 381](#)
 - [UTM Policies Configuration Page Options on page 371](#)

Address Book Configuration Page Options

1. Select **Configure>Security>Address Book** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Configure>Security>Objects>Global Addresses** in the J-Web user interface.

The Address Books Configuration page appears. [Table 198 on page 327](#) explains the contents of this page.

2. Click one:

- **Add** or **+**—Adds an address book configuration. Enter information as specified in [Table 199 on page 327](#).
 - **Edit** or **/**—Edits the selected address book configuration.
 - **Delete** or **X**—Deletes the selected address book configuration.
3. Click one:
- **OK**—Saves the configuration and returns to the main configuration page.
 - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
 - **Cancel**—Cancels your entries and returns to the main configuration page.

Table 198: Address Books Configuration Page

Field	Function
Address Books	
Address Book Name	Displays the address book name.
Attached Zone	Displays the name of the zone that is attached to the address book.
Global	Displays information about the predefined address book. The global address book is available by default to all security zones. You do not need to attach a security zone to the global address book.
Address/Address-Set Name	Displays the addresses and address sets associated with the selected address book.
Address Value	Displays the IP address.
Address-Set Members	Displays the addresses in an address set.

Table 199: Add Address Books/Address Sets Configuration Details

Field	Function	Action
Add Address Book		
Address Book Name	Specifies the address book name.	Enter a name for the address book.

Table 199: Add Address Books/Address Sets Configuration Details (continued)

Field	Function	Action
Attach Zones	Specifies which of the predefined zones should be attached to the specified address.	<p>Select the zones from the Available list and use the Right Arrow to move them to the Attached list.</p> <p>You can select more than one zone from the Attached list for one address book. However, make sure that each zone has only one address book attached to it. If there is more than one address book attached to a zone, you will get the following error when you commit the configuration:</p> <p>“Security zone must be unique in address books.”</p>
Add Address		
Address Name	Specifies the address name.	Enter a name for the address.
Address Type	Specifies the type of address.	<p>Select the address type from the list. The options available are:</p> <ul style="list-style-type: none"> • IP address • IP address/network • Domain name • Ranged address
Value	Specifies the address.	Enter an address that matches the selected address type.
Add Address Set		
Address Set Name	Specifies the address set name.	Enter the address set name.
Address List	Specifies which of the preexisting addresses should be included or excluded from the address set.	Select the addresses and use the arrows to move them to the Out of This Set and In This Set lists.
Address Set List	Specifies which of the preexisting address sets should be included or excluded from the list.	Select the address sets and use the arrows to move them to the Out of This Set and In This Set lists.

- See Also**
- [Zones and Screens Configuration Page Options on page 313](#)
 - [Firewall Policies Configuration Page Options](#)

Proxy Profiles Configuration Page Options

The Proxy Profiles page is use to configure the proxy profiles to protect your web servers against client-to-server attacks from malicious clients.

1. Select **Configure>Security Service>Security PolicyObjects>Proxy Profiles** in the J-Web user interface.

The Proxy Profiles configuration page appears. [Table 200 on page 329](#) explains the contents of this page.

2. Click one:

- **Add** or **+**—Adds a new or duplicate proxy profile configuration. Enter information as specified in [Table 201 on page 329](#).
- **Edit** or **/**—Edits a selected proxy profile configuration [Table 201 on page 329](#).
- **Delete** or **X**—Deletes the selected proxy profile configuration.
- **Search Icon**—Enables you to search a proxy profile or rule from the grid.
- **Show Hide Column Filter icon**—Enables you to show or hide a column in the grid.

3. Click one:

Click Commit icon at the top of the J-Web page. The following commit options are displayed.

- **Commit**—Commits the configuration and returns to the main configuration page.
- **Compare**—Enables you to see the configuration changes that you have performed in the Show Pending Changes.
- **Discard**—Discards the configuration changes you performed in the J-Web.
- **Preferences**—There are two tab:
 - **Commit preferences**— You can choose to just validate or validate and commit the changes.
 - **Confirm commit timeout (in min)**— You can select the commit timeout interval.

Table 200: Proxy Profile Configuration Page

Field	Function
Profile Name	Displays the name of the proxy profile.
Server IP/ Host Name	Displays the connection type used by the proxy profile.
Port Number	Displays the port number.

Table 201: Add-Edit Proxy Profile Configuration Details

Field	Function	Action
Profile Name	Specifies the name of the proxy profile.	Enter a name for the proxy profile.

Table 201: Add-Edit Proxy Profile Configuration Details (continued)

Field	Function	Action
Connection Type	Specifies the type of connection used by the proxy profile.	Select the connection type server from the list. <ul style="list-style-type: none"> • Server IP • Host Name
Port Number	Specifies the port number used by the proxy profile.	Select a port number for the proxy profile from 0 to 65535.

Security Objects

- [Address Pools Configuration Page Options on page 330](#)
- [Application Tracking Configuration Page Options on page 331](#)

Address Pools Configuration Page Options

1. Select **Configure>Security Objects>Address Pools** in the J-Web user interface.

The Address Pools configuration page appears. [Table 202 on page 330](#) explains the contents of this page.

2. Click one:
 - **+**—Adds a new or duplicate address pools configuration. Enter information as specified in [Table 202 on page 330](#).
 - **Edit** or **/**—Edits the selected address pools configuration.
 - **Delete**—Deletes the selected address pools configuration.
 - Search icon—Enables you to search a address pool in the grid.
 - Show Hide Column Filter icon—Enables you to show or hide a column in the grid.

Table 202: Add Address Pool Configuration Details

General		
Pool Name	Specifies the name of the address pool.	Enter the address pool name.
Network Address	Specifies the network address used by the address pool.	Enter a IPv4 address for the address pool.
XAUTH Attributes		
Primary DNS Server	Specifies the primary-dns IP address.	Enter the primary-dns IP address.
Secondary DNS Server	Specifies the secondary-dns IP address.	Enter the secondary-dns IP address.
Primary WINS Server	Specifies the primary-wins IP address.	Enter the primary-wins IP address.
Secondary WINS Server	Specifies the secondary-wins IP address.	Enter the secondary-wins IP address.

Table 202: Add Address Pool Configuration Details (continued)

Address Ranges		
Name	Specifies the name of the address range.	Enter a name for the IP address range.
Lower Limit	Specifies the lower limit of the address range.	Enter the lower limit of the address range.
High Limit	Specifies the upper limit of the address range.	Enter the upper limit of the address range.
Add	Adds a new address range for the access profile.	Click + to add a new address range for the address pool.
Delete	Deletes the address range for the access profile.	Click Delete to delete the address range for the address pool.

See Also • [Application Tracking Configuration Page Options on page 331](#)

Application Tracking Configuration Page Options

1. Select **Configure>Security Objects>App Tracking** in the J-Web user interface.
The Application Tracking configuration page appears. [Table 203 on page 331](#) explains the contents of this page.
2. Click **Save** to save the configuration.
3. Click **Cancel** to remove all the entries of the configuration.

Table 203: Application Tracking Configuration Page

Field	Function	Action
Application Tracking		
Application tracking	Enables or disables application tracking.	Select this option to enable application tracking.
Logging Type	<p>You can set the following:</p> <ul style="list-style-type: none"> • Log as session(s) created—Generates a log message when a session is created. By default, this option is disabled. • Delay logging first session(s)—Enables you to specify the length of time that must pass before the first log message is created. The default is 1 minute. 	Select an option.
First Update Interval (min)	Interval when the first update message is sent (minutes).	Use the up/down arrow to set the interval time.
Session Update Interval (min)	Enables you to set the interval at which update messages are sent. Default is 5 minutes.	Use the up/down arrow to set the interval time.

Table 203: Application Tracking Configuration Page (continued)

Application Tracking By Zone	Lists the available zones.	<ul style="list-style-type: none"> To enable application tracking, select the zone and click the right arrow to move it to the tracking enabled list. To disable application tracking, select the zone and then click the left arrow to move the zone back into the available list.
------------------------------	----------------------------	---

See Also • [Address Pools Configuration Page Options on page 330](#)

AppSecure

- [Application Signature Configuration Page Options on page 332](#)
- [Application Firewall Configuration Page Options on page 334](#)

Application Signature Configuration Page Options

Use the following procedure to download predefined application signatures and to view installed application signatures and their status.

1. Select **Configure>Security>AppSecure Settings** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Configure>Security>AppSecure>App Signatures** in the J-Web user interface.

The display lists all enabled and disabled application signatures on the device.

2. (Junos OS Release 18.3R1 and later releases) Select **Configure>Security Services>App Secure>App Signatures**.

All enabled and disabled application signatures on the device are displayed in a grid format. A message **Once a new custom application signature is created or modified, the configuration is committed immediately to the device.** is displayed at the top of the page.

A status message is displayed just above the grid. It shows the version number of the installed application, the latest version available, and whether you have downloaded or installed an application package.

Installed application package version : 0 | Latest version 3159 available | No application package is downloaded yet



NOTE: If you successfully download an application package, the Install button is displayed. If you successfully install a downloaded application package, an Uninstall button is displayed.

3. Click one:

- **Global Settings**—Defines run specifications for application identification or for an automatic downloading schedule.
 - Select the **Application Signature** tab to define run conditions, and to enable or disable application signatures and the application system cache. You can also select a proxy profile or create a proxy profile.
 - Select the **Download** tab to specify the URL from where you can download the signature package, set up a schedule for automatic downloads of the latest predefined application signature package.
 - Select the **Application System Cache** tab to enable or disable storing of AI result in application cache, configure ASC security services, configure miscellaneous services such as ABPR, or set the cache entry timeout.
- **Download**—Manually downloads the latest or predefined application signature package.
- **More**—Clone an existing application signature package, create group, or configure the page to show a detailed view.
- **Create**—Create a new application signature or group signatures.
- **Uninstall**—Removes application signatures that are currently installed on your device.

On SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800 devices, specify the type of signature to uninstall. Choose one of the uninstall options:

- **Customized**—Uninstalls all customized application signatures on your device. This option does not uninstall predefined application signatures.
- **Predefined**—Uninstalls all predefined application signatures on your device. This option does not uninstall any customized applications.
- **All**—Uninstalls all customized and predefined application signatures on your device.

4. Click one:

- **OK**—Saves the configuration and returns to the main configuration page.
- **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
- **Cancel**—Cancels your entries and returns to the main configuration page.

- See Also**
- [ALG Configuration Page Options on page 429](#)
 - [Application Firewall Configuration Page Options on page 334](#)

Application Firewall Configuration Page Options

1. Select **Configure>Security>Policy>Define AppFW Policy** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Configure>Security>AppSecure>App Firewall** in the J-Web user interface.

The Application Firewall configuration page displays existing application rule sets for the device. Select a rule set to display its rules in the bottom pane. The content of this display is described in [Table 204 on page 334](#).

2. Click one:
 - **Add** or **+**—Adds a new rule set configuration. Enter the information specified in [Table 205 on page 335](#). To add a rule configuration, click **Add** from the lower pane or from the Add Rule Set page, and enter the information specified in [Table 206 on page 335](#).
 - **Edit** or **/**—Edits the selected rule set or the selected rule. See [Table 205 on page 335](#) for rule set details or [Table 206 on page 335](#) for rule details.
 - **Delete** or **X**—Deletes the selected rule set or the selected rule configuration.
3. Click one:
 - **OK**—Saves the configuration and returns to the main configuration page.
 - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
 - **Cancel**—Cancels your entries and returns to the main configuration page.

Table 204: Application Firewall Configuration Page

Field	Function
Rule Set	
Name	Specifies the name of an existing application rule set configured for the device. Select a rule set to display its associated rules in the lower pane.
Rule	Specifies the name of each rule associated with the rule set. If this field contains more than two rule names, hover over the field to display the names of all the rules in a tool tip.
Rules in Selected Rule-Set	
Rule Name	Displays the name of each rule contained in the selected rule set. This pane is blank until a rule set is selected in the upper pane.
Match Dynamic Applications	Specifies one or more application signatures to be used as match criteria for the rule.

Table 204: Application Firewall Configuration Page (continued)

Field	Function
Action	<p>Specifies the action to be taken if traffic matches one of the specified applications.</p> <ul style="list-style-type: none"> • permit—Permits traffic that matches this rule. • deny—Denies traffic that matches this rule.

Table 205: Add or Edit Rule Set Configuration Details

Field	Function	Action
Rule Set Name	Specifies the rule set name	<p>Enter a rule set name.</p> <p>When editing a rule set, the name cannot be changed.</p>
Rules	When rules are defined for the new rule set, the Rules pane displays each rule name, its associated dynamic applications, and its action.	Click Add to create a rule for this rule set. See Table 206 on page 335 for rule configuration details.

Table 206: Add or Edit Rule Configuration Details

Field	Function	Action
Rule Name	Specifies the name of the rule.	<p>Enter a rule name.</p> <p>When editing a selected rule, the name cannot be changed.</p>
Rule Action	<p>Specifies the action to be taken when traffic matches one of the dynamic application signatures associated with this rule.</p> <ul style="list-style-type: none"> • permit—Permits traffic that matches this rule. • deny—Denies traffic that matches this rule. 	<p>Select permit or deny.</p> <p>NOTE: All rules belonging to a rule set must have the same Action setting.</p> <p>When editing a rule, changing the Action setting will change the setting in all rules in this rule set.</p>
Match Dynamic Application		
Applications	Displays the applications available on your device.	<p>To add applications to the match criteria:</p> <ul style="list-style-type: none"> • Select one or more applications in the Applications list. (Use the Ctrl key to select more than one item.) • Click the right arrow to move the selections to the Matched list.

Table 206: Add or Edit Rule Configuration Details (continued)

Field	Function	Action
Matched	Displays the applications selected as match criteria for the rule.	To delete applications from the match criteria: <ul style="list-style-type: none"> • Select one or more applications in the Matched list. (Use the Ctrl key to select more than one item.) • Click the left arrow to return the selections to the Applications list.
Search	Redisplays the Applications list with the specified application at the top.	Enter an application name.

- See Also**
- [Application Signature Configuration Page Options on page 332](#)
 - [IPv4 Firewall Filters Configuration Page Options on page 437](#)
 - [IPv6 Firewall Filters Configuration Page Options on page 450](#)
 - [Assign to Interfaces Configuration Page Options on page 461](#)

UTM

- [Default Configuration Page Options on page 336](#)
- [Antivirus Configuration Page Options on page 346](#)
- [Web Filtering Configuration Page Options on page 353](#)
- [Category Update Configuration Page Options on page 363](#)
- [Antispam Configuration Page Options on page 364](#)
- [Content Filtering Configuration Page Options on page 366](#)
- [Custom Objects Configuration Page Options on page 368](#)
- [UTM Policies Configuration Page Options on page 371](#)

Default Configuration Page Options

The Default Configuration page describes the security features of Unified threat management (UTM).

This default configuration will be used, If there are multiple UTM policies present in the potential list. The global configuration will be used till the exact match is found in the potential list.

The following security features are parts of UTM default configuration:

- **Sophos Antivirus**— Sophos antivirus is an in-the-cloud antivirus solution. The virus pattern and malware database is located on external servers maintained by Sophos (Sophos Extensible List) servers.
- **Web filtering**—Web filtering lets you to manage Internet usage by preventing access to inappropriate Web content.

- **Antispam**—This feature examines transmitted messages to identify any e-mail spam.
- **Content filtering**— This feature blocks or permits certain types of traffic based on the MIME type, file extension, protocol command, and embedded object type.

1. Select **Configure>Security>UTM>Default Configuration** in the J-Web user interface.

The Default Configuration page appears. [Table 207 on page 337](#) explains the contents of this page.

2. Click one:

- **Anti-Virus**—Select this tab to view or create anti-virus configuration. Enter information as specified in [Table 208 on page 338](#).
- **Web Filtering**—Select this tab to view or create the web filtering configuration. Enter information as specified in [Table 208 on page 338](#).
- **Anti-Spam**—Select this tab to view or create the anti-spam configuration. Enter information as specified in [Table 208 on page 338](#).
- **Content-Filtering**—Select this tab to view or create the anti-spam configuration. Enter information as specified in [Table 208 on page 338](#).

3. Click one:

Click Commit icon at the top of the J-Web page. The following commit options are displayed.

- **Commit**—Commits the configuration and returns to the main configuration page.
- **Compare**—Enables you to see the configuration changes that you have performed in the Show Pending Changes.
- **Discard**—Discards the configuration changes you performed in the J-Web.
- **Preferences**—There are two tab:
 - **Commit preferences**— You can choose to just validate or validate and commit the changes.
 - **Confirm commit timeout (in min)**— You can select the timeout interval.

Table 207: Default Configuration main page

Field	Function
Anti-Virus	Displays the configured antivirus. You can also configure an antivirus.
Web Filtering	Displays the configured web filtering. You can also configure a web filtering.
Anti-Spam	Displays the configured antispam. You can also configure an anti-spam.
Content-Filtering	Displays the configured content filtering. You can also configure a content filtering.

Table 208: Default configuration option page

Field	Function	Action
Create antivirus		
Type	Displays the anti-virus engine type.	Select the require required engine type: <ul style="list-style-type: none"> • Anti-Virus None • Sophos Engine
URL Whitelist	Specifies a unique customized list of all URLs or IP addresses for a given category that are to be bypassed for scanning.	Select the customized object from the list.
MIME Whitelist		
list	Specifies the comprehensive list of MIME types that can bypass antivirus scanning.	Select the customized object from the list.
Exception	Specifies a list of MIME types to be excluded from the whitelist. The exception MIME whitelist is a subset of MIME types found in the MIME whitelist.	Select the customized object from the list.
Sophos Engine options		
General Settings		
Timeout	Specify the Sophos antivirus engine timeout.	Select a time, ranges from 1 to 5 seconds.
Retry	Specify the number of times retry the Sophos antivirus engine query.	Select the number of retries from 1 to 5 numeric values.
Server		
Server IP	Specify the DNS Server IP.	Enter a valid DNS server IP address.
Routing Instance	Specify the name of the routing instance.	Select a valid routing instance name..
Pattern Update		
URL	Specifies the URL of the database server.	Enter the URL for the pattern database.
Routing Instance	Specifies the routing instance name.	Select a routing instance from the drop down list. Routing instance can be defined under, 'Configure / Network / Routing Instance'.
Pattern Update Interval (sec)	Specifies the interval at which the database server is queried for a new version of the database.	Enter the time interval for automatically updating the pattern database. The range is from 10 through 10080 seconds. The default interval is 60 seconds.
Auto Update	Specifies that the antivirus pattern database is configured to be automatically updated.	Select the auto update option.

Table 208: Default configuration option page (continued)

Field	Function	Action
No Auto Update	Specifies that the automatic download and update of the antivirus engine and signature database are disabled.	Select the no auto update option.
Proxy Profile	Specify the name of the proxy profile.	Select the proxy profile for Anti virus
Create Proxy Profile		
Profile Name	Specifies the proxy profile name .	Enter a valid profile name.
Connection Type	Specifies the type of connection.	Select any one option from the following: <ul style="list-style-type: none"> • Server IP— Enter the server IP address. • Host Name— Enter the host name.
Port Number	Specifies the port number.	Enter the port number in the range 0 to 65535.
Email Notify		
Admin Email	Specify that the Admin email to be notify about the pattern file update.	Enter a valid admin email id.
Custom Message subject	Specify the custom message subject for notification.	Enter the subject of the custom message.
Custom Message	Displays the custom message for notification.	Enter the custom message for notification.
Fallback Settings		
Default	Specifies all errors other than the categorized settings. This could include either unhandled system exceptions (internal errors) or other unknown errors. The available actions are block or log-and-permit.	Select Log and Permit. The default action is Block.
Content Size	Fallback action for over content size.	Select from the following permit, block, log and permit.
Engine-not-ready	Specifies that the scan engine is not ready during certain processes, for example, while the signature database is loading. The available actions are block or log-and-permit.	Select from the following permit, block, log and permit.
Timeout	Specifies that if the time taken to scan exceeds the timeout setting in the antivirus profile, the processing is aborted and the content is passed or blocked without completing the virus checking.	Select Log and Permit. The default action is Block.

Table 208: Default configuration option page (continued)

Field	Function	Action
Out-of-resources	Specifies the resource constraints error received during virus scanning. This error can be or by the can be sent by the scan engine (as a scan-code) or scan manager. When the system is out of resources occurs, scanning is aborted. The available actions are block or log-and-permit.	Select Log and Permit. The default action is Block.
Too-many-requests	Specifies that if the total number of messages received concurrently exceeds the device limits, the content is passed or blocked depending on the too-many-request fallback option. The available actions are block or log-and-permit.	Select Log and Permit. The default action is Block.
Scan Option		
URI Check	Specify the antivirus URI check.	Enable the URI check.
Content Size Limit	Specifies the accumulated TCP payload size.	Enter the content size limit, a value from 20 through 40,000 KB.
Timeout	Specifies the timeframe between the scan requests generated to the scan result returned by the scan engine. Tricking timeout value is used by all supported protocols. Each protocol can have a different timeout value.	Enter the time interval from 1 through 1800 seconds. The default value is 180 seconds.
Trickling		
Trickling Timeout	Displays the trickling timeout interval.	Enter the time interval from 0 through 600 seconds.
Virus Detection		
Type	Specifies the type of notification to be sent when a virus is detected.	Select Protocol Only or Message option.
Notify Mail Sender	Specifies whether or not a notification is sent to the virus-detection notification e-mail address when a virus is detected.	Select yes to send a notification and no to not send a notification.
Custom Message Subject	Specifies the subject line text for your custom message for the virus detection notification.	Enter the subject line text for your custom message.
Custom Message	Specifies the customized message text for the virus detection notification.	Enter the text for this custom notification message.
Fallback Block		
Type	Specifies the type of notification sent when a fallback option of block is triggered.	Select the Protocol Only or the Message check box.

Table 208: Default configuration option page (continued)

Field	Function	Action
Notify Mail Sender	Specifies that when a virus is detected and a fallback option of block is triggered, an e-mail is sent to the administrator.	Select the Notify Mail Sender check box to enable this notification.
Custom Message	Specifies the customized message text for the fallback block notification.	Enter the text for this custom notification message
Custom Message Subject	Specifies the subject line text for your custom message for the fallback block notification.	Enter the subject line text for your custom message.
Fallback Non Block		
Notify Mail Recipient	Notify mail sender	
Custom Message Subject	Specifies the customized message text for the fallback nonblock notification.	Enter the text for this custom notification message.
Custom Message	Specifies the subject line for your custom message for the fallback nonblock notification.	Enter the subject line text for your custom message.
Create Web filtering		
HTTP persist	Configure the web-filtering engine type	Enable/Disable the option.
HTTP Reassemble	Specifies a unique customized list of all URLs or IP addresses for a given category that are to be bypassed for scanning.	Reassemble HTTP request segments
Type	Specifies a unique customized list of all URLs or IP addresses for a given category that are scanned for blacklisting.	Select from the drop down list: <ul style="list-style-type: none"> • Juniper Enhanced • Juniper Local • Websense Redirect
URL Blacklist	Specifies a unique customized list of all URLs or IP addresses for a given category that are to be bypassed for scanning.	Configure custom URL for blacklist category
URL Whitelist	Specifies a unique customized list of all URLs or IP addresses for a given category that are scanned for blacklisting.	Configure custom URL for whitelist category
Juniper Enhanced Options		
Specifies that the Juniper Enhanced Web filtering intercepts the HTTP and the HTTPS requests and sends the HTTP URL or the HTTPS source IP to the Websense ThreatSeeker Cloud (TSC).		
Global		
Base Filter	Select the base filter from the drop down list.	Select the base filter from the drop down list.

Table 208: Default configuration option page (continued)

Field	Function	Action
Custom Block Message	Specify the juniper enhanced custom block message sent to HTTP Client.	Enter a message to be displayed when content is blocked.
Default Action	Juniper enhanced profile default.	Select Log and Permit. The default action is Log and Permit.
No Safe Search	Specifies not to perform safe-search for Juniper enhanced protocol.	Enable/Disable this option to choose this type of search. NOTE: Do not perform safe-search for Juniper enhanced protocol
Quarantine Custom Message	Juniper enhanced quarantine custom message.	Enter the quarantine custom message.
Timeout	Juniper enhanced timeout.	Select a timeout interval from 1 to 1800 seconds.
Cache		
Size	Specify Juniper enhanced cache size	Select a cache size from 0 to 4096 Killobytes.
Time out	Specify Juniper enhanced cache time out.	Select a timeout interval from 1 to 1800 seconds.
Block Messages		
Type	Specify the type of block message.	Select the type of block message.
URL	Specify the URL of the block message.	Enter URL of the block messages.
Fallback Settings		
Default	Specifies all errors other than the categorized settings. These could include either unhandled system exceptions (internal errors) or other unknown errors. The available actions are block or log-and-permit.	Select Log and Permit. The default action is Log and Permit.
Server-connectivity	Specifies that the server connection is not established during certain processes, for example, while the signature database is loading. The available actions are block or log-and-permit.	Select Log and Permit. The default action is Log and Permit.
Timeout	Specifies that if the time taken to scan exceeds the timeout setting in the Web filtering profile, the processing is aborted and the content is passed or blocked without completing filtering.	Select Log and Permit. The default action is Log and Permit.

Table 208: Default configuration option page (continued)

Field	Function	Action
Too-many-requests	Specifies that if the total number of messages received concurrently exceeds the device limits, the content is passed or blocked depending on the too-many-request fallback option. The available actions are block or log-and-permit.	Select Log and Permit. The default action is Log and Permit.
Category	<p>Specifies a unique customized list of categories.</p> <ul style="list-style-type: none"> • Add (+)—Adds the selected category and the corresponding action to the list of available categories for the Juniper Enhanced Web Filtering profile. • Delete(X)—Deletes the selected category from the list of available categories for the Juniper Enhanced Web Filtering profile. 	Select a category from the list.
Action	Specifies the action that the device must take for the category selected.	Select Permit, Log and Permit, or Block.
Quarantine Message		
Type	Specify type of quarantine message desired.	Select a type.
URL	URL of quarantine message.	Enter a valid URL.
Server		
Host	Specifies the address of the host server.	Enter the address of the host server.
Port	Specifies the port number of the server.	Enter the port number of the server.
Routing Instance	Specify the routing instance name.	Select a routing instance.
Proxy Profile	Specify the proxy profile for Web filtering.	Create a Proxy profile

Table 208: Default configuration option page (continued)

Field	Function	Action
Site Reputation Action	Specify the action to be taken depending on the site reputation returned for all types of URLs whether it is categorized or uncategorized.	<p>Displays the following options:</p> <ul style="list-style-type: none"> • Very Safe— Permit, log-and-permit, block, or quarantine a request if a site-reputation of 90 through 100 is returned. • Moderately Safe— Permit, log-and-permit, block, or quarantine a request if a site-reputation of 80 through 89 is returned. • Fairly Safe— Permit, log-and-permit, block, or quarantine a request if a site-reputation of 70 through 79 is returned. • Suspicious— Permit, log-and-permit, block, or quarantine a request if a site-reputation of 60 through 69 is returned. • Harmful— Permit, log-and-permit, block, or quarantine a request if a site-reputation of zero through 59 is returned. <p>Click Reset to position the slider to the recommended levels.</p>
Juniper Local	Specify the Local profile type.	Select this option to use the Local profile type.
Websense Redirect		
Account	Displays the user account for which this profile is intended.	
Sockets	Displays the number of sockets used for communicating between the client and server.	Enter the number of sockets.
Delete All Default Configurations	Deletes all the configurations	-
Create Anti-Spam		
Address Whitelist	Specifies the comprehensive list of MIME types that can bypass antivirus scanning.	Select the customized object from the list.
Address Blacklist	Specifies a list of MIME types to be excluded from the whitelist. The exception MIME whitelist is a subset of MIME types found in the MIME whitelist.	Select the customized object from the list.
Type	Specify the antispam type.	—
SBL settings		

Table 208: Default configuration option page (continued)

Field	Function	Action
Custom Tag String	Specifies the custom string that is used to identify a spam message.	Enter a custom string for identifying a message as spam. By default the devices uses ***SPAM***
SBL Default Server	Specifies the profile that uses SBL server. The SBL server is predefined on the device.	Select the check box if you are using the default server.
Spam Action	Displays the Spam action.	Select any one from the action. <ul style="list-style-type: none"> • Block Email • Tag header email • Tag subject email.
Create Content Filtering Click one: <ul style="list-style-type: none"> • Expand/Collapse- All • Edit- Edits the options. • Delete- Delete the option. 		
Permit Command List	Displays the permitted protocol command name.	Select the protocol command name to be permitted from the list.
Block Command List	Displays the blocked protocol command.	Select the protocol command name to be blocked from the list.
Block Extension List	Specifies the blocked extension list name.	Select the extension to be blocked from the list.
Block MIME List	Specifies the blocked MIME.	Select the MIME type from the list.
Block MIME Exception List	Specifies the blocked MIME list.	Select the MIME type to be excluded from the list.
Type	Specifies the content filtering type.	Select the type.
Block Content Type	Specifies the blocked content type. <ul style="list-style-type: none"> • activex • exe • http-cookie • java-applet • zip 	Select the content type to be blocked.
Notification Options		
Type	Specifies the type of notification sent when a content block is triggered.	Select the Protocol Only or the Message check box.


Table 208: Default configuration option page (continued)

Field	Function	Action
Notify Mail Sender	Specifies that when a virus is detected and a content block is triggered, an e-mail is sent to the administrator.	Select the Notify Mail Sender check box.
Custom Notification Message	Specifies the customized message text for the content-block notification.	Enter the text for this custom notification message (if you are using one).

- See Also**
- [Web Filtering Configuration Page Options on page 353](#)
 - [Antispam Configuration Page Options on page 364](#)
 - [Content Filtering Configuration Page Options on page 366](#)
 - [Custom Objects Configuration Page Options on page 368](#)

Antivirus Configuration Page Options

1. Select **Configure>Security>UTM>Anti-Virus** in the J-Web user interface.
The Antivirus configuration page appears. [Table 209 on page 346](#) explains the contents of this page.
2. Click one:
 - **Global Options**—Defines general specifications for antivirus configuration. Enter information as specified in [Table 210 on page 347](#).



NOTE: Global Options are NOT enabled for logical systems users. It is enabled only for root users.

 - **Add or +**—Adds a new or duplicate antivirus profile configuration. Enter information as specified in [Table 211 on page 349](#).
 - **Edit or /**—Edits the selected antivirus configuration.
 - **Delete or X**—Deletes the selected antivirus configuration.
3. Click one:
 - **OK**—Saves the configuration and returns to the main configuration page.
 - **Cancel**—Cancels your entries and returns to the main configuration page.

Table 209: Antivirus Configuration Page

Field	Function
Profile Name	Displays the unique name of the antispam profile.
Profile Type	Displays the profile type selected.

Table 209: Antivirus Configuration Page (continued)

Field	Function
Intelligent Prescreening	Displays the intelligent prescreening status.
Scan Mode	Displays the scan mode option selected.
Trickling Timeout	Displays the trickling timeout interval.

Table 210: Global Options Antivirus Configuration Details

Field	Function	Action
Main		
MIME Whitelist	Specifies the comprehensive list of MIME types that can bypass antivirus scanning.	Select the customized object from the list.
Exception MIME Whitelist	Specifies a list of MIME types to be excluded from the whitelist. The exception MIME whitelist is a subset of MIME types found in the MIME whitelist.	Select the customized object from the list.
URL Whitelist	Specifies a unique customized list of all URLs or IP addresses for a given category that are to be bypassed for scanning.	Select the customized object from the list.
Engine Type		
Kaspersky Lab	Specifies the internal scan engine for full antivirus protection provided by Kaspersky Labs. NOTE: This option is not supported on SRX1500 devices.	Select this option to choose the Kaspersky Lab engine type.
Juniper Express	Specifies the internal scan engine for full antivirus protection provided by Juniper Networks. NOTE: This option is not supported on SRX1500 devices.	Select this option to choose the Juniper Express engine type.
Sophos	Specifies the internal scan engine for full antivirus protection provided by Sophos. NOTE: SRX1500 devices support only this option.	Select this option to choose the Sophos engine type.
Kaspersky Lab Engine Options		
Admin Email	Specifies the e-mail address for the notification to be sent to the administrator when the pattern update is complete.	Enter the administrator e-mail address.

Table 210: Global Options Antivirus Configuration Details (continued)

Field	Function	Action
Custom Message	Specifies the text of the pattern-update e-mail notification that is sent when the pattern update is complete.	Enter the customized message.
Custom Message Subject	Specifies the customized message subject line for the custom message.	Enter the customized message subject line.
Juniper Express Engine Options		
Pattern Update URL	Specifies the URL of the database server.	Enter the URL for the pattern database.
Pattern Update Interval (sec)	Specifies the interval at which the database server is queried for a new version of the database.	Enter the time interval for automatically updating the pattern database. The range is from 10 through 10080 seconds. The default interval is 60 seconds.
Auto Update	Specifies that the antivirus pattern database is configured to be automatically updated.	Select the auto update option.
No Auto Update	Specifies that the automatic download and update of the antivirus engine and signature database are disabled.	Select the no auto update option.
Sophos Engine Options		
Pattern Update URL	Specifies the URL of the database server.	Enter the URL for the pattern database.
Pattern Update Interval (sec)	Specifies the interval at which the database server is queried for a new version of the database.	Enter the time interval for automatically updating the pattern database. The range is from 10 through 10080 seconds. The default interval is 60 seconds.
Auto Update	Specifies that the antivirus pattern database is configured to be automatically updated.	Select the auto update option.
No Auto Update	Specifies that the automatic download and update of the antivirus engine and signature database are disabled.	Select the no auto update option.
Proxy Options		
Proxy Server Host	Specifies the host name of the proxy server.	Enter the IP address or hostname of the proxy server.
Proxy Server Port	Specifies the port with which the proxy server is associated.	Enter the port number.
Proxy Server Username	Specifies the username to use on the proxy server.	Enter the username.
Proxy Server Password	Specifies the password to use on the proxy server.	Enter the password.

Table 210: Global Options Antivirus Configuration Details (continued)

Field	Function	Action
Confirm Proxy Server Password	Verifies the login password for the proxy server.	Re-enter the password.

Table 211: Add Antivirus Configuration Details

Field	Function	Action
Main		
Profile Name	Specifies a unique name for the antivirus profile.	Enter a unique name for the antispyware profile.
Profile Type	Displays the internal scan engine for full antivirus option selected in the global options. Intelligent prescreening is only intended for use with non-encoded traffic.	-
Trickle Timeout	Specifies the trickle timeout value.	Enter timeout parameters.
Scan Options for Kaspersky Lab Engine		
Intelligent Prescreening	Specifies the antivirus module used to begin scanning a file and improves antivirus scanning performance. The antivirus module generally begins to scan data after the gateway device has received all the packets of a file.	Select yes to enable intelligent prescreening.
Content Size Limit	Specifies the accumulated TCP payload size.	Enter the content size limit, a value from 20 through 20000 KB.
Scan Engine Timeout	Specifies the timeframe between the scan request generated to the scan result returned by the scan engine. Tricking timeout value is used by all supported protocols. Each protocol can have a different timeout value.	Enter the time interval from 1 through 1800 seconds. The default value is 180 seconds.
Decompress Layer Limit	Specifies the number of layers of nested compressed files the internal antivirus scanner can decompress before the execution of the virus scan.	Enter the decompress layer limit, a value from 1 through 4 layers.
Scan Mode		
Scan All Files	Specifies all files to be scanned.	Select this option to scan all files.
Scan Files With Specified Extension	Specifies the list of file extensions.	Select this option to scan files with specific extensions.
Scan Engine Filename Extension	Specifies the file extensions found in the traffic being scanned.	Select this option to scan the engine filename extension.
Scan Options for Juniper Express Engine		

Table 211: Add Antivirus Configuration Details (continued)

Field	Function	Action
Intelligent Prescreening	Specifies the antivirus module used to begin scanning a file and improves antivirus scanning performance. The antivirus module generally begins to scan data after the gateway device has received all the packets of a file.	Select yes to enable intelligent prescreening.
Content Size Limit	Specifies the accumulated TCP payload size.	Enter the content size limit, a value from 20 through 20,000 KB.
Scan Engine Timeout	Specifies the timeframe between the scan request generated to the scan result returned by the scan engine. Trickling timeout value is used by all supported protocols. Each protocol can have a different timeout value.	Enter the time interval from 1 through 1800 seconds. The default value is 180 seconds.
Scan Options for Sophos Engine		
URI Check	Specifies Uniform Resource Identifier blocking: an effective measure for preventing malware from reaching the endpoint. URI lookup is performed against an in-the-cloud malicious/infected URI database on each URI requested via HTTP.	Select the URI check check box to enable URI check.
Content Size Limit	Specifies the accumulated TCP payload size.	Enter the content size limit, a value from 20 through 20,000 KB.
Scan Engine Timeout	Specifies the timeframe between the scan request generated to the scan result returned by the scan engine. Trickling timeout value is used by all supported protocols. Each protocol can have a different timeout value.	Enter the time interval from 1 through 1800 seconds. The default value is 180 seconds.
Query Interval	Specifies the antivirus engine query timeout interval.	Enter the query interval from 1 through 5 seconds.
Query Retries	Specifies the antivirus engine query retry (number of times) value.	Enter the query retry value from 0 through 5.
Fallback Settings		
Default Action	Specifies all errors other than the categorized settings. This could include either unhandled system exceptions (internal errors) or other unknown errors. The available actions are block or log-and-permit.	Select Log and Permit . The default action is Block .
Corrupt File	Specifies the error returned by the scan engine when it detects a corrupted file. The available actions are block or log-and-permit.	Select Log and Permit . The default action is Block .

Table 211: Add Antivirus Configuration Details (continued)

Field	Function	Action
Password File	Specifies the error returned by the scan engine when the scanned file is protected by a password. The available actions are block or log-and-permit.	Select Log and Permit . The default action is Block .
Decompress Layer	Specifies the error returned by the scan engine when the scanned file has too many compression layers. The available actions are block or log-and-permit.	Select Log and Permit . The default action is Block .
Content Size	Specifies that if the content size exceeds a set limit, the content is passed or blocked depending on the max-content-size fallback option. The available actions are block or log-and-permit.	Select Log and Permit . The default action is Block .
Engine Not Ready	Specifies that the scan engine is not ready during certain processes, for example, while the signature database is loading. The available actions are block or log-and-permit.	Select Log and Permit . The default action is Block .
Timeout	Specifies that if the time taken to scan exceeds the timeout setting in the antivirus profile, the processing is aborted and the content is passed or blocked without completing the virus checking. The decision is made based on the timeout fallback option. The available actions are block or log-and-permit.	Select Log and Permit . The default action is Block .
Out Of Resource	Specifies the resource constraints error received during virus scanning. This error can be or by the can be sent by the scan engine (as a scan-code) or scan manager. When the system is out of resources occurs, scanning is aborted. The available actions are block or log-and-permit.	Select Log and Permit . The default action is Block .
Too Many Requests	Specifies that if the total number of messages received concurrently exceeds the device limits, the content is passed or blocked depending on the too-many-request fallback option. The available actions are block or log-and-permit.	Select Log and Permit . The default action is Block . The allowed request limit is not configurable.
Notification Options		
Fallback Block		
Notification Type	Specifies the type of notification sent when a fallback option of block is triggered.	Select the Protocol Only or the Message check box.
Notify Mail Sender	Specifies that when a virus is detected and a fallback option of block is triggered, an e-mail is sent to the administrator.	Select the Notify Mail Sender check box to enable this notification.

Table 211: Add Antivirus Configuration Details (continued)

Field	Function	Action
Custom Message	Specifies the customized message text for the fallback block notification.	Enter the text for this custom notification message (if you are using one).
Custom Message Subject	Specifies the subject line text for your custom message for the fallback block notification.	Enter the subject line text for your custom message.
Display Hostname	Specifies the device name.	Select the check box to display the hostname.
Allow Email	Specifies that a notification e-mail address must be allowed.	Select the check box to allow e-mail.
Administrator Email Address	Specifies the administrator e-mail address where notification is sent when a fallback error occurs.	Enter the administrator e-mail address.
Fallback Nonblock		
Notify Mail Recipient	Specifies that the fallback nonblock notification is sent when a fallback e-mail option without a blocking action is triggered.	Select the Notify Mail Sender check box.
Custom Message	Specifies the customized message text for the fallback nonblock notification.	Enter the text for this custom notification message (if you are using one).
Custom Message Subject	Specifies the subject line for your custom message for the fallback nonblock notification.	Enter the subject line text for your custom message.
Virus Detection		
Notification Type	Specifies the type of notification to be sent when a virus is detected.	Select Protocol Only or Message option.
Notify Mail Sender	Specifies whether or not a notification is sent to the virus-detection notification e-mail address when a virus is detected.	Select yes to send a notification and no to not send a notification.
Custom Message	Specifies the customized message text for the virus detection notification.	Enter the text for this custom notification message (if you are using one).
Custom Message Subject	Specifies the subject line text for your custom message for the virus detection notification.	Enter the subject line text for your custom message.

- See Also**
- [Web Filtering Configuration Page Options on page 353](#)
 - [Antispam Configuration Page Options on page 364](#)
 - [Content Filtering Configuration Page Options on page 366](#)
 - [Custom Objects Configuration Page Options on page 368](#)

Web Filtering Configuration Page Options

1. Select **Configure>Security>UTM>Web Filtering** in the J-Web user interface to display the Web Filtering configuration page.

The Web Filtering configuration page appears, [Table 212 on page 358](#) explains the contents of this page.

2. Click one:

- **Global Options**—Defines general specifications for a Web filtering configuration. Enter information as specified in [Table 213 on page 358](#).



NOTE: Global Options are not enabled for logical systems users. It is enabled only for root users.

- **Add or +**—Adds a new or duplicate Web filtering configuration. Enter information as specified in [Table 214 on page 359](#).
- **Edit or /**—Edits the selected Web filtering configuration.
- **Delete or X**—Deletes the selected Web filtering configuration.

3. Click one:

- **OK**—Saves the configuration and returns to the main configuration page.
- **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
- **Cancel**—Cancels your entries and returns to the main configuration page.

To configure Web filtering using the J-Web Configuration editor, if you are using custom objects, you must create the custom objects (URL pattern list, custom URL category list).



NOTE: In addition to custom object lists, you can use included default lists and whitelist and blacklist categories.

Configure a URL Pattern List Custom Object as follows:



NOTE: Because you use URL pattern lists to create custom URL category lists, you must configure URL pattern list custom objects before you configure a custom URL category list.

1. Select **Configure>Security>UTM>Custom Objects**.
2. From the **URL Pattern List** tab, click **Add** to create URL pattern lists.

3. Next to URL Pattern Name, enter a unique name for the list you are creating. This name appears in the Custom URL Category List Custom Object page for selection.
4. Next to URL Pattern Value, enter the URL or IP address that you want to add to list for bypassing scanning.



NOTE: URL pattern wildcard support—The wildcard rule is as follows: `*\.[]\?*` and you must precede all wildcard URLs with `http://`. You can only use “*” if it is at the beginning of the URL and is followed by a “.”. You can only use “?” at the end of the URL.

The following wildcard syntax is supported: `http://*juniper.net`, `http://www.juniper.ne?`, `http://www.juniper.n??`. The following wildcard syntax is not supported: `*juniper.net`, `www.juniper.ne?`, `http://*juniper.net`, `http://*`.

5. Click **Add** to add your URL pattern to the Values list box.

The list can contain up to 8192 items. You can also select an entry and use the Delete button to delete it from the list. Continue to add URLs or IP addresses in this manner.

6. Click **OK** to save the selected values as part of the URL pattern list you have created.
7. If the configuration item is saved successfully, you receive a confirmation. Click **OK**. If it is not saved successfully, you can click **Details** in the pop-up window that appears to discover why.

Configure a custom URL category list custom object as follows:



NOTE: Because you use URL pattern lists to create custom URL category lists, you must configure URL pattern list custom objects before you configure a custom URL category list.

1. Select **Configure>Security>UTM>Custom Objects**.
2. From the **URL Category List** tab, click **Add** to create URL category lists.
3. Next to URL Category Name, enter a unique name for the list you are creating. This name appears in the URL Whitelist, Blacklist, and Custom Category lists when you configure Web filtering global options.
4. In the Available Values box, select a URL Pattern List name from the list for bypassing scanning, and click the right arrow button to move it to the Selected Values box.
5. Click **OK** to save the selected values as part of the custom URL list you have created.
6. If the configuration item is saved successfully, you receive a confirmation. Click **OK**. If it is not saved successfully, you can click **Details** in the pop-up window that appears to discover why.

Now that your custom objects have been created, you can configure the integrated Web filtering feature profile.



NOTE: The below steps use Surf Control Web filtering type. SRX1500 devices do not support Surf Control Integrated option. Hence replace Surf Control with Websense.

1. Select **Configure>Security>UTM>Global options**.
2. In the **Web Filtering**, next to URL whitelist, select the Custom URL list you created from the available options.

This is the first filtering category that both integrated and redirect Web filtering use. If there is no match, the URL is sent to the SurfControl server.



NOTE: The SurfControl option is not supported on SRX1500 devices. For SRX1500 devices, the URL is sent to the Websense server.

3. Next to URL blacklist, select the Custom URL list that you have created from the list.
This is the first filtering category that both integrated and redirect Web filtering use. If there is no match, the URL is sent to the SurfControl server.
4. In the Filtering Type section, select the type of Web filtering engine you are using.
In this case, you would select **Surf Control Integrated**.
5. In the SurfControl Integrated options section, next to Cache timeout, enter a timeout limit, in minutes, for expiring cache entries (24 hours is the default and the maximum allowed life span).
6. Next to Cache Size, enter a size limit, in kilobytes, for the cache (500 KB is the default).
7. Next to Server Host, enter the Surf Control server name or IP address.
8. Next to Server Port, enter the port number for communicating with the Surf Control server (default ports are 80, 8080, and 8081).
9. Click **OK** to save these values.
10. If the configuration item is saved successfully, you receive a confirmation. Click **OK**. If it is not saved successfully, you can click **Details** in the pop-up window that appears to discover why.
11. Select **Web Filtering**, under UTM, in the left pane.
12. In Web filtering Profiles Configuration, click **Add** to create a profile for Surf Control Integrated Web filtering. (To edit an existing item, select it and click **Edit**.)
13. In Profile name, enter a unique name for this Web filtering profile.
14. Select the Profile Type. In this case, select **Surf Control**.
15. Next to Default action, select **Permit**, **Log and permit**, or **Block**.

This is the default action for this profile for requests that shows errors.

16. Next to Custom Block Message, enter a custom message to be sent when HTTP requests are blocked.
17. Next to Timeout, enter a value in seconds.
Once this limit is reached, fail mode settings are applied. The default limit here is 10 seconds. You can enter a value from 10 to 240 seconds.
18. Next to Custom block message subject, enter text to appear in the subject line of your custom message for this block notification.
19. Select the **Fallback** options tab.
20. Next to Default, select **Log** and **Permit** or **Block** as the action to occur when a request fails for any reason not specifically called out.
21. Next to Server Connectivity, select **Log** and **Permit** or **Block** as the action to occur when a request fails for this reason.
22. Next to Timeout, select **Log** and **Permit** or **Block** as the action to occur when a request fails for this reason.
23. Next to Too Many Requests, select **Log** and **Permit** or **Block** as the action to occur when a request fails for this reason.
24. Click **Save**.
25. Select **Custom Objects**, under UTM, in the left pane.
26. Select the **URL category list** tab.
27. In the custom URL category list section, click **Add** to use a configured custom URL category list custom object in the profile.
28. Next to Categories, select a configured custom object from the list.
29. Next to Actions, select **Permit**, **Block**, or **Log** and **Permit** from the list.
30. Click **Add**.
31. Click **OK**.
32. If the configuration item is saved successfully, you receive a confirmation. Click **OK**. If it is not saved successfully, click **Details** in the pop-up window that appears to discover why.



NOTE: Next, you configure a UTM policy for Web filtering to which you attach the content filtering profile you have configured.

1. Select **Configure>Security>Policy>UTM Policies**.
2. From the UTM policy configuration window, click **Add** to configure a UTM policy.
The policy configuration pop-up window appears.
3. Select the **Main** tab in pop-up window.
4. In the Policy Name box, enter a unique name for the UTM policy that you create.

5. In the Session per client limit box, enter a session per client limit from 0 to 20000 for this UTM policy.
6. For Session per client over limit, select one of the following: **Log** and **Permit** or **Block**. This is the action the device takes when the session per client limit for this UTM policy is exceeded.
7. Select the **Web Filtering profiles** tab in the pop-up window.
8. Next to HTTP profile, select the profile you have configured from the list.
9. Click **OK**.
10. If the policy is saved successfully, you receive a confirmation. Click **OK**. If the profile is not saved successfully, click **Details** in the pop-up window that appears to discover why.



NOTE: Next, you attach the UTM policy to a security policy that you create.

1. Select **Configure>Security>Policy>FW Policies**.
2. From the Security Policy window, click **Add** to configure a security policy with UTM. The policy configuration pop-up window appears.
3. In the **Policy** tab, enter a name in the Policy Name box.
4. Next to **From Zone**, select a zone from the list.
5. Next to **To Zone**, select a zone from the list.
6. Choose a **Source Address**.
7. Choose a **Destination Address**.
8. Choose an **Application**. Do this by selecting junos-<protocol> (for all protocols that support Web filtering, http in this case) in the Application Sets box and click the —> button to move them to the Matched box.
9. Next to Policy Action, select one of the following: **Permit**, **Deny**, or **Reject**.



NOTE: When you select Permit for Policy Action, several additional fields become available in the Applications Services tab, including UTM Policy.

10. Select the **Application Services** tab in the pop-up window.
11. Next to UTM Policy, select the appropriate policy from the list. This attaches your UTM policy to the security policy.



NOTE: There are several fields on this page that are not described in this section. See the section on Security Policies for detailed information on configuring security policies and all the available fields.

12. Click **OK**.
13. If the policy is saved successfully, you receive a confirmation. Click **OK**. If the profile is not saved successfully, you can click **Details** in the pop-up window that appears to discover why.

Table 212: Web Filtering Configuration Page

Field	Function
Profile Name	Displays the unique name of the antispyam profile.
Profile Type	Displays the profile type selected.
Account	Displays the user account for which this profile is intended.
Server	Displays the server name.
Timeout	Displays the timeout interval.

Table 213: Global Options Web Filtering Configuration Details

Field	Function	Action
URL Whitelist	Specifies a unique customized list of all URLs or IP addresses for a given category that are to be bypassed for scanning.	Select the customized object from the list.
URL Blacklist	Specifies a unique customized list of all URLs or IP addresses for a given category that are scanned for blacklisting.	Select the customized object from the list.
Filtering Type		
Surf Control Integrated	Specifies that the Surf Control CPA server intercepts every HTTP request in a TCP connection. The decision making is done on the device after it identifies a category for a URL either from user-defined categories or from the Surf Control category server. NOTE: This option is not supported on SRX1500 devices.	Select this option to choose this type of Web filtering engine.
Websense Redirect	Specifies that the Web filtering module intercepts an HTTP request. The URL in the request is then sent to the external Websense server which makes a permit or a deny decision.	Select this option to choose this type of Web filtering engine.
Local	Specifies that the Web filtering module intercepts URLs and makes a permit/deny decision locally.	Select this option to choose this type of Web filtering engine.

Table 213: Global Options Web Filtering Configuration Details (continued)

Field	Function	Action
Juniper Enhanced	Specifies that the Juniper Enhanced Web filtering intercepts the HTTP and the HTTPS requests and sends the HTTP URL or the HTTPS source IP to the Websense ThreatSeeker Cloud (TSC).	Select this option to choose this type of Web filtering engine. The Juniper Enhanced Options with the respective parameters is displayed.
Juniper Enhanced Options The following options are displayed only if you have selected <i>Juniper Enhanced</i> as the <i>Filtering type</i> .		
Cache timeout (mins)	Specifies the time interval to wait before the cache is cleared.	Enter or select the time using the up/down arrow.
Cache size (kb)	Specifies the size of the cache memory that must be provisioned.	Enter the size of cache to be provisioned in kilobytes. You can also select a size using the up/down arrow.
Server host	Specifies the address of the host server.	Enter the address of the host server.
Server port	Specifies the port number of the server that is used for communication.	Enter the port number or select using the up/down arrow.
Reputation Level	Specifies the level at which the device must take appropriate action (permit, log and permit, or block) when the site reputation level reaches the level that you have defined.	Move each of the four sliders to the desired level or number. Each slider is named (A to D) and represents the following degree of assessment along with the recommended range. A: Very Safe (90 to 100) B: Moderately Safe (80-89) C: Fairly Safe (70-79) D: Suspicious (58-69) E: Harmful (1-57). This is not represented as a slider. Click Reset to position the slider to the recommended levels.

Table 214: Add Web Filtering Configuration Details

Field	Function	Action
Main		
Profile Name	Displays the unique name of the Web filtering profile.	Enter a unique name for the Web filtering profile. NOTE: The profile Name should not be longer than 29 characters.

Table 214: Add Web Filtering Configuration Details (continued)

Field	Function	Action
Main		
Profile Type	<p>Displays the profile type based on the Filtering Type selected. The options available are:</p> <ul style="list-style-type: none"> • Websense—Select this option to use the Websense profile type. • Surf Control—Select this option to use Surf Control profile type. • Local—Select this option to use the Local profile type. • Juniper-Enhanced—Select this option to use the Juniper-enhanced profile type. 	Select an option.
Account	Displays the user account for which this profile is intended.	Enter a user account name.
Server	Displays the server name.	Enter the server name.
Port	Displays the port number used to communicate with the server.	Enter the port number.
Sockets	Displays the number of sockets used for communicating between the client and server.	Enter the number of sockets.
Default Action	<p>Displays the default action to be taken for Web filtering. The options available are:</p> <ul style="list-style-type: none"> • Permit—Permits access to content. • Log and Permit—Logs details of the URL and permits access to content. • Block—Blocks access to content. 	Select an option.
Timeout	Specifies the time interval to wait before the connection to the server is closed.	Type the interval in seconds.
Safe Search	<p>Displays the search results based on the option selected.</p> <p>A safe-search solution is used to ensure that the embedded objects such as images on the URLs received from the search engines are safe and that no undesirable content is returned to the client.</p> <p>Safe-search is applicable to juniper-enhanced Web filtering type only.</p>	Select this option to choose this type of search.
No Safe Search	Specifies not to perform safe-search for Juniper enhanced protocol.	Select this option to choose this type of search.

Table 214: Add Web Filtering Configuration Details (continued)

Field	Function	Action
Main		
Base Filter	Specifies the base filter that is attached to the profile. All categories has a default action in a base filter. For categories that are not configured in the profile, the base filter is considered for action.	Select the base filter from the drop down list.
Custom Block Message	Specifies the customized block message to be displayed when content is blocked.	Enter a message to be displayed when content is blocked.
<p>NOTE: The fields Account, Server, Port, and Sockets are displayed only when you select Websense-Redirect filtering type on the Global Configuration page.</p>		
Fallback Options		
Default	Specifies all errors other than the categorized settings. These could include either unhandled system exceptions (internal errors) or other unknown errors. The available actions are block or log-and-permit.	Select Log and Permit . The default action is Log and Permit.
Server Connectivity	Specifies that the server connection is not established during certain processes, for example, while the signature database is loading. The available actions are block or log-and-permit.	Select Log and Permit . The default action is Log and Permit.
Timeout	Specifies that if the time taken to scan exceeds the timeout setting in the Web filtering profile, the processing is aborted and the content is passed or blocked without completing filtering. The decision is made based on the timeout fallback option. The available actions are block or log-and-permit.	Select Log and Permit . The default action is Log and Permit.
Too Many Requests	Specifies that if the total number of messages received concurrently exceeds the device limits, the content is passed or blocked depending on the too-many-request fallback option. The available actions are block or log-and-permit.	Select Log and Permit . The default action is Log and Permit.
Site Reputation Action		
Very Safe	Specifies that the device must take appropriate action (permit, log and permit, or block) if the site reputation reaches the % score that is defined by you. If you have not defined the percentage, the default score is 90 through 100.	<p>Enter the percentage value in the % field.</p> <p>Select Permit, Log and Permit, or Block.</p>

Table 214: Add Web Filtering Configuration Details (continued)

Field	Function	Action
Main		
Moderately Safe	Specifies that the device must take appropriate action (permit, log and permit, or block) if the site reputation reaches the % score that is defined by you. If you have not defined the percentage, the default score is 80 through 89.	Enter the percentage value in the % field. Select Permit , Log and Permit , or Block .
Fairly Safe	Specifies that the device must take appropriate action (permit, log and permit, or block) if the site reputation reaches the % score that is defined by you. If you have not defined the percentage, the default score is 70 through 79.	Enter the percentage value in the % field. Select Permit , Log and Permit , or Block .
Suspicious	Specifies that the device must take appropriate action (permit, log and permit, or block) if the site reputation reaches the % score that is defined by you. If you have not defined the percentage, the default score is 60 through 69.	Enter the percentage value in the % field. Select Permit , Log and Permit , or Block .
Harmful	Specifies that the device must take appropriate action (permit, log and permit, or block) if the site reputation reaches the % score that is defined by you. If you have not defined the percentage, the default score is 0 through 59.	Enter the percentage value in the % field. Select Permit or Log and Permit , or Block .
URL Category Action List		
Categories	Specifies a unique customized list of categories. <ul style="list-style-type: none"> • Add—Adds the selected category and the corresponding action to the list of available categories for the Juniper Enhanced Web Filtering profile. • Delete—Deletes the selected category from the list of available categories for the Juniper Enhanced Web Filtering profile. 	Select a category from the list.
Action	Specifies the action that the device must take for the category selected.	Select Permit , Log and Permit , or Block .

- See Also**
- [Antivirus Configuration Page Options on page 346](#)
 - [Antispam Configuration Page Options on page 364](#)
 - [Content Filtering Configuration Page Options on page 366](#)
 - [Custom Objects Configuration Page Options on page 368](#)

Category Update Configuration Page Options

The Category Update page enables you to download and install a new Juniper Enhanced Web Filtering category. You can either set for an automatic download or perform a manual download and installation of the new category. You can also check for the latest version of categories available or uninstall an existing category.

1. Select **Configure>Security>UTM>Category Update** in the J-Web user interface to display the UTM category installed or to download and install a new UTM category.

The Category Update page appears.

The number of installed version is displayed in the left top corner of the page. Next to it, the download and installation status is displayed when you download and install a profile.

2. Click one:

- **Install**—Installs the already downloaded category.
- **Uninstall**—Enables you to uninstall the existing category. Uninstall link appears only when there is an installed version.



NOTE: You cannot uninstall the category that is being used in web filtering profiles.

You cannot uninstall a category if its base filters are being used in web filtering profiles.

You cannot Install or uninstall if a commit is pending.

- **Check Latest**—Opens a new browser page and displays the latest list of EWF category files.
 - **Download**—Enables you to download and install the latest Juniper Enhanced Web Filtering (EWF) category file. See [Table 215 on page 364](#) for available options.
 - **Search icon**—Enables you to search a category by name by using the search icon in the installed version row or by base filter by using the search icon in the Base Filters band.
3. Click one:
 - **OK**—Saves the configuration and returns to the main configuration page.
 - **Cancel**—Cancels your entries and returns to the main configuration page.
 - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.

Table 215: Category Download Options

Field	Function
Download	<p>Click Download. The Manually Download window opens and displays the available versions. You can check the available version by clicking the URL.</p> <p>Version - You can choose the latest version or select the version number which you want to download.</p>
Download and Install	<p>Click Download and Install. The Manually Download and Install window opens and displays the available versions. You can check the available version by clicking the URL.</p> <p>Version - You can choose the latest version or select the version number which you want to download and install.</p>
Auto Download and Install	<p>Click Auto Download and Install to enable J-Web to automatically detect for newer version of UTM category, download if found, and install it on your device. The Auto Download Settings window is displayed.</p> <p>Select Download On to enter the following details.</p> <ul style="list-style-type: none"> • URL—URL from where you download the category. • Interval time—Time period to download and check install category file. • Start time—Start date and time to initiate automatic download and installation process. <p>Select Download Off to turn off the Auto Download and Install feature.</p>

Category Name—Lists the category names that are installed. UTM EWF License is required for installing the categories. You can launch License Management from this page, if there is no license installed. Once license is installed, initially the default Web Filtering Categories that comes with the software is displayed.

Base Filters—Lists the categories for the selected base filter. By default no base filters are listed. Base filters are listed once the categories are downloaded and installed on the device.

- See Also**
- [Antivirus Configuration Page Options on page 346](#)
 - [Antispam Configuration Page Options on page 364](#)
 - [Content Filtering Configuration Page Options on page 366](#)
 - [Custom Objects Configuration Page Options on page 368](#)

Antispam Configuration Page Options

1. Select **Configure>Security>UTM>Anti-Spam**.

The Antispam configuration page appears. [Table 216 on page 365](#) explains the contents of this page.

2. Click one:

- **Global Options**—Defines general specifications for antispam configuration. Enter information as specified in [Table 217 on page 365](#).
- **Add or +**—Adds a new or duplicate antispam profile configuration. Enter information as specified in [Table 218 on page 365](#).
- **Edit or /**—Edits the selected antispam configuration.
- **Delete or X**—Deletes the selected antispam configuration.

3. Click one:

- **OK**—Saves the configuration and returns to the main configuration page.
- **Cancel**—Cancels your entries and returns to the main configuration page.

Table 216: Antispam Configuration Page

Field	Function
Profile Name	Displays the unique name of the antispam profile.
Profile Type	Displays the profile type selected.
Custom Tag String	Displays the custom string used to identify a spam message.
Action	Displays the default action selected.

Table 217: Global Options Antispam Configuration Details

Field	Function	Action
Address Whitelist	Specifies the comprehensive list of MIME types that can bypass antivirus scanning.	Select the customized object from the list.
Address Blacklist	Specifies a list of MIME types to be excluded from the whitelist. The exception MIME whitelist is a subset of MIME types found in the MIME whitelist.	Select the customized object from the list.

Table 218: Add Antispam Configuration Details

Field	Function	Action
Main		
Profile Name	Specifies a unique name for the antivirus profile.	Enter a unique name for the antispam profile.

Table 218: Add Antispam Configuration Details (continued)

Field	Function	Action
Default SBL Server	Specifies the profile that uses SBL server. The SBL server is predefined on the device. It ships with the name and address of the Symantec SBL server preloaded. If you do not select this check box, you are disabling server-based spam filtering. Disable this function if you are using only local lists or if you do not have a license for server-based spam filtering.	Select the check box if you are using the default server.
Custom Tag String	Specifies the custom string that is used to identify a spam message.	Enter a custom string for identifying a message as spam. By default the devices uses ***SPAM*** .
Default Action	<p>Specifies the option to be taken when a spam message is detected. The options available are:</p> <ul style="list-style-type: none"> • Tag Subject—Adds the custom string at the beginning of the subject of the e-mail. • Block email—Blocks the spam e-mail. • Tag Header—Adds the custom string to the e-mail header. 	Select an option.

- See Also**
- [Antivirus Configuration Page Options on page 346](#)
 - [Web Filtering Configuration Page Options on page 353](#)
 - [Content Filtering Configuration Page Options on page 366](#)
 - [Custom Objects Configuration Page Options on page 368](#)

Content Filtering Configuration Page Options

1. Select **Configure>Security>UTM>Content Filtering**.

The Content Filtering configuration page appears. [Table 219 on page 367](#) explains the contents of this page.

2. Click one:
 - **Add** or **+**—Adds a new or duplicate content-filtering profile configuration. Enter information as specified in [Table 220 on page 367](#).
 - **Edit** or **/**—Edits the selected content-filtering configuration.
 - **Delete** or **X**—Deletes the selected content-filtering configuration.
3. Click one:
 - **OK**—Saves the configuration and returns to the main configuration page.
 - **Cancel**—Cancels your entries and returns to the main configuration page.

Table 219: Content Filtering Configuration Page

Field	Function
Profile Name	Displays the unique name of the antispam profile.
Permit Command List	Displays the permitted protocol command name.
Block Command List	Displays the blocked protocol command.
Notification Options Type	Displays the notification type opted.

Table 220: Add Content Filtering Configuration Details

Field	Function	Action
Main		
Profile Name	Specifies a unique name for the antivirus profile.	Enter a unique name for the antispam profile.
Permit Command List	Specifies the permitted protocol command.	Select the protocol command name to be permitted from the list.
Block Command List	Specifies the blocked protocol command name. By blocking certain commands, traffic can be controlled on the protocol command level.	Select the protocol command name to be blocked from the list.
Block Extension List	Specifies the blocked extension list name.	Select the extension to be blocked from the list.
Block MIME List	Specifies the blocked MIME.	Select the MIME type from the list.
Block MIME Exception List	Specifies the blocked MIME list.	Select the MIME type to be excluded from the list.
Block Content Type	Specifies the blocked content type.	Select the content type to be blocked.
Notification Options		
Notification Type	Specifies the type of notification sent when a content block is triggered.	Select the Protocol Only or the Message check box.
Notification Mail Sender	Specifies that when a virus is detected and a content block is triggered, an e-mail is sent to the administrator.	Select the Notify Mail Sender check box.
Custom Notification Message	Specifies the customized message text for the content-block notification.	Enter the text for this custom notification message (if you are using one).

- See Also**
- [Antivirus Configuration Page Options on page 346](#)
 - [Web Filtering Configuration Page Options on page 353](#)

- [Antispam Configuration Page Options on page 364](#)
- [Custom Objects Configuration Page Options on page 368](#)

Custom Objects Configuration Page Options

1. Select **Configure>Security>UTM>Custom Objects**.

The Custom Objects configuration page appears. [Table 221 on page 368](#) explains the contents of this page.

2. Click one:

- **Add** or **+**—Adds a new or duplicate custom objects configuration. Enter information as specified in [Table 222 on page 369](#).
- **Edit** or **/**—Edits the selected custom objects configuration.
- **Delete** or **X**—Deletes the selected custom objects configuration.

3. Click one:

- **OK**—Saves the configuration and returns to the main configuration page.
- **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
- **Cancel**—Cancels your entries and returns to the main configuration page.

Table 221: Custom Objects Configuration Page

Field	Function
MIME Pattern List	
Name	Displays the user-defined name or a predefined MIME pattern name.
Value	Displays the user-defined value or a predefined MIME pattern value.
Filename Extension List	
Name	Displays the user-defined name or a predefined file extension name.
Value	Displays the user-defined value or a predefined file extension value.
Protocol Command List	
Name	Displays only user-defined protocol command names.
Value	Displays only user-defined protocol command values.
URL Pattern List	

Table 221: Custom Objects Configuration Page (continued)

Field	Function
Name	Displays only user-defined URL pattern names.
Value	Displays only user-defined URL pattern values.
URL Category List	
Name	Displays only predefined URL categories.
Value	Displays only predefined URL categories from the SurfControl server. You can also configure URLs. The URLs configured in the URL pattern list are displayed here.
Custom Message List	
The Custom Message List displays the custom messages that you have created and the type of action it takes when Enables you to create block message or URL, or quarantine message or URL for each category.	
Name	Displays the name of the custom message that you have created.
Type	Displays the type of custom message. It is either Redirect-URL or User Message.
Content	Displays the content of the custom message. It is either a user message or an URL to be redirected to.

Table 222: Add Custom Objects Configuration Details

Field	Function	Action
MIME Pattern List		
Add MIME Pattern		
MIME Pattern Name	Displays the user-defined name or a predefined MIME pattern name.	Enter a MIME pattern name.
MIME Pattern Value	Displays the user-defined pattern value or a predefined MIME pattern value. The options available are: <ul style="list-style-type: none"> • Delete—Deletes the selected MIME pattern value. • Add—Adds the selected MIME pattern value. 	Select an option.
Filename Extension List		
Add File Extension		
File Extension Name	Displays the user-defined name or a predefined file extension name.	Enter a file extension name.

Table 222: Add Custom Objects Configuration Details (continued)

Field	Function	Action
Available Values	Displays the user-defined value or a predefined file extension value.	Select a value to associate it with the file extension name.
Protocol Command List		
Add Protocol Command		
Protocol Command Name	Displays only user-defined protocol command names.	Enter a protocol command name.
Protocol Command Value	Displays only user-defined protocol command values. The options available are: <ul style="list-style-type: none"> • Delete—Deletes the selected protocol command value. • Add—Adds the selected protocol command value. 	Select an option.
URL Pattern List		
Add URL Pattern		
URL Pattern Name	Displays only user-defined URL pattern names.	Enter a URL pattern name.
URL Pattern Value	Displays only user-defined URL pattern values. The options available are: <ul style="list-style-type: none"> • Delete—Deletes the selected URL pattern value. • Add—Adds the selected URL pattern value. 	Select an option.
URL Category List		
Add URL Category		
URL Category Name	Displays only predefined URL categories.	Enter a URL category name.
Available Values	Displays only predefined URL categories from the SurfControl server. You can also configure URLs. The URLs configured in the URL pattern list are displayed here.	Select a value to associate it with the URL category name.

- See Also**
- [Antivirus Configuration Page Options on page 346](#)
 - [Web Filtering Configuration Page Options on page 353](#)

- [Antispam Configuration Page Options on page 364](#)
- [Content Filtering Configuration Page Options on page 366](#)

UTM Policies Configuration Page Options

1. Select **Configure>Security>Policy>Define UTM Policy**.

The UTM policy configuration page appears. [Table 223 on page 371](#) explains the contents of this page.

2. Click one:

- **Add** or **+**—Adds a new or duplicate UTM policy configuration. Enter information as specified in [Table 224 on page 371](#).
- **Edit** or **/**—Edits the selected UTM policy configuration.
- **Delete** or **X**—Deletes the selected UTM policy configuration.

3. Click one:

- **OK**—Saves the configuration and returns to the main configuration page.
- **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
- **Cancel**—Cancels your entries and returns to the main configuration page.

Table 223: UTM Policy Configuration Page

Field	Function
UTM policy name	Displays the UTM policy name.
Anti-Virus	Displays the Anti-Virus profile.
Anti-Spam	Displays the Anti-Spam profile.
Web filtering	Displays the Web filtering profile.
Content filtering	Displays the content filtering profiles.

Table 224: Add UTM Policy Configuration Details

Field	Function	Action
Main		
Policy name	Specifies the UTM policy name.	Enter a UTM policy name.
Session per client limit	Specifies the session per client limit.	Enter a value from 0 through 20000.

Table 224: Add UTM Policy Configuration Details (continued)

Field	Function	Action
Session per client over limit	Specifies the session per client over limit. The options available are: <ul style="list-style-type: none"> Log and permit Block 	Select an option.
Anti-Virus profiles		
HTTP profile	Specifies the UTM policy for the HTTP protocol to be scanned.	Select the check box.
FTP upload profile	Specifies the UTM policy for the FTP protocol to be scanned.	Select the check box.
FTP download profile	Specifies the UTM policy for the FTP protocol to be scanned.	Select the check box.
IMAP profile	Specifies the UTM policy for the IMAP protocol to be scanned.	Select the check box.
SMTP profile	Specifies the UTM policy for the SMTP protocol to be scanned.	Select the check box.
POP3 profile	Specifies the UTM policy for the POP3 protocol to be scanned.	Select the check box.
Web filtering profiles		
HTTP profile	Specifies the UTM policy for the HTTP protocol to be scanned.	Select an option from the list.
Anti-Spam profiles		
SMTP profile	Specifies the UTM policy for the SMTP protocol to be scanned.	Select an option from the list.
Content filtering profiles		
HTTP profile	Specifies the UTM policy for the HTTP protocol to be scanned.	Select an option from the list.
FTP upload profile	Specifies the UTM policy for the FTP protocol to be scanned.	Select an option from the list.
FTP download profile	Specifies the UTM policy for the FTP protocol to be scanned.	Select an option from the list.
IMAP profile	Specifies the UTM policy for the IMAP protocol to be scanned.	Select an option from the list.
SMTP profile	Specifies the UTM policy for the SMTP protocol to be scanned.	Select an option from the list.

Table 224: Add UTM Policy Configuration Details (continued)

Field	Function	Action
POP3 profile	Specifies the UTM policy for the POP3 protocol to be scanned.	Select an option from the list.

- See Also**
- [Firewall Policies Configuration Page Options](#)
 - [IDP Policies Configuration Page Options on page 381](#)
 - [Zones and Screens Configuration Page Options on page 313](#)

IPS

- [Signature Update Configuration Page Options on page 373](#)
- [Sensor Configuration Page Options on page 375](#)
- [IDP Policies Configuration Page Options on page 381](#)

Signature Update Configuration Page Options

1. Select **Configure>Security>IDP>Signature Update** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Configure>Security>IPS>Signature Update** in the J-Web user interface.

The Signature Update configuration page appears. [Table 225 on page 374](#) explains the contents of this page.

2. Click one:
 - **Download**—Downloads the latest available version of the signature database from the security server. Enter information as specified in [Table 226 on page 374](#).
 - **Install**—Installs the selected signature. Enter information as specified in [Table 227 on page 374](#).
 - **Check Status**—Checks the install and download status of the signature. [Table 228 on page 374](#) explains the contents of this page.
 - **Download Setting**—Sets the URL for automatic download. Enter information as specified in [Table 229 on page 374](#).
3. Click one:
 - **OK**—Saves the configuration and returns to the main configuration page.
 - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
 - **Cancel**—Cancels your entries and returns to the main configuration page.

Table 225: Signature Update Configuration Page

Field	Function
Name	Displays the field values for install or download operation.
Value	Displays the install or download status of the operation.

Table 226: Download Configuration Page

Field	Function	Action
Security Package Manual Download		
Download	Downloads the existing signature database.	Click Download on the task bar.
URL	Specifies the predefined default URL used by the device to download the signature database.	Select the URL from the list.
Version	Specifies the version number of the security package from the portal.	Select the version from the list.
Full Package	Enables the device to download the latest security package with the full set of attack signature tables from the portal.	Select the check box.

Table 227: Install Configuration Page

Field	Function	Action
Security Package Manual Installation		
Install	Installs the existing signature database.	Click Install on the task bar.
Do not set to active after installed	Specifies whether or not to activate the installed security package.	Select the check box.

Table 228: Check Status Options

Field	Function	Action
Check Status		
Download Status	Shows the security package download status in the message box.	Select Download Status from the Check Status list.
Install Status	Shows the security package install status in the message box.	Select Install Status from the Check Status list.

Table 229: Download Setting Configuration Page

Field	Function	Action
Security Package Automatic Download		

Table 229: Download Setting Configuration Page (continued)

Field	Function	Action
Download Setting	Sets the parameters of automatic download.	Click Download Setting .
URL Setting	Specifies the predefined default URL used by the device to download the signature database.	Click URL Setting and type a URL <i>NOTE:</i> The URL configured in the URL Setting window is displayed by default in the Download window.
Auto Download Setting		
Interval	Specifies the time interval for automatic download.	Enter an integer.
Start Time	Specifies that the latest policy templates are to be installed from the portal.	Enter a time value in <i>MM-DD.hh:mm</i> format.
Enable Schedule Update	Enables the auto-download settings feature.	Select the check box to activate automatic download settings.
Reset Setting	Resets the values configured in this tab.	Select the check box to reset the values.

- See Also**
- [Forwarding Configuration Page Options on page 280](#)
 - [ALG Configuration Page Options on page 429](#)

Sensor Configuration Page Options

1. Select **Configure>Security>IDP>Sensor** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Configure>Security Services>IPS>Sensor** in the J-Web user interface.

The Sensor configuration page appears. explains the contents of this page.



NOTE: Starting in Junos OS Release 19.2R1, you can configure IP sensor in three sections: Basic Settings, Advance Settings, and Detectors.

2. Click one:
 - **Add** or **+**—Adds the detector configuration. Enter information as specified in [Table 230 on page 376](#).
 - **Edit** or **/**—Updates the existing the detector configuration.
 - **Delete** or **X**— Deletes the existing the detector configuration
3. Click one:

- **OK**—Saves the configuration and returns to the main configuration page.
 - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
 - **Cancel**—Cancels your entries and returns to the main configuration page.
4. (Junos OS Release 19.2R1 and later) Click one:
- **Save**—Saves all the configuration.



NOTE: For all the configuration options, tool tip on the right-side represents different icons for notifications, validation errors, and successful configuration.

- **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
- **Cancel**—Cancels all the configuration changes you made.

Table 230: Configuring IDP Sensor Configuration Page

Field	Function	Action
Basic Settings		Select to configure basic IPS sensor settings.
IDP Protection Mode		
Protection Mode	Specifies the inspection parameters for efficient inspection of traffic in the device. The options available are: <ul style="list-style-type: none"> • DataCenter—Disables all STC traffic inspection. • Datacenter Full—Disables all STC traffic inspection. • Perimeter—Inspects all STC (Server To Client) traffic. • Perimeter Full—Inspects all STC traffic. 	Select an option from the list.
Intelligent Inspection		
IDP By Pass	Provides flexibility to bypass IDP or to drop the packets when the system CPU utilization reaches a high level.	Enable or disable the IDP Intelligent Bypass option.
IDP By Pass CPU Threshold	Specifies when CPU utilization reaches the defined threshold value, the IDP stops inspecting new sessions.	Enter the threshold value. Range: 0 through 99. Default value: 85.
IDP By Pass CPU Tolerance	Specifies the CPU tolerance value.	Enter the CPU tolerance value. Range: 1 through 99. Default value: 5.

Table 230: Configuring IDP Sensor Configuration Page (continued)

Field	Function	Action
Intelligent Inspection	Minimizes IDP processing during system overload.	<p>Enable or disable this option.</p> <p>If you enable this option, enter the following details:</p> <ul style="list-style-type: none"> Ignore Content Decompression— Signature Severity—Select the severity level of the attack from the list that the signature will report for IDP processing. The available options are: minor, major, and critical. <p>NOTE: Click Clear All to clear all the selected severity values.</p> <ul style="list-style-type: none"> Protocols—Select the protocols from the list that needs to be processed in Intelligent Inspection mode. <p>NOTE: Click Clear All to clear all the selected protocols.</p> <ul style="list-style-type: none"> CPU Threshold (%)—Enter the value of CPU usage threshold percentage for intelligent inspection. Range: 0 through 99 percent. CPU Tolerance (%)—Enter the value of CPU usage tolerance percentage for intelligent inspection. Range: 0 through 99 percent. Memory Tolerance—Enter the value of memory tolerance percentage for intelligent inspection. Range: 0 through 100 percent. Free Memory Threshold—Enter the value of free memory threshold percentage for intelligent inspection. Range: 0 through 100 percent. Session Bytes Depth—Enter the value of session bytes scanning depth. Range: 1 through 1000000 bytes.
Memory Lower Threshold	Species the memory lower threshold limit percentage.	<p>Enter the memory lower threshold limit percentage.</p> <p>Range: 1 through 100.</p>
Memory Upper Threshold	Species the memory upper threshold limit percentage.	<p>Enter the memory upper threshold limit percentage.</p> <p>Range: 1 through 100.</p>

Flow

Table 230: Configuring IDP Sensor Configuration Page (continued)

Field	Function	Action
Drop On Limit	Specifies the dropped connections on exceeding resource limits.	Enable or disable this option.
Drop On Failover	Specifies the dropped traffic on HA failover sessions.	Enable or disable this option.
Drop If No Policy Loaded	Specifies all the dropped traffic till IDP policy gets loaded.	Enable or disable this option.
Packet Log		
NOTE: Starting in Junos OS Release 19.2R1, Packet Log configuration is available.		
IP Address	Specifies the destination host to send packet log.	Enter the IP address of the destination host.
Port	Specifies the UDP port number.	Enter the UDP port number. Range: 0-65535.
Source Address	Specifies the source IP address used to transport packet log to a host.	Enter the source IP address.
Advanced Settings		Select to configure advanced IPS sensor settings.
IDP Flow		
Log Errors	Specifies if the flow errors have to be logged.	Select an option from the list.
Flow FIFO Max Size	Specifies the maximum FIFO size.	Enter a value. Range: : 1 through 65535. Default value is 1.
Hash Table Size	Specifies the hash table size.	Enter a value. Range: 1024 through 1,000,000. Default value is 1024.
Max Timers Poll Ticks	Specifies the maximum amount of time at which the timer ticks at a regular interval.	Enter a value. Range: 0 through 1000 ticks. Default value is 1000 ticks.
Reject Timeout	Specifies the amount of time in milliseconds within which a response must be received.	Enter a value. Range: 1 through 65,535 seconds. Default value is 300 seconds.
Global		

Table 230: Configuring IDP Sensor Configuration Page (continued)

Field	Function	Action
Enable All Qmodules	Specifies if all the qmodules of the global rulebase IDP security policy are enabled.	Select an option from the list.
Enable Packet Pool	Specifies if the packet pool is enabled to be used when the current pool is exhausted.	Select an option from the list.
Policy Lookup Cache	Specifies if the cache is enabled to accelerate IDP policy lookup.	Select an option from the list.
Memory Limit Percent	Specifies to limit IDP memory usage at this percent of available memory.	Enter a value. Range: 10 through 90 percent.
IPS		
Detect Shellcode	Specifies if shellcode detection has to be applied.	Select an option from the list.
Ignore Regular Expression	Specifies if the sensor has to bypass DFA and PCRE matching.	Select an option from the list.
Process Ignore Server-to-Client	Specifies if the sensor has to bypass IPS processing for server-to-client flows.	Select an option from the list.
Process Override	Specifies if the sensor has to execute protocol decoders even without an IDP policy.	Select an option from the list.
Process Port	Specifies a port on which the sensor executes protocol decoders.	Enter an integer. Range: 0 through 65535.
IPS FIFO Max Size	Specifies the maximum allocated size of the IPS FIFO.	Enter an integer. Range: 1 through 65535.
Minimum Log Supercade	Specifies the minimum number of logs to trigger the signature hierarchy feature.	Enter an integer. Range: 0 through 65535.
Log		
Cache Size	Specifies the size in bytes for each user's log cache.	Enter a value. Range: 1 through 65,535 bytes.
Disable Suppression	Specifies if the log suppression has to be disabled.	Enable or disable this option.
Include Destination Address	Specifies to combine log records for events with a matching source address.	Select an option from the list.

Table 230: Configuring IDP Sensor Configuration Page (continued)

Field	Function	Action
Max Logs Operate	Specifies the maximum number of logs on which log suppression can operate. IDP can operate on 16,384 log records by default.	Enter an integer. Range: 256 through 65,536 records.
Max Time Report	Specifies the time (seconds) after which suppressed logs will be reported. IDP reports suppressed logs after 5 seconds by default.	Enter an integer. Range: 1 through 60 seconds.
Start Log	Specifies the number of log occurrences after which log suppression begins. Log suppression begins with the first occurrence by default.	Enter an integer. Range: 1 through 128.
Reassembler		
Ignore Memory Overflow	Specifies if the user has to allow per-flow memory to go out of limit.	Select an option from the list.
Ignore Reassembly Memory Overflow	Specifies if the user has to allow per-flow reassembly memory to go out of limit.	Select an option from the list.
Ignore Reassembly Overflow	Specifies the TCP reassembler to ignore the global reassembly overflow to prevent the dropping of application traffic.	Enable or disable this option.
Max Flow Memory	Specifies the maximum per-flow memory for TCP reassembly in kilobytes.	Enter an integer. Range: 64 through 4,294,967,295 kilobytes.
Max Packet Memory	Specifies the maximum packet memory for TCP reassembly in kilobytes.	Enter an integer. Range: 64 through 4,294,967,295 kilobytes
Max Synacks Queued	Specifies the maximum limit for queuing Syn/Ack packets with different SEQ numbers.	Enter an integer. Range: 0 through 5
Packet Log		
Max Sessions	Specifies the maximum number of sessions actively conducting pre-attack packet captures on a device at one time.	Enter an integer. Range: 1 through 100 percent
Total Memory	Specifies the maximum amount of memory to be allocated to packet capture for the device.	Enter an integer. Range: 1 through 100 percent
Detectors		Click + and enter the following fields.

Table 230: Configuring IDP Sensor Configuration Page (continued)

Field	Function	Action
Protocol	Specifies the name of the protocol to enable or disable the detector.	Select the name of the protocol from the list.
Tunable Name	Specifies the name of the tunable parameter to enable or disable the protocol detector for each of the services.	Select the name of the specific tunable parameter from the list.
Tunable Value	Specifies the value of the tunable parameter to enable or disable the protocol detector for each of the services.	Enter the protocol value of the specific tunable parameter. Range: 0 to 4294967295

- See Also**
- [Signature Update Configuration Page Options on page 373](#)
 - [Forwarding Configuration Page Options on page 280](#)

IDP Policies Configuration Page Options

1. Select **Configure>Security>IPS>Policy** in the J-Web user interface.

The IDP Policy configuration page appears. [Table 231 on page 382](#) explains the contents of this page.



NOTE: IDP policies that are created by root users in root-logical-system are not displayed in security profile advanced settings if you have logged in as a logical system user.

The **IPS Signature Package version** and **IPS Policy Status**—Displays the version of IPS signature database and its status, if it is published or not.

2. Click the following:
 - **Template**—Downloads, installs, and loads a template. Enter information as specified in [Table 232 on page 383](#).



NOTE: The Template option is available only for root users. It is not available for logical system users.

3. Click the following:

- **Check Status**—Checks download or install status. Enter information as specified in [Table 233 on page 383](#).



NOTE: The Check Status option is available only for root users. It is not available for logical system users.

4. **Set Default**—Sets the selected IPS policy from the policy list as the default policy. Once you set it as default, **(default-policy)** is displayed next to the policy name.
5. Click one:
 - **Add** or **+**—Adds a new or duplicate IDP policy configuration. Enter information as specified in [Table 234 on page 383](#).
 - **Edit** or **/**—Edits the selected IDP policy configuration.
 - **Delete** or **X**—Deletes the selected IDP policy configuration.
6. Click the following:
 - **Clone**—Clones or copies a policy. Select a record in the Policy List. Enter information as specified in [Table 235 on page 385](#).
7. Click **Activate** to validate and activate the configuration.



NOTE: Starting Junos OS Release 18.2R1, **Activate** is unavailable.

8. Click **Deactivate** to remove the IDP active policy from the configuration.



NOTE: Starting Junos OS Release 18.2R1, **Deactivate** is unavailable.

9. Click one:
 - **OK**—Saves the configuration and returns to the main configuration page.
 - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
 - **Cancel**—Cancels your entries and returns to the main configuration page.

Table 231: IDP Policy Configuration Page

Field	Function
-------	----------

Policy List

NOTE: IDP policies that are created by root users in root-logical-system are not displayed in security profile advanced settings if you have logged in as a logical system user.

Table 231: IDP Policy Configuration Page (continued)

Field	Function
Status	Displays the status of the policy.
Name	Displays the IDP policy name.
Type	Displays the IDP policy type.
IPS Rule Number	Displays the number of rule based IP profiles that are configured.
Exempt Rule Number	Displays the number of rule based exempt profiles that are configured.

Table 232: Template Details

Field	Function	Action
Template	<p>Loads a predefined IDP template. The options available are:</p> <ul style="list-style-type: none"> • Download Template—Downloads a template from the server. • Install Template—Installs the template to the router. • Load Template—Loads the predefined policies to the policy list. 	Click Template and select an option.

Table 233: Check Status Details

Field	Function	Action
Check Status	<p>Checks download or install status. The options available are:</p> <ul style="list-style-type: none"> • Download Status—Downloads status information from the Check Status list. • Install Status—Installs status information from the Check Status list. 	Click Check Status and select an option.

Table 234: Add IDP Policy Configuration Details

Field	Function	Action
Policy Name	Specifies the name of the IDP policy.	Enter a policy name.
Activate	Specifies whether or not the configured IDP policy is set as the active policy.	Select the check box.

Table 234: Add IDP Policy Configuration Details (continued)

Field	Function	Action
IPS Rule	Specifies the IPS rule created. The options available are: <ul style="list-style-type: none"> • Add—Adds a new IPS rule. • Edit—Edits the selected IPS rule. • Delete—Deletes the selected record. • Move—Organize rows. Select Move up, Move down, Move to top, or Move to down. 	Select an option.
Basic		
Policy Name	Specifies the name of the IDP policy.	Displays the name of the IDP policy.
Rule Name	Specifies the name of the IPS rulebase rule.	Enter a rule name.
Rule Description	Specifies a description for the rule.	Enter the description for the rule.
Action	Specifies the list of all the rule actions for IDP to take when the monitored traffic matches the attack objects specified in the rules.	Select a rule action from the list.
Application	Specifies the list of one or multiple configured applications.	Select the applications to be matched.
Attack Type	Specifies the attack type that you do not want the device to match in the monitored network traffic. The options available are: <ul style="list-style-type: none"> • Predefined Attacks • Predefined Attack Groups 	Select an option from the list and click the right arrow to match an attack object or attack group to the rule.
Category	Specifies the category used for scrutinizing rules of sets.	Select a category from the list.
Severity	Specifies the rule severity levels in logging to support better organization and presentation of log records on the log server.	Select a severity level from the list.
Direction	Specifies the direction of network traffic you want the device to monitor for attacks.	Select a direction level from the list.
Matched	Specifies the type of network traffic you want the device to monitor for attacks.	Select the traffic type and click the right arrow to move it to the matched list.
Advanced		
IP Action	Specifies the action that IDP takes against future connections that use the same IP address.	Select an IP action from the list.
IP Target	Specifies the destination IP address.	Select an IP target from the list.

Table 234: Add IDP Policy Configuration Details (continued)

Field	Function	Action
Timeout	Specifies the number of seconds the IP action should remain effective before new sessions are initiated within that specified timeout value.	Enter the timeout value, in seconds. The maximum value is 65,535 seconds.
Log IP Action	Specifies whether or not the log attacks are enabled to create a log record that appears in the log viewer.	Select the check box.
Enable Attack Logging	Specifies whether or not the configuring attack logging alert is enabled.	Select the check box.
Set Alert Flag	Specifies whether or not an alert flag is set.	Select the check box.
Severity	Specifies the rule severity level.	Select an option from the list.
Terminal	Specifies whether or not the terminal rule flag is set.	Select the check box.
Match		
From Zone	Specifies the match criteria for the source zone for each rule.	Select the match criteria from the list.
To Zone	Specifies the match criteria for the destination zone for each rule.	Select the match criteria from the list.
Source Address	<p>Specifies the zone exceptions for the from-zone and source address for each rule. The options available are:</p> <ul style="list-style-type: none"> Match—Matches the from-zone and source address/address sets to the rule. Except—Enables the exception criteria. 	<p>Select the from-zone and source addresses/address sets from the list and do one of the following:</p> <ul style="list-style-type: none"> Click Match and then click the right arrow. Click Except.
Destination Address	<p>Specifies the zone exceptions for the to-zone and destination address for each rule. The options available are:</p> <ul style="list-style-type: none"> Match—Matches the from-zone and destination address/address sets to the rule. Except—Enables the exception criteria. 	<p>Select the to-zone and destination addresses/address sets from the list and do one of the following:</p> <ul style="list-style-type: none"> Click Match and then click the right arrow. Click Except.

Table 235: Clone Details

Field	Function	Action
Copy Policy	Displays the policy name that was created.	—
New Policy	Specifies the new policy name.	Enter a new policy name.

- See Also**
- [UTM Policies Configuration Page Options on page 371](#)
 - [Address Book Configuration Page Options on page 326](#)
 - [Firewall Policies Configuration Page Options](#)

skyATP or Threat Prevention

- [Threat Prevention Policies Configuration Page Options on page 386](#)

Threat Prevention Policies Configuration Page Options

1. Select **Configure>Security>SkyATP or Threat Prevention>Policies** in the J-Web user interface.

The Threat Prevention Policies page appears. [Table 203 on page 331](#) explains the contents of this page.
2. Click one:
 - **+**—Create a new or duplicate threat prevention policy. Enter information as specified in [Table 122 on page 204](#).
 - **/**—Edit the selected threat prevention policy.
 - **X**—Delete the selected threat prevention policy.

Table 236: Threat Prevention Policies Page

Field	Function
Name	Displays the threat prevention policy name.
C&C Server	Displays the range value of threat score set for this policy on a C&C server. A C&C profile would provide information on C&C servers that have attempted to contact and compromise hosts on your network. If the threat score of a feed is between this range, the feed will be blocked or permitted based on the threat score.
Infected Host	Displays the range value of threat score set for this policy if . An infected host profile would provide information on compromised hosts and their associated threat levels.
Malware HTTP	A malware profile would provide information on files downloaded by hosts and found to be suspicious based on known signatures or URLs.
Malware SMTP	A malware profile would provide information on files downloaded by hosts and found to be suspicious based on known signatures or URLs.
Log	All traffic is logged by default. Use the pulldown to narrow the types of traffic to be logged.
Description	Displays the description of the policy.

IPSec VPN

- [VPN Global Settings Configuration Page Options on page 387](#)
- [IKE \(Phase I\) Configuration Page Options on page 389](#)

- [IKE \(Phase II\) Configuration Page Options on page 397](#)
- [VPN Manual Key Configuration Page Options on page 404](#)
- [Dynamic VPN Global Settings Configuration Page Options on page 407](#)

VPN Global Settings Configuration Page Options

1. Select **Configure>IPSec VPN>Global Settings** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Configure>Security>IPSec VPN>Global Settings** in the J-Web user interface.

The VPN Global Settings configuration page appears. [Table 237 on page 387](#) explains the contents of this page.

2. Click one:
 - **Save**—Applies changes to the configuration. Enter information as specified in [Table 238 on page 387](#).
 - **Reset**—Resets the configuration without saving changes.

Table 237: VPN Global Configuration Options

Field	Function
IKE Global Settings	
Response Bad SPI	Displays the response to invalid IPsec SPI values.
Maximum Responses	Displays the number of times to respond to invalid SPI values per gateway.
IPsec Global Settings	
VPN Monitor Options	Displays whether or not VPN monitoring options is selected.
Interval	Displays the interval at which ICMP requests are sent to the peer.
Threshold	Displays the number of consecutive unsuccessful pings before the peer is declared unreachable.
Internal SA	Enables secure login and prevents attackers from gaining privileged access through this control port by configuring the internal IPsec security association (SA).
Key (24 bytes)	Specifies the encryption key. You must ensure that the manual encryption key is in ASCII text and 24 characters long; otherwise, the configuration will result in a commit failure.

Table 238: Add VPN Global Configuration Details

Field	Function	Action
IKE Global Settings		

Table 238: Add VPN Global Configuration Details (continued)

Field	Function	Action
Response Bad SPI	Provides response to invalid IPsec security parameter index values. If the SAs between two peers of an IPsec VPN become unsynchronized, the device resets the state of a peer so that the two peers are synchronized.	Select the check box if you want the device to respond to IPsec packets with bad SPI values.
Maximum Responses	Specifies the number of times to respond to invalid SPI values per gateway.	Enter a value from 1 through 30. The default is 5. This option is available when Response Bad SPI is selected.
IPSec Global Settings		
VPN Monitor Options	Provides VPN monitoring options.	Select the check box if you want the device to monitor VPN liveliness.
Interval	Specifies the interval at which ICMP requests are sent to the peer.	Enter a value from 1 through 36,000 seconds.
Threshold	Specifies the number of consecutive unsuccessful pings before the peer is declared unreachable.	Enter a value from 1 through 65,536.
Internal SA	Enables secure login and prevents attackers from gaining privileged access through this control port by configuring the internal IPsec security association (SA).	Select the check box to enable Internal SA.
Key (24 bytes)	Specifies the encryption key.	Enter the encryption key. Ensure that the manual encryption key is in ASCII text and 24 characters long; otherwise, the configuration will result in a commit failure.
PowerMode IPSec	<p>Pushes the relevant IPSec configuration required for the device.</p> <p>NOTE: Starting in Junos OS Release 19.1R1, PowerMode IPSec (PMI) configuration supports only SRX4100, SRX4200, SRX4600, SRX5000 Series devices with SPC3 card, and vSRX2.0</p>	<p>Select the check box to enable PMI.</p> <p>NOTE:</p> <ul style="list-style-type: none"> By default, PFE service restarts automatically after the commit. The PFE service will not explicitly restart. The J-Web user interface allows you to enable or disable PMI depending on the configuration required for each of the devices.

- See Also**
- [IKE \(Phase I\) Configuration Page Options on page 389](#)
 - [IKE \(Phase II\) Configuration Page Options on page 397](#)
 - [VPN Manual Key Configuration Page Options on page 404](#)
 - [Dynamic VPN Global Settings Configuration Page Options on page 407](#)

IKE (Phase I) Configuration Page Options

1. Select **Configure>IPSec VPN>Auto Tunnel> Phase I** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Configure>Security>IPSec VPN>VPN Tunnel I** in the J-Web user interface.

The VPN Gateway configuration page appears.

2. (Junos OS Release 18.3R1 and later releases) Select **Configure > Security Services > IPSec VPN > IKE (Phase I)** in the J-Web user interface.

The IKE (Phase I) configuration page appears. [Table 239 on page 389](#) explains the contents of this page.

3. Click one:

- **Add** or **+**—Adds a new or duplicate VPN gateway configuration. Enter information as specified in [Table 240 on page 390](#).
- **Edit** or **/**—Edits a selected VPN gateway configuration.
- **Delete** or **X**—Deletes the selected VPN gateway configuration.

4. Click one:

- **OK**—Saves the configuration and returns to the main configuration page.
- **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
- **Cancel**—Cancels your entries and returns to the main configuration page.

Table 239: IKE (Phase I) Configuration Page

Field	Function
Gateway	
Gateway Name	Displays the name of the gateway to be searched.
Search	Displays the text box for searching a gateway.
Name	Displays the name of the destination peer gateway, specified as an alphanumeric string.
IKE Policy	Displays the name of the IKE policy.
External Interface	Displays the name of the interface to be used to send traffic to the IPSec VPN.
Remote Identity	Displays information about the remote peer.
IKE Policy	

Table 239: IKE (Phase I) Configuration Page (continued)

Field	Function
Name	Displays the name of the policy.
Description	Provides a description of the policy.
Mode	Displays the mode of configuration.
Authentication Method	Displays the authentication method configured.
Proposal	Displays the name of the proposal configured to be used by this policy in Phase 1.
Proposal	
Name	Displays the name of the proposal selected.
Authentication Algorithm	Displays the hash algorithm configured or selected.
Authentication Method	Displays the authentication method selected.
Encryption Algorithm	Displays the supported IKE proposals.

Table 240: Add Gateway Configuration Details

Field	Function	Action
IKE Gateway		
Name	Specifies the name of the gateway.	Enter the name of the gateway.
Policy	Specifies the name of the policy.	Enter the name of the policy you configured for Phase 1.
External Interface	Specifies the name of the interface to be used to send traffic to the IPsec VPN. Specifies the outgoing interface for IKE SAs. This interface is associated with a zone that acts as its carrier, providing firewall security for it.	Select an outgoing interface from the list.
Site to Site VPN	Specifies the VPN configuration type as site to site.	Click the Site to Site radio button.
Address/FQDN	Specifies the address or FQDN of the peer.	Enter information about the peer IP or domain name.
Local ID		

Table 240: Add Gateway Configuration Details (continued)

Field	Function	Action
Identify Type	Specifies the identity type. The identify types are as follows: <ul style="list-style-type: none"> • IP Address • Host Name • Email Address • Distinguished Name 	Select one of the identity type options.
Client Tunnel	Specifies the remote access dynamic VPN.	Select the Client Tunnel radio button.
Connections limit	Specifies the limit on connections.	Enter the connection limit.
IKE user type	Specifies the Internet Key Exchange user type. The IKE user types are as follows: <ul style="list-style-type: none"> • group-ike-id • shared-ike-id 	Select one of the IKE user type options.
Remote ID		
Identity type	Specifies the identity type. The identify types are as follows: <ul style="list-style-type: none"> • IP Address • Host Name • Email Address • Distinguished Name 	Select one of the identity type options.
IKE Gateway Options		

Table 240: Add Gateway Configuration Details (continued)

Field	Function	Action
Identity Type	<p>Specifies the local IKE identity to send in the exchange with the destination peer so that the destination peer can communicate with the local peer. If you do not configure a local identity, the device uses the IP address corresponding to the local endpoint. You can identify the local identity in any of the following ways:</p> <ul style="list-style-type: none"> • IP Address—IPv4 IP address to identify the dynamic peer. • Hostname—Fully qualified domain name (FQDN) to identify the dynamic peer. • User at Hostname—E-mail address to identify the dynamic peer. • Distinguished Name—Name to identify the dynamic peer. The distinguished name appears in the subject line of the Public Key Infrastructure (PKI) certificate. For example: Organization: juniper, Organizational unit: slt, Common name: common. 	Select one of the identity type options.
Dead Peer Detection	Specifies whether to enable DPD.	Select the check box.
Always send	Specifies the device to send DPD requests regardless of whether there is outgoing IPsec traffic to the peer.	Select the check box.
Interval	Specifies the amount of time that the peer waits for traffic from its destination peer before sending a DPD request packet.	Enter the interval at which to send DPD messages. Range: 1 through 60 seconds.
Threshold	Specifies the maximum number of unsuccessful DPD requests that can be sent before the peer is considered unavailable.	Enter the maximum number of unsuccessful DPD requests to be sent. Range: 1 through 5. Default: 5.
AAA	Provides AAA in addition to IKE authentication for remote users trying to access a VPN tunnel.	Select AAA from the list.
NAT-Traversal	Specifies whether to enable NAT-T. NAT-T is enabled by default.	Select the check box to disable or enable.
NAT-keepalive	Specifies the interval at which NAT keepalive packets can be sent so that NAT continues.	Enter the interval, in seconds, at which NAT keepalive packets can be sent. Default: 5 seconds. Range: 1 through 300 seconds.

Add Policy

Table 240: Add Gateway Configuration Details (continued)

Field	Function	Action
IKE Policy		
Name	Specifies the name of the IKE policy.	Enter the policy name.
Description	Provides a description of the policy.	Enter a description of the policy.
Mode	<p>Specifies the mode. The available modes are as follows:</p> <ul style="list-style-type: none"> • Main mode—This mode has three 2-way exchanges between the initiator and receiver. It is secure and preferred in the auto tunnel • Aggressive mode— This mode is faster than main mode. It is less secure and is used mostly for dial-up VPN. 	Select a mode from the list.
Proposal		
Predefined	<p>Specifies the predefined Phase 1 proposals. Use one of the following types of predefined Phase 1 proposals:</p> <ul style="list-style-type: none"> • Basic • Compatible • Standard • Prime-128 • Prime-256 • Suiteb-gcm-128 • Suiteb-gcm-256 	Click Predefined , and select a proposal type.
User defined	Specifies the user-defined Phase 1 proposal.	Click User Defined , select a proposal from the pop-up menu, and click Add .
Proposal List	Specifies one or more proposals that can be used during key negotiation:	<p>Click the Predefined Proposal option button to select proposals preconfigured by JUNOS Software.</p> <p>Click the User Defined Proposal option button to use proposals that you have created.</p>
IKE Policy Options		
Pre Shared Key	<p>Specifies use of a preshared key for the VPN.</p> <p>The available options are as follows:</p> <ul style="list-style-type: none"> • ASCII text • Hexadecimal 	If a preshared key is selected, then configure the appropriate key.

Table 240: Add Gateway Configuration Details (continued)

Field	Function	Action
Certificate	Specifies use of a certificate for the VPN.	Click the option button.
Local Certificate	Specifies use of a particular certificate when the local device has multiple loaded certificates.	Enter a local certificate identifier.
Peer Certificate Type	<p>Specifies use of a preferred type of certificate.</p> <p>The available options are as follows:</p> <ul style="list-style-type: none"> • PKCS7 • X509 	Select a certificate type.
Trusted CA	<p>Specifies the preferred CA to use when requesting a certificate from the peer. If no value is specified, then no certificate request is sent (although incoming certificates are still accepted).</p> <p>The options that are available are as follows:</p> <ul style="list-style-type: none"> • None—Use none of configured certificate authorities. • Use All—Device uses all configured certificate authorities. • CA Index—Preferred certificate authority ID for the device to use. 	Select a trusted CA from the list.
Add Proposal		
IKE Proposal		
Name	Specifies the name of the proposal.	Enter the name of the proposal.

Table 240: Add Gateway Configuration Details (continued)

Field	Function	Action
Authentication Algorithm	<p>Specifies the AH algorithm that the device uses to verify the authenticity and integrity of a packet. Supported algorithms include the following:</p> <ul style="list-style-type: none"> • md5—Produces a 128-bit digest. • sha1—Produces a 160-bit digest. • sha-256—Produces a 256-bit digest. <p>NOTE: The sha-256 authentication algorithm is not supported with the dynamic VPN feature.</p> <ul style="list-style-type: none"> • sha-384—Produces a 384-bit digest. • sha-512—Starting in Junos OS Release 19.1R1, this option is supported. Produces a 512-bit digest. <p>NOTE: Starting in Junos OS Release 19.1R1, the new Authentication algorithm supports SRX5000 Series devices with SPC3 card upon installation of junos-ike package only. To install junos-ike package from J-Web, navigate to Configure > Security Services > IPsec VPN > Global Settings and click Install.</p>	Select a hash algorithm from the available option.
Authentication Method	<p>Specifies the method the device uses to authenticate the source of IKE messages. The available options are as follows:</p> <ul style="list-style-type: none"> • pre-shared-key—Key for encryption and decryption that both participants must have before beginning tunnel negotiations. • rsa-key—Kinds of digital signatures, which are certificates that confirm the identity of the certificate holder. 	Select an option.
Description	Provides a description of the proposal for easy identification .	Enter a brief description of the IKE proposal.

Table 240: Add Gateway Configuration Details (continued)

Field	Function	Action
DH Group	<p>Specifies the Diffie-Hellman group. The DH exchange allows participants to produce a shared secret value over an unsecured medium without actually transmitting the value across the connection.</p> <p>The available options are as follows:</p> <ul style="list-style-type: none"> • None • group1 • group2 • group5 • group14 • group19 • group20 • group24 • group15—Starting in Junos OS Release 19.1R1, this option is supported. • group16—Starting in Junos OS Release 19.1R1, this option is supported. • group21—Starting in Junos OS Release 19.1R1, this option is supported. <p>NOTE: Starting in Junos OS Release 19.1R1, the new DH-Groups supports SRX5000 Series devices with SPC3 card upon installation of junos-ike package only. To install junos-ike package from J-Web, navigate to Configure > Security Services > IPsec VPN > Global Settings and click Install.</p>	Select a group. If you configure multiple (up to four) proposals for Phase 1 negotiations, use the same Diffie-Hellman group in all proposals.
Encryption Algorithm	<p>Specifies the supported Internet Key Exchange (IKE) proposals. It includes the following:</p> <ul style="list-style-type: none"> • 3des-cbc—3DES-CBC encryption algorithm. • aes-128-cbc—AES-CBC 128-bit encryption algorithm. • aes-192-cbc—AES-CBC 192-bit encryption algorithm. • aes-256-cbc—AES-CBC 256-bit encryption algorithm. • des-cbc—DES-CBC encryption algorithm. 	Select an encryption algorithm from the list.
Lifetime seconds	Specifies the lifetime, in seconds, of an IKE SA. When the SA expires, it is replaced by a new SA and SPI or is terminated.	Select a lifetime for the IKE SA. Default: 3,600 seconds. Range: 180 through 86,400 seconds.

- See Also**
- [IKE \(Phase II\) Configuration Page Options on page 397](#)
 - [VPN Manual Key Configuration Page Options on page 404](#)

[IKE \(Phase II\) Configuration Page Options](#)

1. Select **Configure>IPSec VPN>Auto Tunnel>Phase II** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Configure>Security>IPSec VPN>VPN Tunnel II** in the J-Web user interface.

The VPN Auto Key configuration page appears.

2. (Junos OS Release 18.3R1 and later releases) Select **Configure > Security Services > IPSec VPN > IPSec (Phase II)** in the J-Web user interface.

The IKE (Phase II) configuration page appears. [Table 241 on page 397](#) explains the contents of this page.

3. Click one:

- **Add** or **+**—Adds a new or duplicate VPN AutoKey configuration. Enter information as specified in [Table 242 on page 398](#).
- **Edit** or **/**—Edits a selected VPN AutoKey configuration.
- **Delete** or **X**—Deletes the selected VPN AutoKey configuration.

4. Click one:

- **OK**—Saves the configuration and returns to the main configuration page.
- **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
- **Cancel**—Cancels your entries and returns to the main configuration page.

Table 241: IKE (Phase II) Configuration Page

Field	Function
VPN	
VPN name	Enter the name of the VPN to be searched.
Search	Displays the search specific to a VPN.
Name	Displays the name of the VPN.
Gateway	Displays the name of the gateway.
IPSec Policy	Displays the policy associated with this IPSec tunnel.

Table 241: IKE (Phase II) Configuration Page (continued)

Field	Function
Bind Interface	Displays the tunnel interface to which the route-based VPN is bound.
Proxy Identity	Displays the IPsec proxy identity.
VPN Monitoring	Displays the name of the VPN monitoring option selected.
IPsec Policy	
Name	Displays the name of the IPsec policy.
Description	Displays the description of the policy.
Perfect Forward Secrecy	Displays the method the device uses to generate the encryption key. PFS generates each new encryption key independent of the previous key.
Proposal	Displays the name of the proposal to be used by the IPsec policy in Phase 2.
Proposal	
Name	Displays the name of the Phase 2 proposal.
Authentication Algorithm	Displays the hash algorithm that authenticates packet data.
Protocol	Displays the type of security protocol.
Encryption algorithm	Displays the IKE encryption algorithm type.

Table 242: Add VPN Configuration Details

Field	Function	Action
Add VPN		
IPsec VPN		
VPN Name	Specifies the name of the remote gateway.	Enter a name.
Remote Gateway	Provides association of a policy with IPsec tunnel.	Select a name.
IPsec Policy	Specifies the tunnel interface to which the route-based VPN is bound.	Select a policy.
Bind to tunnel interface	Specifies the tunnel interface to which the route-based VPN is bound.	Select an interface.

Table 242: Add VPN Configuration Details (continued)

Field	Function	Action
Establish tunnels	<p>Specifies when IKE is activated.</p> <ul style="list-style-type: none"> • immediately—IKE is activated immediately after VPN configuration and configuration changes are committed. • on-traffic—IKE is activated only when data traffic flows and must be negotiated. • responder-only—Starting in Junos OS Release 19.1R1, this option is supported. IKE is activated only when the device responds to negotiation request received from the peer. <p>NOTE:</p> <ul style="list-style-type: none"> • The responder-only mode supports SRX5000 Series devices with SPC3 card upon installation of junos-ike package only. To install junos-ike package from J-web, navigate to Configure > Security Services > IPsec VPN > Global Settings and click Install. • When responder-only mode is configured for multiple VPN objects with single gateway configuration, all VPN objects must be configured with responder-only mode only. • Responder-only mode is supported only for site-to-site VPN and it is not supported on AutoVPN. • responder-only-no-rekey—Starting in Junos OS Release 19.1R1, this option is supported. Disables rekey in the responder-only mode. 	Select any of the available options.
Disable anti replay	Specifies to disable the antireplay checking feature of IPsec. By default, antireplay checking is enabled.	Select the check box.
Add St Logical Interface		
Tunnel Interface st0	Specifies the logical unit number.	Enter the logical unit number.
Zone	Specifies the zones for the logical interface.	Select a zone.
Unnumbered	Disables the configuration for logical interface.	Select Unnumbered .
Numbered	Determines if the logical unit is numeric.	Select Numbered .

Table 242: Add VPN Configuration Details (continued)

Field	Function	Action
IPv4 Address	Displays the IPv4 address. NOTE: This field is disabled if Unnumbered is selected.	Enter an IPv4 address.
IPv6 Address	Displays the IPv6 address. NOTE: This field is disabled if Unnumbered is selected.	Enter an IPv6 address.
Multipoint		
Multipoint	Enable to configure multipoint.	Select the check box.
St0 Interface Configuration		
Automatic	Enables the configuration to automatically specify the next hop tunnel address and VPN name.	Select Automatic .
Manual	Enables the configuration to manually provide the next-hop tunnel address and VPN name. Enables the Add and Delete options.	Select Manual .
Next hop tunnel address	Specifies the next-hop tunnel address. Ensure that no two configurations have the same IP address.	Select the check box and enter the IP address.
VPN Name	Specifies the VPN name, displays a list of route-based VPNs.	Select a VPN name.
Routing Protocols		
Enable routing protocols.	Enable the available routing protocols.	Select the check boxes to select protocols.
IPSec VPN Options		
Enable VPN Monitor	Specifies whether to enable VPN monitor.	Select the check box.
Destination IP	Provides association of a policy with IPsec tunnel.	Enter an IP address.
Optimized	Specifies the tunnel interface to which the route-based VPN is bound.	Select the check box.
Source Interface	Specify the source interface for ICMP requests. If no source interface is specified, the device automatically uses the local tunnel endpoint interface.	Specify a source interface.

Table 242: Add VPN Configuration Details (continued)

Field	Function	Action
Use Proxy Identity		
Local IP/Netmask	Specifies the local IP address and subnet mask for proxy identity.	Enter an IP address.
Remote IP/Netmask	Specifies the remote IP address and subnet mask for proxy identity.	Enter an IP address.
Service	Specifies the service (port and protocol combination) to protect.	Select a service.
Do not fragment bit	<p>Specifies how the device handles the DF bit in the outer header.</p> <p>The options available are as follows:</p> <ul style="list-style-type: none"> • clear—Clear (disable) the DF bit from the outer header. This is the default. • copy—Copy the DF bit to the outer header. • set—Set (enable) the DF bit in the outer header. 	Select an option from the list.
Idle Time	Specifies the maximum amount of idle time to delete an SA.	Enter the idle time. Range: 60 through 999999 seconds.
Install interval	Specifies the maximum number of seconds to allow installation of a rekeyed outbound security association (SA) on the device.	Specify a value from 0 through 10 seconds.
Add Policy		
IPSec Policy		
Name	Specifies the name of the remote gateway.	Enter a name.
Description	Provides a description for associating a policy with an IPSec tunnel.	Enter a text description.

Table 242: Add VPN Configuration Details (continued)

Field	Function	Action
Perfect Forward Secrecy	<p>Displays the method the device uses to generate the encryption key. PFS generates each new encryption key independent of the previous key.</p> <ul style="list-style-type: none"> • None. • group1—Diffie-Hellman Group 1. • group2—Diffie-Hellman Group 2. • group5—Diffie-Hellman Group 5. • group14—Diffie-Hellman Group 14. • group19—Diffie-Hellman Group 19. • group20—Diffie-Hellman Group 20. • group24—Diffie-Hellman Group 24. • group15—Starting in Junos OS Release 19.1R1, Diffie-Hellman Group 15 is supported. • group16—Starting in Junos OS Release 19.1R1, Diffie-Hellman Group 16 is supported. • group21—Starting in Junos OS Release 19.1R1, Diffie-Hellman Group 21 is supported. <p>NOTE: Starting in Junos OS Release 19.1R1, the new DH-Groups supports SRX5000 Series devices with SPC3 card upon installation of junos-ike package only. To install junos-ike package from J-Web, navigate to Configure > Security Services > IPsec VPN > Global Settings and click Install.</p>	Select a method.
Proposal		
Predefined	<p>Specifies that the anti-replay checking feature of IPsec be disabled. By default, anti-replay checking is enabled.</p> <p>The options available are as follows:</p> <ul style="list-style-type: none"> • basic • compatible • standard • Prime-128 • Prime-256 • Suiteb-gcm-128 • Suiteb-gcm-256 	Click Predefined , and select one of the option.
User defined	Specifies a list of proposals previously defined by the user.	Click User Defined , select proposals from the pop-up menu, and then click Add .

Table 242: Add VPN Configuration Details (continued)

Field	Function	Action
Proposal List	Specifies the available proposal list.	Select the proposals for Phase 2 from the Available Phase 2 Proposal list. Rearrange the list as required.
Add Proposal		
IPsec Proposal		
Name	Specifies the name of the Phase 2 proposal.	Enter a name.
Description	Provides a description of the Phase 2 proposal.	Enter a text description.
Authentication Algorithm	<p>Specifies the hash algorithm for authenticating packet data. The available options are as follows:</p> <ul style="list-style-type: none"> • none • hmac-md5-96—Produces a 128-bit digest. • hmac-sha1-96—Produces a 160-bit digest. • hmac-sha-256-128—Produces a 256-bit digest. • hmac-sha-512—Starting in Junos OS Release 19.1R1, this option is supported. Produces a 512-bit digest. • hmac-sha-384—Starting in Junos OS Release 19.1R1, this option is supported. Produces a 384-bit digest. <p>NOTE: Starting in Junos OS Release 19.1R1, the new Authentication algorithm SRX5000 Series devices with SPC3 card upon installation of junos-ike package only. To install junos-ike package from J-Web, navigate to Configure > Security Services > IPsec VPN > Global Settings and click Install.</p>	Select an option.

Table 242: Add VPN Configuration Details (continued)

Field	Function	Action
Encryption Algorithm	<p>Specifies an IKE encryption algorithm.</p> <ul style="list-style-type: none"> • none • 3des-cbc—Has a block size of 24 bytes; the key size is 192 bits long. • des-cbc—Has a block size of 8 bytes; the key size is 48 bits long. • aes-128-cbc—AES 128-bit encryption algorithm. • aes-192-cbc—AES 192-bit encryption algorithm. • aes-256-cbc—AES 256-bit encryption algorithm. 	Select an option.
Lifetime Kilobytes	Specifies the lifetime, in kilobytes, of an IPsec SA. The SA is terminated when the specified number of kilobytes of traffic has passed.	Enter a value from 64 through 1,048,576 bytes.
Lifetime Seconds Protocol	Specifies the lifetime, in seconds, of an IKE SA. When the SA expires, it is replaced by a new SA and SPI or is terminated.	Enter a value from 180 through 86,400 seconds.
Protocol	<p>Specifies the networking protocol name.</p> <p>The options available are as follows:</p> <ul style="list-style-type: none"> • none • ah—IP Security Authentication Header • esp—IPsec Encapsulating Security Payload 	Select a protocol from the list.

- See Also**
- [IKE \(Phase I\) Configuration Page Options on page 389](#)
 - [VPN Manual Key Configuration Page Options on page 404](#)

VPN Manual Key Configuration Page Options

1. Select **Configure>IPSec VPN>Manual Tunnel** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Configure>Security>IPSec VPN>Manual Key VPN** in the J-Web user interface.

The VPN Manual Key configuration page appears. [Table 243 on page 405](#) explains the contents of this page.

2. Click one:

- **Add** or **+**—Adds a new or duplicate VPN manual key configuration. Enter information as specified in [Table 244 on page 405](#).
 - **Edit** or **/**—Edits a selected VPN manual key configuration.
 - **Delete** or **X**—Deletes the selected VPN manual key configuration.
3. Click one:
- **OK**—Saves the configuration and returns to the main configuration page.
 - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
 - **Cancel**—Cancels your entries and returns to the main configuration page.

Table 243: VPN Manual Key Configuration Page

Field	Function
Name	Displays the name of the manual tunnel.
Gateway	Displays the selected gateway.
Bind Interface	Displays the tunnel interface to which the route-based VPN is bound.
Df Bit	Displays the DF bit in the outer header.

Table 244: Add VPN Manual Key Configuration Details

Field	Function	Action
IPSec Manual Key		
VPN Name	Specifies the name of the VPN for the IPsec tunnel.	Enter the VPN name.
Remote Gateway	Specifies the name of the remote gateway.	Enter the gateway.
External Interface	Specifies the external interface.	Select an interface from the list.
Protocol	Specifies the types of protocols available for configuration. The available options are as follows: <ul style="list-style-type: none"> • ESP • AH 	Select an option.
SPI	Specifies the SPI value. Range: 256 through 16639.	Enter a value.

Table 244: Add VPN Manual Key Configuration Details (continued)

Field	Function	Action
Bind to tunnel interface	Specifies the tunnel interface to which the route-based VPN is bound.	Select an interface from the list.
Do not fragment bit	<p>Specifies how the device handles the DF bit in the outer header.</p> <p>The available options are as follows:</p> <ul style="list-style-type: none"> • clear—Clear (disable) the DF bit from the outer header. This is the default. • Set—Set the DF bit to the outer header. • copy—Copy the DF bit to the outer header. 	Select an option from the list
Enable VPN Monitor		
Destination IP	Specifies the IP address of the destination peer.	Enter an IP address.
Optimized	Specifies that the device uses traffic patterns as evidence of peer liveliness. If enabled, ICMP requests are suppressed. This feature is disabled by default.	Select the check box to enable the feature.
Source Interface	Specifies the source interface for ICMP requests (VPN monitoring “hellos”). If no source interface is specified, the device automatically uses the local tunnel endpoint interface.	Specify a source interface.
Key Values		
Authentication		
Algorithm	<p>Specifies the hash algorithm that authenticates packet data. The options available are as follows:</p> <ul style="list-style-type: none"> • hmac-md5-96—Produces a 128-bit digest. • hmac-sha1-96—Produces a 160-bit digest. 	Select a hash algorithm from the available option.
ASCII Text	Specifies the preshared value of the key in ASCII format.	Select the ASCII Text option, and enter the key in the appropriate format.
Hexadecimal	Specifies the preshared value of the key in hexadecimal format.	Select the Hexadecimal option, and enter the key in the appropriate format.
Encryption		

Table 244: Add VPN Manual Key Configuration Details (continued)

Field	Function	Action
Encryption	<p>Specifies the supported Internet Key Exchange (IKE) proposals, which includes the following:</p> <ul style="list-style-type: none"> • 3des-cbc—3DES-CBC encryption algorithm. • aes-128-cbc—AES-CBC 128-bit encryption algorithm. • aes-192-cbc—AES-CBC 192-bit encryption algorithm. • aes-256-cbc—AES-CBC 256-bit encryption algorithm. • des-cbc—DES-CBC encryption algorithm. 	Select an option.
ASCII Text	Specifies the preshared value of the key in ASCII format.	Enable the ASCII Text option and enter the key in the appropriate format.
Hexadecimal	Specifies the preshared value of the key in hexadecimal format.	Enable the Hexadecimal option and enter the key in the appropriate format.

- See Also**
- [IKE \(Phase I\) Configuration Page Options on page 389](#)
 - [IKE \(Phase II\) Configuration Page Options on page 397](#)

Dynamic VPN Global Settings Configuration Page Options

1. Select **Configure>IPSec VPN>Dynamic VPN>Global Settings** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Configure>Security>IPSec VPN>Dynamic VPN** in the J-Web user interface.

The Dynamic VPN Global Settings configuration page appears. [Table 245 on page 408](#) explains the contents of this page.

2. Click one:
 - **Add** or **+**—Adds a new client VPN configuration. Enter information as specified in [Table 246 on page 408](#).
 - **/**—Edits a selected VPN gateway configuration.
 - **Apply**—Applies the selected configuration.
 - **Delete** or **X**—Deletes the selected client VPN configuration.
3. Click one:
 - **OK**—Saves the configuration and returns to the main configuration page.

- **Cancel**—Cancels your entries and returns to the main configuration page.

Table 245: Add Dynamic VPN Global Settings Configuration Page

Field	Function	Action
Dynamic VPN		
Access Profile	<p>Specifies the access profile that controls the authentication of users who want to download Access Manager. (You will need to select these access profiles when configuring the IKE gateway and dynamic VPN global options. You can use the same access profile to authenticate users in both cases, or you can use separate access profiles to authenticate downloads and VPN sessions.)</p> <p>NOTE: This Access Profile option does not control authentication for VPN sessions. For session authentication, use the Access Profile option on the IKE Gateway Configuration page. For more information, see "Configuring an IKE Gateway Configuration (Dynamic VPNs)."</p>	Select a previously created access profile from the list that is displayed.
Force Upgrade	<p>Specifies an option to set up a program to automatically download the latest client and install it on the user's computer when the setup program detects a version mismatch between the client and server. Otherwise, the setup program prompts the user to upgrade the client when it detects a version mismatch, but does not force the upgrade. If the user does not choose to upgrade, the setup program will launch the existing client version on the user's computer.</p>	Select the check box to enable or disable force upgrade. (Enabled by default.)

Table 246: Add Client VPN Global Settings Configuration Details

Field	Function	Action
Name	Specifies the name of the client configuration.	Enter a name.
IPSec VPN	Specifies the IKE AutoKey configuration to use when establishing the VPN tunnel.	Select a previously configured IKE AutoKey configuration from the list that is displayed.
Remote Protected Resources IP	<p>Specifies the IP address and net mask of a resource behind the firewall. Traffic to the specified resource will go through the VPN tunnel and therefore will be protected by the firewall's security policies.</p> <p>NOTE: The device does not validate that the IP/net mask combination that you enter here matches up with your security policies.</p>	Enter an IP address and net mask and click Add .
Remote Exceptions IP	Specifies the IP address and net mask of exceptions to the remote protected resources list.	Enter an IP address and net mask and click Add .

Table 246: Add Client VPN Global Settings Configuration Details (continued)

Field	Function	Action
Users	<p>Specifies the list of users who can use this client configuration.</p> <p>NOTE: The server does not validate the names that you enter here, but the names must be the names that the users use to log in to the device when downloading the client.</p>	Enter an user name, and click Add .

- See Also**
- [Dynamic VPN IKE Configuration Page Options](#)
 - [Dynamic VPN IPsec AutoKey Configuration Page Options](#)
 - [VPN Global Settings Configuration Page Options on page 387](#)

User Firewall

- [Configuring Active Directory on page 409](#)
- [Authentication Priority Configuration Page Options on page 413](#)
- [Local Authentication Configuration Page Options on page 414](#)
- [Identity Management Configuration Page Options on page 415](#)

Configuring Active Directory

Use the Create Active Directory Profile page to configure the IP address-to-user mapping information and the user-to-group mapping information to access the LDAP server.

1. Select **Configure>Security>User Firewall>Active Directory** in the J-Web user interface.
2. (Junos OS Release 19.2R1 and later) Select **Configure>Security Services>User Firewall>Active Directory**.
3. Click **Create Active Directory**.



NOTE: This option is not available starting from Junos OS Release 19.2R1 and later.

4. Complete the configuration by using the guidelines in [Table 247 on page 410](#).
5. Click **Finish**.
A Summary page providing a preview of the complete configuration.

You can edit or delete the configuration by clicking the Edit icon (/) or Delete Icon (X).

6. (Junos OS Release 19.2R1 and later) Click **Save** to save all the configurations or click **Cancel** to discard the changes made.

Table 247: Active Directory Configuration Options

Field	Function
General Information	
General	
No on Demand Probe	Enable the manual on-demand probing of a domain PC as an alternate method for the SRX Series device to retrieve address-to-user mapping information.
Timeout	
Authentication Entry Timeout	<p>Set the timeout to 0 to avoid having the user's entry being removed from the authentication table after the timeout.</p> <p>NOTE: When a user is no longer active, a timer is started for that user's entry in the Active Directory authentication table. When the time is up, the user's entry is removed from the table. Entries in the table remain active as long as there are sessions associated with the entry.</p> <p>The default authentication entry timeout is 30 minutes. Starting in Junos OS Release 19.2R1, the default value is 60 minutes.</p> <p>To disable timeout, set the interval to zero. The range is 10 through 1440 minutes.</p>
WMI Timeout	<p>Configure the number of seconds that the domain PC has to respond to the SRX Series device's query through Windows Management Instrumentation (WMI) or Distributed Component Object Module (DCOM).</p> <p>If no response is received from the domain PC within the wmi-timeoutinterval, the probe fails and the system either creates an invalid authentication entry or updates the existing authentication entry as invalid. If an authentication table entry already exists for the probed IP address, and no response is received from the domain PC within the wmi-timeout interval, the probe fails and that entry is deleted from the table.</p> <p>The range is 3 through 120 seconds.</p>
Invalid Authentication Entry Timeout	<p>When a user is no longer active, a timer is started for that user's entry in the Active Directory authentication table. When the time is up, the user's entry is removed from the table.</p> <p>If this value is not configured, all the invalid auth entry from Active Directory will use the default value as 30 minutes.</p> <p>The range is 10 through 1440 minutes.</p>
Firewall Authentication Forced Timeout	<p>This is the firewall authentication fallback time. Set the timeout to 0 to avoid having the user's entry being removed from the authentication table after the timeout.</p> <p>The range is 10 through 1440 minutes.</p>

Table 247: Active Directory Configuration Options (continued)

Field	Function
Filter	
Include	<p>Enable to include IP addresses from the Available column.</p> <p>Click the Add icon (+) to create a new IP address and add it as either include or exclude from monitoring.</p> <p>Click the Delete icon to delete a new IP address and add it as either include or exclude from monitoring.</p>
Exclude	<p>Enable to exclude IP addresses from the Available column.</p> <p>Click the Add icon (+) to create a new IP address and add it as either include or exclude from monitoring.</p> <p>Click the Delete icon to delete a new IP address and add it as either include or exclude from monitoring.</p>
Domain Settings	
Test	<p>Click Test to check the Domain Connection status.</p> <p>test:Status page appears and displays the status.</p>
+	<p>Click + to add a domain.</p> <p>The Add Domain page appears.</p> <p>NOTE:</p> <ul style="list-style-type: none"> Starting in Junos OS Release 19.2R1, for SRX4200, SRX1500, SRX550M, and vSRX, and for the SRX5000 and SRX3000 lines of devices, you can configure the integrated user firewall in a maximum of two domains. For the other SRX Series devices, you can create only one domain. You can select the pencil icon to edit the domain or select delete icon to delete the domain.
General	
Domain Name	<p>Enter the name of the domain.</p> <p>The range for the domain name is 1 through 64 characters.</p>
User Name	<p>Enter the password for the Active Directory account password.</p> <p>The range for the username is 1 through 64 characters. Example: admin</p>
Password	<p>Enter the username for the Active Directory account name.</p> <p>The range for the password is 1 through 128 characters. Example: A\$BC123</p>
Domain Controller(s)	

Table 247: Active Directory Configuration Options (continued)

Field	Function
Domain Controller(s)	<p>Click the add icon (+) to add domain controller settings.</p> <ul style="list-style-type: none"> Domain Controller Name—Enter the domain controller name. Name can range from 1 through 64 characters. You can configure up to maximum of 10 domain controllers. IP Address—Enter the IP address of the domain controller.
User Group Mapping (LDAP)	
User Group Mapping (LDAP)	<p>Click the add icon (+):</p> <ul style="list-style-type: none"> IP Address—Enter the IP address of the LDAP server. If no address is specified, the system uses one of the configured Active Directory domain controllers. Port—Enter the port number of the LDAP server. If no port number is specified, the system uses port 389 for plaintext or port 636 for encrypted text. Default value is port 443. Example: 192.0.2.16
Base Distinguish Name	<p>Enter the LDAP base distinguished name (DN).</p> <p>Example: DC=example,DC=net</p>
User Name	Enter the username of the LDAP account. If no username is specified, the system will use the configured domain controller's username.
Password	Enter the password for the account. If no password is specified, the system uses the configured domain controller's password.
Use SSL	Enable Secure Sockets Layer (SSL) to ensure secure transmission with the LDAP server. Disabled by default, then the password is sent in plaintext.
Authentication Algorithm	Specify the algorithm used while the SRX Series device communicates with the LDAP server. By default simple is selected to configure simple(plaintext) authentication mode.
IP User Mapping	
Discovery Method (WMI)	<p>Enable the method of discovering IP address-to-user mappings.</p> <p>WMI—Windows Management Instrumentation (WMI) is the discovery method used to access the domain controller. This option should be enabled only for internal hosts or trusted hosts.</p>
Event Log Scanning Interval	<p>Enter the scanning interval at which the SRX Series device scans the event log on the domain controller. The range is 5 through 60 seconds.</p> <p>Default value is 60 seconds.</p>

Table 247: Active Directory Configuration Options (continued)

Field	Function
Initial Event Log TimeSpan	Enter the time of the earliest event log on the domain controller that the SRX Series device will initially scan. This scan applies to the initial deployment only. After WMI and the user identification start working, the SRX Series device scans only the latest event log. The range is 1 through 168 hours. Default value is 1 hour.

See Also • [Local Authentication Configuration Page Options on page 414](#)

Authentication Priority Configuration Page Options

1. Select **Configure>Security>User Firewall>Auth Priority** in the J-Web user interface.
The authentication priority configuration page appears. [Table 248 on page 413](#) explains the contents of this page.
2. Click one:
 - **OK**—Saves the configuration and returns to the main configuration page.
 - **Actions>Commit**—Commits the configuration and returns to the main configuration page.
 - **Reset**—Resets your entries and returns to the main configuration page.

Table 248: Authentication Priority Configuration Options

Field	Function	Action
Priority		
Enable local authentication	Enables you to add local authentication and set a priority.	Select the Enable local authentication check box to enable local authentication.
Priority	Enables you to set an authentication priority.	Enter a priority value (1- 65,535) in the Priority field. NOTE: The default local authentication priority value is 100.
Enable firewall authentication	Enables you to add firewall authentication and set a priority.	Select the Enable firewall authentication check box to enable firewall authentication.
Priority	Enables you to set an authentication priority.	Enter a priority value (1- 65,535) in the Priority field. NOTE: The default firewall authentication priority value is 150.

Table 248: Authentication Priority Configuration Options (continued)

Field	Function	Action
Enable UAC authentication	Enables you to add UAC authentication and set a priority.	Select the Enable unified access control check box to enable UAC authentication.
Priority	Enables you to set an authentication priority.	Enter a priority value (1- 65,535) in the Priority field. <i>NOTE:</i> The default local authentication priority value is 200.

See Also • [Local Authentication Configuration Page Options on page 414](#)

Local Authentication Configuration Page Options

1. Select **Configure>Security>User Firewall>Local Auth** in the J-Web user interface.
The local authentication configuration page appears. [Table 249 on page 414](#) explains the contents of this page.
2. Click one:
 - **Add** or **+**—Adds a new or duplicate local authentication configuration. Enter information as specified in [Table 250 on page 415](#).
 - **Delete** or **/**—Deletes the selected local authentication configuration.
 - **Clear All**—Clears all local authentication configuration entries.
3. Click one:
 - **OK**—Saves the configuration and returns to the main configuration page.
 - **Actions>Commit**—Commits the configuration and returns to the main configuration page.
 - **Cancel**—Cancels your entries and returns to the main configuration page.

Table 249: Local Authentication Configuration Page

Field	Function
Filter by	Displays the local authentication configuration based on the selected filter.
IP	Displays the IP address.
User Name	Displays the name of the user.
Role List	Displays the list of roles assigned to the username.

Table 250: Add Local Authentication Configuration Details

Field	Function	Action
IP Address	Specifies the IP address.	Enter an IP address for the local authentication.
User Name	Specifies the username.	Enter a username for the local authentication.
Role List	Specifies the list of roles for the local authentication.	<p>Enter roles for the local authentication entry. Enter the role and click + to add a role.</p> <p>To delete a role, select the role and click –.</p> <p>NOTE: You can configure 200 roles for one local authentication entry.</p>

See Also • [Authentication Priority Configuration Page Options on page 413](#)

Identity Management Configuration Page Options

1. Select **Configure>Security>User Firewall>Identity Management** in the J-Web user interface.

The Identity Management page appears.



NOTE: You cannot configure identity management if active directory is configured. Disable active directory to create a identity management profile.

This page displays:

- The values that you have configured for identity management. You can either edit a few values or delete the entire configuration.
- The connection status of this SRX device with the Juniper Identity Management Service (JIMS), primary as well as secondary server.



NOTE: If you have not configured the identity management profile, the configure button is displayed; click Configure to create a profile.

Table 251 on page 416 explains the contents of this page.

2. If you want to edit or delete the existing profile, click one:
 - /—Enables you to edit the existing profile.
 - X—Deletes the existing profile.

3. Click one:

- **Finish**—Saves the configuration and returns to the main configuration page.
- **Back**—Displays the General Information page and enables you to edit it.
- **Cancel**—Cancels your entries and returns to the main configuration page.

Table 251: Identity Management Profile Page

Field	Displays the
General Information	
Connection Type	type of connection (HTTP or HTTPS).
Port Number	connection port to JIMS server.
Primary IP Address	primary IP address of the JIMS server.
Primary CA Certificate	primary CA certificate of the JIMS server.
Primary Client ID	client-id of the device to obtain access token from primary JIM Server
Secondary IP Address	secondary IP address of the JIMS server.
Secondary Connection Status	connection status to the secondary JIMS server.
Secondary CA Certificate	secondary CA certificate of the JIMS server.
Secondary Client ID	client-id of the device to obtain access token from secondary JIMS server.
Query API	path of the URL for querying user identities.
Token API	path of the URL for acquiring access token.
Advanced Settings	
NOTE: Advanced query cannot be configured when <i>active-directory</i> auth or <i>ClearPass Webapi</i> is enabled. Disable <i>active-directory-access</i> and <i>authentication-source</i> under <i>User-Identification</i> and disable <i>webapi services</i> before committing identity management configuration.	
Items per Batch	maximum items number in one batch query.
No IP Query	status of no-ip-query; Enabled/Disabled
Authentication Entry Timeout	timeout value of auth entry from identity-management.
No Authentication Entry Timeout	

Table 251: Identity Management Profile Page (continued)

Field	Displays the
Address-book	
Address-set	
Domain	

Table 252: Configure or Edit Identity Management Profile

Field	Function	Action
General Information - Connection for Primary and Secondary Identity		
Connection Type	Specifies the type of connection that you want when the device accesses the JIMS server.	Enter a connection type. The options available are: HTTPS and HTTP.
Port	Specifies the connection port of JIMS server.	Enter the port number or press up or down arrow to either increment or decrement the port number. The default value is 443.
Primary IP Address	Specifies the primary IP address of JIMS server.	
Primary CA Certificate	Specifies the primary certificate of the JIMS. SRX device will use it to verify JIMS's certificate for SSL connection.	Select Upload CA certificate to device or Specify the path of the file on device .
Primary CA Certificate file upload	Enables you to locate and upload the CA certificate.	Click Browse to locate the CA certificate on your device and click Upload the selected CA certificate.
Primary Client ID	Specifies the primary client ID of the SRX device to obtain access token. It must be consistent with the configuration of the API client created on JIMS.	Enter an ID.
Primary Client Secret	Specifies the client secret of the SRX device to obtain access token. It must be consistent with the configuration of the API client created on JIMS.	Enter a password which enables you to access the primary identity management server.

Table 252: Configure or Edit Identity Management Profile (continued)

Field	Function	Action
Secondary Identity Management Server	Enables a secondary JIMS server, its IP address, CA certificate, client ID, and client secret.	<p>Select Enable to enable the secondary server.</p> <p>NOTE: If you enable, the Secondary IP Address, Secondary CA Certificate file upload, Secondary Client ID, Secondary Client Secret rows are displayed. Enter the IP address of the secondary server, browse and upload the secondary CA certificate, enter the secondary client ID and secret in the respective fields.</p>
Token API	Specifies the path of the URL for acquiring access token.	Enter the token API. Default is 'oauth_token/oauth'.
Query API	Specifies the path of the URL for querying user identities.	<p>Enter the path where the URL for querying is located. Default is 'user_query/v2'.</p> <p>Click Next. The Advanced Settings page is displayed.</p>
Advanced Settings		
Batch Query		
Item Per Batch	Specifies the maximum number of items in one batch query.	Enter the number of items. Range is 100 to 1000 and the default number is 200.
Query Interval	Specifies the interval for querying the newly generated user identities.	Enter the number of seconds you need between each query. The range is 1~60 (seconds), and the default value is 5.
IP Query		
Query Delay Time	Specifies the time delay to send individual IP query.	Enter the time in seconds. The range is 0~60 (seconds). The default value is 15 seconds, which depends on the delay time of auth entry retrieved from JIMS to SRX.
No IP Query	Allows you to disable IP query.	Select if you want to disable the IP query function that is enabled by default.
Authentication Timeout		

Table 252: Configure or Edit Identity Management Profile (continued)

Field	Function	Action
Authentication Entry Timeout	Specifies the time out value for authentication entry in identity management. The timeout interval begins from when the authentication entry is added to the identity-management authentication table. If a value of 0 is specified, the entries will never expire.	Enter the value in minutes. The value range is 0 or 10~1440 (minutes). 0 means no need for a timeout. the default value is 60.
Invalid Authentication Entry Timeout	Specifies the timeout value of invalid auth entry in the SRX Series authentication table for either Windows active directory or Aruba ClearPass.	Enter the value in minutes. The value range is 0 or 10~1440 (minutes). 0 means no need for a timeout. the default value is 60.
Filter		
Include IP Address Book	Specifies the predefined address book in which an address-set must be selected as IP filter.	Select an IP address book from the list.
Include IP Address Set	Specifies the predefined address set selected as IP filter.	Select an IP address set from the list. To add a new address set for the IP address book, click Add New Address Set
Exclude IP Address Book	Specifies the IP address book that you want identity management profile to exclude.	Select an IP address set from the list that you want to exclude.
Exclude IP Address Set	Specifies the predefined address set that you want identity management profile to exclude.	Select an IP address book from the list.
Filter to Domain	Specified one or more active directory domains of interest to the SRX Series device. You can specify up to twenty domain names for the filter.	Enter the domain names separated by commas.

See Also • [Authentication Priority Configuration Page Options on page 413](#)

SSL Profiles

- [Configuring SSL Initiation Profile on page 419](#)
- [Configuring SSL Proxy on page 423](#)

Configuring SSL Initiation Profile

As a part of SSL initiation profile, you can specify actions related to certification revocations checks and chose an option to ignore certificate validation, root CA expiration dates, and other such issues based on your requirements. Commonly ignored errors include the inability to verify CA signature, incorrect certificate expiration dates, and so

forth. We do not recommend using this option for authentication because configuring it results in websites not being authenticated at all.



NOTE: SSL initiation profile is supported in SRX340, SRX345, SRX550m, SRX1500, SRX4100, SRX4200, and vSRX2.0 platforms.

1. Select **Configure>Security>SSL Initiation**.

The SSL Proxy Profiles page appears. [Table 253 on page 420](#) explains the contents of this page.

2. Click one:

- Add icon (+)—Create a new SSL initiation client profile. Enter information as specified in [Table 254 on page 421](#).
- Edit icon (/)—Edits the selected SSL proxy configuration. Enter information as specified in [Table 254 on page 421](#).
- Delete(X)—Deletes the selected SSL proxy configuration.
- Search icon—Enables you to search a SSL proxy in the grid.
- Show Hide Column Filter icon—Enables you to show or hide a column in the grid.

3. Click Commit icon at the top of the J-Web page. The following commit options are displayed.

- **Commit**—Commits the configuration and returns to the main configuration page.
- **Compare**—Enables you to see the configuration changes that you have performed in the Show Pending Changes.
- **Discard**—Discards the configuration changes you performed in the J-Web.
- **Preferences**—There are two tab:

Commit preferences—You can choose to just validate or validate and commit the changes.

Startup page upon login—You can choose what page should be displayed as soon as you login to J-Web. The options are: Configuration, Monitoring, Dashboard, and Last accessed.

Table 253: SSL Initiation Profile Page

Field	Function
Name	Displays the name of the SSL initiation profile.
Flow Tracing	Displays whether flow trace is enabled or disabled for troubleshooting policy-related issues.
Protocol Version	Displays the accepted protocol SSL version.

Table 253: SSL Initiation Profile Page (continued)

Field	Function
Preferred Cipher	Displays the preferred cipher which the SSH server uses to perform encryption and decryption function.
Session Cache	Displays whether SSL session cache is enabled or not.
Server Authentication Failure	Displays the action that will be performed if errors are encountered during the server certificate verification process (such as CA signature verification failure, self-signed certificates, and certificate expiry).
Certificate Revocation	Displays the criterion for certificate revocation for the SSL initiation profile.

Table 254: Create-Edit SSL Initiation Profile - Configuration Details

Field	Function	Action
Policy Options		
Name	Specifies the name of the SSL initiation profile.	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed; maximum length is 63 characters.
Flow Tracing	Specifies whether or not to enable flow tracing for this profile.	Select this option to enable flow trace for troubleshooting policy-related issues for this profile.
Protocol Version	Specifies the accepted protocol SSL version.	Select the protocol from the dropdown list: None, All, TLSv1, TLSv1.1, or TLSv1.2.
Preferred Cipher	Specify the cipher depending on their key strength. Ciphers are divided into the following categories. <ul style="list-style-type: none"> • Custom—Configure custom cipher suite and order of preference. • Medium—Use ciphers with key strength of 128 bits or greater. • Strong—Use ciphers with key strength of 168 bits or greater. • Weak—Use ciphers with key strength of 40 bits or greater. 	Select a preferred cipher from the dropdown list.
Session Cache	Specifies whether SSL session cache is enabled or not.	Select this option to enable SSL session cache.
Certificate		

Table 254: Create-Edit SSL Initiation Profile - Configuration Details (continued)

Field	Function	Action
Trusted CA	Specify the set of ciphers the SSH server can use to perform encryption and decryption functions. If this option is not configured, the server accepts any supported suite that is available.	Select the trusted certificate authority profile from the dropdown list.
Client Certificate	Specify a client certificate that is required to effectively authenticate the client. <ul style="list-style-type: none"> None SSLRP_Automation_Cert_2 SSLFP_Automation_Cert_1 SSLRP_Automation_Cert_1 SSLFP_Automation_Cert_2 SSL2 	Select the appropriate client certificate from the dropdown list.
Actions		
Server Authentication Failure	Specifies if you want to ignore server authentication completely. <p>In this case, SSL forward proxy ignores errors encountered during the server certificate verification process (such as CA signature verification failure, self-signed certificates, and certificate expiry).</p> <p>We do not recommend this option for authentication, because configuring it results in websites not being authenticated at all. However, you can use this option to effectively identify the root cause for dropped SSL sessions.</p>	Select this option to ignore server authentication completely.
CRL Validation	Specifies certificate revocation actions, whether CRL validation is enabled or disabled.	Select if you want to disable CRL validation.
Action	Specifies the action if CRL information is not present. <ul style="list-style-type: none"> None Allow Drop 	Select the action if CRL info is not present from the options: Allow session, Drop session, or None.
Hold Instruction Code	Specifies if you want to hold the instruction code for this profile.	Select Ignore if you want to keep the instruction code on hold.

- See Also**
- [Zones and Screens Configuration Page Options on page 313](#)
 - [UTM Policies Configuration Page Options on page 371](#)
 - [IDP Policies Configuration Page Options on page 381](#)

- *Chassis Configuration Page Options*

Configuring SSL Proxy

Secure Sockets Layer (SSL) is an application-level protocol that provides encryption and decryption technology for the Internet by residing between the server and the client. SSL, also called Transport Layer Security (TLS), ensures the secure transmission of data between a client and a server through a combination of privacy, authentication, confidentiality, and data integrity. SSL relies on certificates and private-public key exchange pairs for this level of security.

J-Web supports both forward proxy and reverse proxy profiles.



NOTE: SSL proxy is supported in SRX340, SRX345, SRX550m, SRX1500, SRX4100, SRX4200, and vSRX2.0 platforms.

1. Select **Configure>Security>SSL Proxy**.

The SSL Proxy Profiles page appears. [Table 255 on page 424](#) explains the contents of this page.

2. Click one:

- **Global Config**—Configures the session cache timeout and applies it globally to all the policies.
- **Add icon (+)**—Adds a new SSL proxy or global policy configuration. Enter information as specified in [Table 256 on page 424](#).
- **Edit icon (/)**—Edits the selected SSL proxy configuration. Enter information as specified in [Table 256 on page 424](#).
- **Delete (X)**—Deletes the selected SSL proxy configuration.
- **More**—Enables you to clone an SSL proxy from the selected SSL proxy configuration, display a detailed view of the selected SSL proxy, and clear all selections in the grid.
- **Search icon**—Enables you to search a SSL proxy in the grid.
- **Show Hide Column Filter icon**—Enables you to show or hide a column in the grid.

3. Click **Commit** icon at the top of the J-Web page. The following commit options are displayed.

- **Commit**—Commits the configuration and returns to the main configuration page.
- **Compare**—Enables you to see the configuration changes that you have performed in the Show Pending Changes.
- **Discard**—Discards the configuration changes you performed in the J-Web.
- **Preferences**—There are two tab:

Commit preferences—You can choose to just validate or validate and commit the changes.

Startup page upon login—You can choose what page should be displayed as soon as you login to J-Web. The options are: Configuration, Monitoring, Dashboard, and Last accessed.

Table 255: SSL Proxy Profiles Page

Field	Function
Name	Displays the name of the SSL Proxy profile.
Protection Type	Displays the type of protection the profile provides. One is client protection and the other one is server protection. Client protection is for SSL forward proxy and server protection is for reverse proxy.
Preferred Cipher	Displays the category of the profile depending on their key strength.
Custom Cipher	Displays the custom cipher which the SSH server uses to perform encryption and decryption function.
Flow Tracing	Displays whether flow trace is enabled or disabled for troubleshooting policy-related issues.
Exempted Addresses	Displays the addresses to whitelists that bypass SSL forward proxy processing.
Server Auth Failure	Displays the action that will be performed if errors are encountered during the server certificate verification process (such as CA signature verification failure, self-signed certificates, and certificate expiry).
Session Resumption	Displays whether the session resumption is disabled or not.

Table 256: Create-Update SSL Proxy Profile - Configuration Details

Field	Function	Action
Policy Options		
Name	Specified the name of the SSL proxy profile.	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed; maximum length is 63 characters.

Table 256: Create-Update SSL Proxy Profile - Configuration Details (continued)

Field	Function	Action
Preferred Cipher	<p>Specify the cipher depending on their key strength. Ciphers are divided into the following categories.</p> <ul style="list-style-type: none">• Medium—Use ciphers with key strength of 128 bits or greater.• Strong—Use ciphers with key strength of 168 bits or greater.• Weak—Use ciphers with key strength of 40 bits or greater.• Custom—Configure custom cipher suite and order of preference.	Select a preferred cipher from the dropdown list.

Table 256: Create-Update SSL Proxy Profile - Configuration Details (continued)

Field	Function	Action
Custom Ciphers	<p>Specify the set of ciphers the SSH server can use to perform encryption and decryption functions. If this option is not configured, the server accepts any supported suite that is available.</p> <p>The available custom ciphers are:</p> <ol style="list-style-type: none"> 1. rsa-with-RC4-128-md5—RSA, 128-bit RC4, MD5 hash 2. rsa-with-RC4-128-sha—RSA, 128-bit RC4, SHA hash 3. rsa-with-des-cbc-sha—RSA, DES/CBC, SHA hash 4. rsa-with-3DES-ede-cbc-sha—RSA, 3DES EDE/CBC, SHA hash 5. rsa-with-aes-128-cbc-sha—RSA, 128-bit AES/CBC, SHA hash 6. rsa-with-aes-256-cbc-sha—RSA, 256 bit AES/CBC, SHA hash 7. rsa-export-with-rc4-40-md5—RSA-export, 40 bit RC4, MD5 hash 8. rsa-export-with-des40-cbc-sha—RSA-export, 40 bit DES/CBC, SHA hash 9. rsa-with-aes-256-gcm-sha384—RSA, 256 bit AES/GCM, SHA384 hash 10. rsa-with-aes-256-cbc-sha256—RSA, 256 bit AES/CBC, SHA256 hash 11. rsa-with-aes-128-gcm-sha256—RSA, 128 bit AES/GCM, SHA256 hash 12. rsa-with-aes-128-cbc-sha256—RSA, 256 bit AES/CBC, SHA256 hash 13. ecdhe-rsa-with-aes-256-gcm-sha384—ECDHE, RSA, 256 bit AES/GCM, SHA384 hash 14. ecdhe-rsa-with-aes-256-cbc-sha—ECDHE, RSA, 256 bit AES/CBC, SHA hash 15. ecdhe-rsa-with-aes-256-cbc-sha384—ECDHE, RSA, 256 bit AES/CBC, SHA384 hash 16. ecdhe-rsa-with-aes-3des-ede-cbc-sha—ECDHE, RSA, 3DES, EDE/CBC, SHA hash 17. ecdhe-rsa-with-aes-128-gcm-sha256—ECDHE, RSA, 128 bit AES/GCM, SHA256 hash 18. ecdhe-rsa-with-aes-128-cbc-sha—ECDHE, RSA, 128 bit AES/CBC, SHA hash 19. ecdhe-rsa-with-aes-128-cbc-sha256—ECDHE, RSA, 128 bit AES/CBC, SHA256 hash 	Select the set of ciphers from the dropdown list.
Flow Trace	Specify this option to enable flow trace for troubleshooting policy-related issues.	Select this option if you want to enable flow trace else leave it blank..

Table 256: Create-Update SSL Proxy Profile - Configuration Details (continued)

Field	Function	Action
Certificate Type	<p>Specifies whether the certificate that you want to associate with this profile is a root CA or server certificate. Server certificate is used for SSL reverse proxy. If you choose server certificate, the trusted CA, CRL, and server auth failure options will not be available. For forward proxy profile, choose the root CA</p> <p>In a public key infrastructure (PKI) hierarchy, the root CA is at the top of the trust path. The root CA identifies the server certificate as a trusted certificate.</p> <p>NOTE:</p>	
Certificate	Specifies the certificate that you created in the Administration > Certificate Management page of J-Web. In a public key infrastructure (PKI) hierarchy, the CA is at the top of the trust path. The CA identifies the server certificate as a trusted certificate.	Select the certificate that you want to associate with this SSL proxy profile from the dropdown list.
Trusted Certificate Authorities	Specifies the trusted CA associated with the certificate that you selected.	<p>Select the trusted CA that are available on the device from the following options: All, None, Select specific.</p> <p>If you choose Select specific, you need to select the Certificate Authorities from the Available window and move it to the Selected window.</p>
Exempted Addresses	<p>Specifies addresses to create whitelists that bypass SSL forward proxy processing.</p> <p>Because SSL encryption and decryption are complicated and expensive procedures, network administrators can selectively bypass SSL proxy processing for some sessions. Such sessions mostly include connections and transactions with trusted servers or domains with which network administrators are very familiar. There are also legal requirements to exempt financial and banking sites. Such exemptions are achieved by configuring the IP addresses or domain names of the servers under whitelists.</p>	Select the addresses from the from the Available window and move it to the Selected window.
Exempted URL Categories	<p>Specifies URL categories to create whitelists that bypass SSL forward proxy processing.</p> <p>These URL categories are exempted during SSL inspection. Only the predefined URL categories can be selected for the exemption.</p>	Select URL categories from the from the Available window and move it to the Selected window.

Table 256: Create-Update SSL Proxy Profile - Configuration Details (continued)

Field	Function	Action
Actions		
Server Auth Failure	<p>Specifies if you to ignore server authentication completely.</p> <p>In this case, SSL forward proxy ignores errors encountered during the server certificate verification process (such as CA signature verification failure, self-signed certificates, and certificate expiry).</p> <p>We do not recommend this option for authentication, because configuring it results in websites not being authenticated at all. However, you can use this option to effectively identify the root cause for dropped SSL sessions.</p>	Select this option to ignore server authentication completely.
Session Resumption	To improve throughput and still maintain an appropriate level of security, SSL session resumption provides a session caching mechanism so that session information, such as the pre-master secret key and agreed-upon ciphers, can be cached for both the client and server.	Select the Disable Session Resumption option if you do not want session resumption.
Logging	<p>Specifies whether to generate logs.</p> <p>You can choose to log All events, Warnings, general Information, Errors, or different sessions (whitelisted, Allowed, Dropped, or Ignored).</p>	Select this option to generate logs.
Renegotiation	<p>After a session is created and SSL tunnel transport has been established, a change in SSL parameters requires renegotiation. SSL forward proxy supports both secure (RFC 5746) and nonsecure (TLS v1.0 and SSL v3) renegotiation.</p> <p>You can specify whether to Allow nonsecure renegotiation, Allow-secure renegotiation, or Drop renegotiation.</p> <p>When session resumption is enabled, session renegotiation is useful in the following situations:</p> <ul style="list-style-type: none"> • Cipher keys need to be refreshed after a prolonged SSL session. • Stronger ciphers need to be applied for a more secure connection. 	Select if a change in SSL parameters requires renegotiation. The options are: None (selected by default), Allow, Allow-secure, and Drop.
Certificate Revocation	Specifies if you want to revoke the certificate.	Select Disable if you want to revoke the certificate.

Table 256: Create-Update SSL Proxy Profile - Configuration Details (continued)

Field	Function	Action
If CRL info not present	Specifies if you want to allow or drop if CRL info is not present.	Select the action if CRL info is not present from the options: Allow session, Drop session, or None.
Hold Instruction Code	Specifies if you want to hold the instruction code for this profile.	Select Ignore if you want to keep the instruction code on hold.

- See Also**
- [Zones and Screens Configuration Page Options on page 313](#)
 - [UTM Policies Configuration Page Options on page 371](#)
 - [IDP Policies Configuration Page Options on page 381](#)
 - [Chassis Configuration Page Options](#)

ALG

- [ALG Configuration Page Options on page 429](#)

ALG Configuration Page Options

1. Select **Configure>Security>ALG**.

The ALG configuration page appears. [Table 257 on page 429](#) explains the contents of this page.

2. Click one:
 - **OK**—Saves the configuration and returns to the main configuration page.
 - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
 - **Reset**—Resets your entries and returns to the main configuration page.

Table 257: ALG Configuration Options

Field	Function	Action
Main		
Enable TFTP	Provides an ALG for Trivial File Transfer Protocol. The TFTP ALG processes TFTP packets that initiate a request and opens a gate to allow return packets from the reverse direction to the port that sends the request.	Select the check box to enable the ALG.
Enable PPTP	Provides an ALG for Point-to-Point Tunneling Protocol. PPTP is a Layer 2 protocol that tunnels PPP data across TCP/IP networks. The PPTP client is freely available on Windows systems and is widely deployed for building VPNs.	Select the check box to enable the ALG.

Table 257: ALG Configuration Options (continued)

Field	Function	Action
Main		
Enable RSH	Provides an ALG for the remote shell. The RSH ALG handles TCP packets destined for port 514 and processes the RSH port command. The RSH ALG performs NAT on the port in the port command and opens gates as necessary.	Select the check box to enable the ALG.
Enable RTSP	Provides an ALG for the Real-Time Streaming Protocol.	Select the check box to enable the ALG.
Enable SQL	Provides an ALG for Structured Query Language. The SQLNET ALG processes SQL TNS response frames from the server side. It parses the packet and looks for the (HOST=ipaddress), (PORT=port) pattern and performs NAT and gate opening on the client side for the TCP data channel.	Select the check box to enable the ALG.
Enable TALK	Provides an ALG for the TALK protocol. The TALK protocol uses UDP port 517 and port 518 for control-channel connections. The talk program consists of a server and a client. The server handles client notifications and helps to establish talk sessions. There are two types of talk servers: ntalk and talkd. The TALK ALG processes packets of both ntalk and talkd formats. It also performs NAT and gate opening as necessary.	Select the check box to enable the ALG.
DNS		
Enable DNS	Provides an ALG for the domain name system. The DNS ALG monitors DNS query and reply packets and closes the session if the DNS flag indicates the packet is a reply message.	Select the check box to enable the ALG.
Doctoring	Specifies the sanity check.	Select the check box to enable the option.
Maximum Message length	Specifies the maximum message length.	Select a number from Size is (512-8192 bytes).
Enable Oversize message drop.	Specify to enable the oversize message drop.	Select the check box.
FTP		
Enable FTP	Provides an ALG for File Transfer Protocol. The FTP ALG monitors PORT, PASV, and 227 commands. It performs Network Address Translation (NAT) on IP/port in the message and gate opening on the device as necessary. The FTP ALG supports FTP put and FTP get command blocking. When FTP_NO_PUT or FTP_NO_GET is set in the policy, the FTP ALG sends back a blocking command and closes the associated opened gate when it detects an FTP STOR or FTP RETR command.	Select the check box to enable the ALG.

Table 257: ALG Configuration Options (continued)

Field	Function	Action
Main		
Enable allow mismatch IP address	Allows any mismatch in IP address.	Select the check box to enable.
Enable FTP Extension	Enables the file extension.	Select the checkbox to enable File extension.
Enable line Break Extension	Enables the line break extension.	Select the checkbox to enable this option.
H323		
Enable H323 ALG	Enables or disables the H.323 ALG.	Select the check box.
Application Screen		
Message Flood Gatekeeper Threshold	Limits the rate per second at which remote access server (RAS) requests to the gatekeeper are processed. Messages exceeding the threshold are dropped. This feature is disabled by default.	Enter a value. The value range is 1 to 50000 messages per second.
Action On Receiving Unknown Message		
Enable Permit NAT Applied	<p>Specifies how unidentified H.323 (unsupported) messages are handled by the device. The default is to drop unknown messages. Permitting unknown messages can compromise security and is not recommended. However, in a secure test or production environment, this statement can be useful for resolving interoperability issues with disparate vendor equipment. By permitting unknown H.323 messages, you can get your network operational and later analyze your VoIP traffic to determine why some messages were being dropped.</p> <p>This statement applies only to received packets identified as supported VoIP packets. If a packet cannot be identified, it is always dropped. If a packet is identified as a supported protocol, the message is forwarded without processing.</p>	Select the check box.
Enable Permit Routed	Specifies that unknown messages be allowed to pass if the session is in route mode. (Sessions in transparent mode are treated as though they are in route mode.)	Select the check box.
DSCP Code Rewrite		

Table 257: ALG Configuration Options (continued)

Field	Function	Action
Main		
Code Point	Specifies a rewrite-rule for the traffic that passes through a voice over IP Application Layer Gateway (VoIP ALG). The value of code point is in binary format. The VoIP rewrite rules modifies the appropriate class of service (CoS) bits in an outgoing packets through Differentiated Services Code Point (DSCP) mechanism that improves the VoIP quality in a congested network.	Select a 6-bit string from the dropdown list.
Endpoints		
Timeout For Endpoint	Controls the duration of the entries in the NAT table.	Enter a value with a range 10 to 65535 seconds.
Enable Permit Media From Any Source Port	Allows media traffic from any port number. By default, this feature is disabled. When enabled, the device allows a temporary opening, or pinhole, in the firewall as needed for media traffic.	Enter a value from 1 through 50,000 seconds.
IKE-ESP		
Enable IKE-ESP	Enables the IKE-ESP option.	Select the checkbox to enable IKE-ESP.
ESP Gate Timeout	Specifies the ESP gate timeout.	Select the gate timeout from 2 to 30 secs.
ESP Session Timeout(sec)	Specifies the ESP session time out.	Select the timeout session from 60 to 2400 sec.
ALG State Timeout(Sec)	Specifies the ALG state time out.	Select the ALG state time out from 180 to 86400 sec.
MGCP		
Enable MGCP	Enables or disables the Media Gateway Control Protocol.	Select the check box.
Inactive Media Timeout	Specifies the maximum time (in seconds) a call can remain active without any media (RTP or RTCP) traffic within a group. Each time an RTP or RTCP packet occurs within a call, this timeout resets. When the period of inactivity exceeds this setting, the temporary openings (pinholes) in the firewall MGCP ALG opened for media are closed. The default setting is 120 seconds; the range is from 10 to 2550 seconds. Note that, upon timeout, while resources for media (sessions and pinholes) are removed, the call is not terminated.	Select a value from 10 through 2,550 seconds.
Maximum Call Duration	Sets the maximum length of a call. When a call exceeds this parameter setting, the MGCP ALG tears down the call and releases the media sessions. The default setting is 720 minutes; the range is from 3 to 720 minutes.	Select a value from 3 through 720 minutes.

Table 257: ALG Configuration Options (continued)

Field	Function	Action
Main		
Transaction Timeout	Specifies a timeout value for MGCP transactions. A transaction is a signalling message, for example, a NTFY from the gateway to the call agent or a 200 OK from the call agent to the gateway. The device tracks these transactions and clears them when they time out.	Enter a value from 3 through 50 seconds.
Application Screen		
Message Flood Threshold	Limits the rate per second at which message requests to the Media Gateway are processed. Messages exceeding the threshold are dropped by the Media Gateway Control Protocol (MGCP). This feature is disabled by default.	Enter a value from 2 through 50,000 seconds per media gateway.
Connection Flood Threshold	Limits the number of new connection requests allowed per Media Gateway (MG) per second. Messages exceeding the ALG.	Enter a value from 2 through 10,000.
Action On Receiving Unknown Message		
Enable Permit NAT Applied	<p>Specifies how unidentified MGCP messages are handled by the Juniper Networks device. The default is to drop unknown (unsupported) messages. Permitting unknown messages can compromise security and is not recommended. However, in a secure test or production environment, this statement can be useful for resolving interoperability issues with disparate vendor equipment. By permitting unknown MGCP (unsupported) messages, you can get your network operational and later analyze your VoIP traffic to determine why some messages were being dropped.</p> <p>This statement applies only to received packets identified as supported VoIP packets. If a packet cannot be identified, it is always dropped. If a packet is identified as a supported protocol, the message is forwarded without processing.</p>	Select the check box.
Enable Permit Routed	Specifies that unknown messages be allowed to pass if the session is in route mode. (Sessions in transparent mode are treated as route mode.)	Select the check box.
MSRPC		
Enable MSRPC	Provides a method for a program running on one host to call procedures in a program running on another host. Because of the large number of RPC services and the need to broadcast, the transport address of an RPC service is dynamically negotiated based on the service program's Universal Unique Identifier (UUID). The specific UUID is mapped to a transport address.	Select the check box to enable the ALG.
Maximum Group Usage (%)	Specify the maximum group usage (%).	Select the usage % from 10 to 100%.

Table 257: ALG Configuration Options (continued)

Field	Function	Action
Main		
Map Entry Timeout(min)	Specify the map entry time out.	Select the timeout session from 5 to 4320 min.
SCCP		
Enable SCCP	Enables or disables the Skinny Client Control Protocol.	Select the check box.
Inactive Media Timeout	Indicates the maximum length of time (in seconds) a call can remain active without any media (RTP or RTCP) traffic within a group. Each time an RTP or RTCP packet occurs within a call, this timeout resets. When the period of inactivity exceeds this setting, the gates opened for media are closed.	Select a value from 10 through 600 seconds.
Application Screen		
Call Flood Threshold	Protects SCCP ALG clients from flood attacks by limiting the number of calls they attempt to process	Select a value from 2 through 1,000.
Action On Receiving Unknown Messages		
Enable Permit NAT Applied	Specifies how unidentified SCCP messages are handled by the device. The default is to drop unknown (unsupported) messages. Permitting unknown messages can compromise security and is not recommended. However, in a secure test or production environment, this statement can be useful for resolving interoperability issues with disparate vendor equipment. By permitting unknown SCCP (unsupported) messages, you can get your network operational and later analyze your VoIP traffic to determine why some messages were being dropped. This statement applies only to received packets identified as supported VoIP packets. If a packet cannot be identified, it is always dropped. If a packet is identified as a supported protocol, the message is forwarded without processing.	Select the check box.
Enable Permit Routed	Specifies that unknown messages be allowed to pass if the session is in route mode. (Sessions in transparent mode are treated as though they are in route mode.)	Select the check box.
SIP		
Enable SIP	Enables or disables Session Initiation Protocol.	Select the check box.
Enable Retain Hold Resource	Enables or disables whether the device frees media resources for a SIP, even when a media stream is placed on hold. By default, media stream resources are released when the media stream is held.	Select the check box.

Table 257: ALG Configuration Options (continued)

Field	Function	Action
Main		
Maximum Call Duration	Sets the absolute maximum length of a call. When a call exceeds this parameter setting, the SIP ALG tears down the call and releases the media sessions. The default setting is 720 minutes, the range is from 3 to 720 minutes.	Select a value from 3 through 720 minutes.
C Timeout	Specifies the INVITE transaction timeout at the proxy, in minutes; the default is 3. Because the SIP ALG is in the middle, instead of using the INVITE transaction timer value B (which is $(64 * T1) = 32$ seconds), the SIP ALG gets its timer value from the proxy.	Select a value from 3 through 10 minutes.
T4 Interval	Specifies the maximum time a message remains in the network. The default is 5 seconds; the range is 5 through 10 seconds. Because many SIP timers scale with the T4-Interval (as described in RFC 3261), when you change the value of the T4-Interval timer, those SIP timers also are adjusted.	Select a value from 5 through 10 seconds.
Inactive Media Timeout	Specifies the maximum time (in seconds) a call can remain active without any media (RTP or RTCP) traffic within a group. Each time an RTP or RTCP packet occurs within a call, this timeout resets. When the period of inactivity exceeds this setting, the temporary openings (pinholes) in the firewall SIP ALG opened for media are closed. The default setting is 120 seconds; the range is 10 through 2550 seconds. Note that, upon timeout, while resources for media (sessions and pinholes) are removed, the call is not terminated.	Select a value from 10 through 2,550 seconds.
T1 Interval	Specifies the roundtrip time estimate, in seconds, of a transaction between endpoints. The default is 500 milliseconds. Because many SIP timers scale with the T1-Interval (as described in RFC 3261), when you change the value of the T1-Interval timer, those SIP timers also are adjusted.	Select a value from 500 through 5000 milliseconds.

Action On Receiving Unknown Message

Table 257: ALG Configuration Options (continued)

Field	Function	Action
Main		
Enable Permit NAT Applied	<p>Specifies how unidentified SIP messages are handled by the device. The default is to drop unknown (unsupported) messages. Permitting unknown messages can compromise security and is not recommended. However, in a secure test or production environment, this statement can be useful for resolving interoperability issues with disparate vendor equipment. By permitting unknown SIP messages, you can get your network operational and later analyze your VoIP traffic to determine why some messages were being dropped.</p> <p>This statement applies only to received packets identified as supported VoIP packets. If a packet cannot be identified, it is always dropped. If a packet is identified as a supported protocol, the message is forwarded without processing.</p>	Select the check box.
Enable Permit Routed	Specifies that unknown messages be allowed to pass if the session is in route mode. (Sessions in transparent mode are treated as route mode.)	Select the check box.
Protect Options		
Application Screen		
SIP Invite Attack Table Entry Timeout	Specifies the time (in seconds) to make an attack table entry for each INVITE, which is listed in the application screen.	Enter a value from 1 through 3,600 seconds.
Enable Attack Protection	Protects servers against INVITE attacks. Configures the SIP application screen to protect the server at some or all destination IP addresses against INVITE attacks.	<p>Select All Servers or Selected Servers as the options.</p> <p>When Selected Servers option is selected, UI provides the option to add/delete Destination IPs.</p>
SUNRPC		
Enable SUNRPC	Provides a method for a program running on one host to select the check box to enable the ALG. call procedures in a program running on another host. Because of the large number of RPC services and the need to broadcast, the transport address of an RPC service is dynamically negotiated based on the service's program number and version number. Several binding protocols are defined for mapping the RPC program number and version number to a transport address.	Select the checkbox to enable SUNRPC.
Maximum Group Usage (%)	Specify the maximum group usage (%).	Select the usage % from 10 to 100%.
Map Entry Timeout	Specify the map entry time out.	Select the timeout session from 5 to 4320 min.

- See Also**
- [Signature Update Configuration Page Options on page 373](#)
 - [Forwarding Configuration Page Options on page 280](#)

Firewall Filters

- [IPv4 Firewall Filters Configuration Page Options on page 437](#)
- [IPv6 Firewall Filters Configuration Page Options on page 450](#)
- [Assign to Interfaces Configuration Page Options on page 461](#)

IPv4 Firewall Filters Configuration Page Options

1. Select **Configure>Security>Filters>IPv4 Firewall Filters** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Configure>Security>Firewall Filters>IPv4** in the J-Web user interface.

The IPv4 Firewall Filters configuration page appears.
2. Click one:
 - **Add**—Adds a new or duplicate IPv4 firewall filters configuration. Enter information as specified in [Table 258 on page 437](#).
 - **Edit**—Edits the selected IPv4 firewall filters configuration.
 - **Delete**—Deletes the selected IPv4 firewall filters configuration.
3. Click one:
 - **OK**—Saves the configuration and returns to the main configuration page.
 - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
 - **Cancel**—Cancels your entries and returns to the main configuration page.

Table 258: Add IPv4 Firewall Filters Configuration Details

Field	Function	Action
IPv4 Filter Summary		

Table 258: Add IPv4 Firewall Filters Configuration Details (continued)

Field	Function	Action
Action column	<p>Displays up and down arrows and a X, allowing you to delete or change the order of a filter or term. The order of an item is important because it determines the order in which corresponding actions are carried out.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • To move an item upward—Locate the item and click the up arrow from the same row. • To move an item downward—Locate the item and click the down arrow from the same row. • To delete an item—Locate the item and click the X from the same row. 	Select an option.
Filter Name	<p>Displays the name of the filter and when expanded, lists the terms attached to the filter.</p> <p>Displays the match conditions and actions that are set for each term.</p> <p>Allows you to add more terms to a filter or modify filter terms.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • To display the terms added to a filter—Click the plus sign next to the filter name. This also displays the match conditions and actions set for the term. • To edit a filter—Click the filter name. To edit a term, click the name of the term. 	Select an option.
Search		
Filter Name	<p>Searches for existing filters by filter name.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • To find a specific filter—Enter the name of the filter in the Filter Name box. • To list all filters with a common prefix or suffix—Use the wildcard character (*) when you enter the name of the filter. For example, te* lists all filters with a name starting with the characters te. 	Select an option.

Table 258: Add IPv4 Firewall Filters Configuration Details (continued)

Field	Function	Action
Term Name	<p>Searches for existing terms by term name.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • To find a specific term—Enter the name of the term in the Term Name box. • To list all terms with a common prefix or suffix—Use the wildcard character (*) when typing the name of the term. For example, ra* lists all terms with a name starting with the characters ra. 	Select an option.
Number of Items to Display	Specifies the number of filters or terms to display on one page. Select the number of items to be displayed on one page.	Select a number from the list.
Add New IPv4 Filter		
Name	<p>Positions the new filter in one of the following locations:</p> <ul style="list-style-type: none"> • After Final IPv4 Filter—At the end of all filters. • After IPv4 Filter—After a specified filter. • Before IPv4 Filter—Before a specified filter. 	Select an option.
Add	Adds a new filter name. Opens the term summary page for this filter allowing you to add new terms to this filter.	Click Add.
Add New IPv4 Term		
Name	<p>Positions the new term in one of the following locations:</p> <ul style="list-style-type: none"> • After Final IPv4 Filter—At the end of all term. • After IPv4 Filter—After a specified term. • Before IPv4 Filter—Before a specified term. 	Select an option.
Add	Opens the Filter Term page allowing you to define the match conditions and the action for this term.	Click Add.
Match Source		

Table 258: Add IPv4 Firewall Filters Configuration Details (continued)

Field	Function	Action
Source Address	<p>Specifies IP source addresses to be included in, or excluded from, the match condition. Allows you to remove source IP addresses from the match condition.</p> <p>If you have more than 25 addresses, this field displays a link that allows you to easily scroll through pages, change the order of addresses, and also search for them.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include the address in the match condition. • Except—To exclude the address from the match condition and then select Add -To include the address in the match condition. • Delete—To remove an IP source address from the match condition. 	Enter an IP source address and prefix length, and select an option.
Source Prefix List	<p>Specifies source prefix lists, which you have already defined, to be included in the match condition. Allows you to remove a prefix list from the match condition.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include a predefined source prefix list in the match condition, type the prefix list name. • Delete—To remove a prefix list from the match condition. 	Select an option.
Source Port	<p>Specifies the source port type to be included in, or excluded from, the match condition. Allows you to remove a source port type from the match condition.</p> <p>NOTE: This match condition does not check the protocol type being used on the port. Make sure to specify the protocol type (TCP or UDP) match condition in the same term.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include the port in the match condition. • Except—To exclude the port from the match condition and then select Add—To include the port in the match condition. • Delete—To remove a port from the match condition. 	Select the port from the port name list; enter the port name, number, or range and then select an option.
Match Destination		

Table 258: Add IPv4 Firewall Filters Configuration Details (continued)

Field	Function	Action
Destination Address	<p>Specifies destination addresses to be included in, or excluded from, the match condition. Allows you to remove a destination IP address from the match condition.</p> <p>If you have more than 25 addresses, this field displays a link that allows you to easily scroll through pages, change the order of addresses, and also search for them.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include the address in the match condition. • Except—To exclude the address from the match condition and then select Add—To include the address in the match condition. • Delete—To remove an IP address from the match condition. 	Enter an IP destination address and prefix length and select an option.
Destination Prefix List	<p>Specifies destination prefix lists, which you have already defined, to be included in the match condition. Allows you to remove a prefix list from the match condition.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include a predefined destination prefix list, enter the prefix list name. • Delete—To remove a prefix list from the match condition. 	Select an option.
Destination Port	<p>Specifies destination port types to be included in, or excluded from, the match condition. Allows you to remove a destination port type from the match condition.</p> <p>NOTE: This match condition does not check the protocol type being used on the port. Make sure to specify the protocol type (TCP or UDP) match condition in the same term.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include the port in the match condition. • Except—To exclude the port from the match condition and then select Add—To include the port in the match condition. • Delete—To remove a port type from the match condition. 	Select the port from the port name list; enter the port name, number, or range; and then select an option.

Match Source or Destination

Table 258: Add IPv4 Firewall Filters Configuration Details (continued)

Field	Function	Action
Address	<p>Specifies IP addresses to be included in, or excluded from, the match condition for a source or destination. Allows you to remove an IP address from the match condition.</p> <p>If you have more than 25 addresses, this field displays a link that allows you to easily scroll through pages, change the order of addresses and also search for them.</p> <p>NOTE: This address match condition cannot be specified in conjunction with the source address or destination address match conditions in the same term.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include the address in the match condition. • Except—To exclude the address from the match condition and then select Add—To include the address in the match condition. • Delete—To remove an IP address from the match condition. 	Enter an IP destination address and prefix length and select an option.
Prefix List	<p>Specifies prefix lists, which you have already defined, to be included in the match condition for a source or destination. Allows you to remove a prefix list from the match condition.</p> <p>NOTE: This prefix list match condition cannot be specified in conjunction with the source prefix list or destination prefix list match conditions in the same term.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include a predefined destination prefix list, type the prefix list name. • Delete—To remove a prefix list from the match condition. 	Select an option.

Table 258: Add IPv4 Firewall Filters Configuration Details (continued)

Field	Function	Action
Port	<p>Specifies a port type to be included in, or excluded from, a match condition for a source or destination. Allows you to remove a destination port type from the match condition.</p> <p>NOTE: This match condition does not check the protocol type being used on the port. Make sure to specify the protocol type (TCP or UDP) match condition in the same term.</p> <p>Also, this port match condition cannot be specified in conjunction with the source port or destination port match conditions in the same term.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include the port in the match condition. • Except—To exclude the port from the match condition and then select Add—To include the port in the match condition. • Delete—To remove a port type from the match condition. 	Select the port from the port name list; enter the port name, number, or range; and then select an option.
Match Interface		
Interface	<p>Specifies interfaces to be included in a match condition. Allows you to remove an interface from the match condition.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include an interface in a match condition. • Delete—To remove an interface from the match condition. 	Select a name from the interface name list or Enter the interface name and select an option.
Interface Set	<p>Specifies interface sets, which you have already defined, to be included in a match condition. Allows you to remove an interface set from the match condition.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include the group in the match condition. • Delete—To remove an interface group from the match condition. 	Enter the interface set name and select an option.

Table 258: Add IPv4 Firewall Filters Configuration Details (continued)

Field	Function	Action
Interface Group	<p>Specifies interface groups, which you have already defined, to be included in, or excluded from, a match condition. Allows you to remove an interface group from the match condition.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include the port in the match condition. • Except—To exclude the port from the match condition and then select Add—To include the port in the match condition. • Delete—To remove a port type from the match condition. 	Enter the name of the group and select an option.
Match Packet and Network		
First Fragment	Matches the first fragment of a fragmented packet.	Select the check box.
Is Fragment	Matches trailing fragments (all but the first fragment) of a fragmented packet.	Select the check box.
Fragment Flags	Specifies fragmentation flags to be included in the match condition.	Enter a text or numeric string defining the flag.
TCP Established	<p>Matches all Transmission Control Protocol packets other than the first packet of a connection.</p> <p>NOTE: This match condition does not verify that the TCP is used on the port. Make sure to specify the TCP as a match condition in the same term.</p>	Select the check box.
TCP Initial	<p>Matches the first Transmission Control Protocol packet of a connection.</p> <p>NOTE: This match condition does not verify that the TCP is used on the port. Make sure to specify the TCP as a match condition in the same term.</p>	Select the check box.
TCP Flags	<p>Specifies Transmission Control Protocol flags to be included in the match condition.</p> <p>NOTE: This match condition does not verify that the TCP is used on the port. Make sure to specify the TCP as a match condition in the same term.</p>	Enter a text or numeric string defining the flag.

Table 258: Add IPv4 Firewall Filters Configuration Details (continued)

Field	Function	Action
Protocol	<p>Specifies IPv4 protocol types to be included in, or excluded from, the match condition. Allows you to remove an IPv4 protocol type from the match condition.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include the protocol in the match condition. • Except—To exclude the protocol from the match condition and then select Add—To include the protocol in the match condition. • Delete—To remove an IPv4 protocol type from the match condition. 	Select a protocol name from the list or enter a protocol name or number and then select an option.
ICMP Type	<p>Specifies ICMP packet types to be included in, or excluded from, the match condition. Allows you to remove an ICMP packet type from the match condition.</p> <p>NOTE: This protocol does not verify that ICMP is used on the port. Make sure to specify an ICMP type match condition in the same term.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include the packet type in the match condition. • Except—To exclude the packet type from the match condition and then select Add—To include the packet type in the match condition. • Delete—To remove an ICMP packet type from the match condition. 	Select a packet type from the list or enter a packet type name or number and then select an option.
ICMP Code	<p>Specifies the ICMP code to be included in, or excluded from, the match condition. Allows you to remove an ICMP code from the match condition.</p> <p>NOTE: The ICMP code is dependent on the ICMP type. Make sure to specify an ICMP type match condition in the same term.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include the packet type in the match condition. • Except—To exclude the packet type from the match condition and then select Add—To include the packet type in the match condition. • Delete—To remove an ICMP packet type from the match condition. 	Select a packet code from the list or enter the packet code as text or a number and select an option.

Table 258: Add IPv4 Firewall Filters Configuration Details (continued)

Field	Function	Action
Fragment Offset	<p>Specifies the fragment offset value to be included in, or excluded from, the match condition. The fragment offset value specifies the location of the fragment in the packet. For example, fragment offset zero specifies the first fragment. Allows you to remove a fragment offset value from the match condition.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include the offset in the match condition. • Except—To exclude the offset from the match condition and then select Add—To include the offset in the match condition. • Delete—To remove a fragment offset value from the match condition. 	Enter a fragment offset number or range and then select an option.
Precedence	<p>Specifies IP precedences to be included in, or excluded from, the match condition. Allows you to remove an IP precedence entry from the match condition.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include the precedence in the match condition. • Except—To exclude the precedence from the match condition and then select Add—To include the precedence in the match condition. • Delete—To remove an IP precedence from the match condition. 	Select IP precedences from the list; or enter the precedence as a keyword, a decimal integer from 0 through 7, or a binary string; and then select an option.
DSCP	<p>Specifies Differentiated Services code points to be included in, or excluded from, the match condition. Allows you to remove a DSCP entry from the match condition.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include the DSCP in the match condition. • Except—To exclude the DSCP from the match condition and then select Add—To include the DSCP in the match condition. • Delete—To remove a DSCP from the match condition. 	Select DSCP from the list; or enter the DSCP value as a keyword, a decimal integer from 0 through 7, or a binary string; and then select an option.

Table 258: Add IPv4 Firewall Filters Configuration Details (continued)

Field	Function	Action
TTL	<p>Specifies the IPv4 time-to-live value to be included in, or excluded from, the match condition. Allows you to remove an IPv4 TTL value from the match condition.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include the TTL in the match condition. • Except—To exclude the TTL from the match condition and then select Add—To include the TTL in the match condition . • Delete—To remove an IPv4 TTL type from the match condition. 	<p>Specify an IPv4 TTL value by entering a number from 1 through 255, and select an option.</p>
Packet Length	<p>Specifies the length of received packets, in bytes, to be included in, or excluded from, the match condition. Allows you to remove a packet length value from the match condition.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include the packet length in the match condition. • Except—To exclude the packet length from the match condition and then select Add—To include the packet length in the match condition. • Delete—To remove a packet length value from the match condition. 	<p>Specify a packet length, enter a value or range.</p> <p>Select an option.</p>
Forwarding Class	<p>Specifies forwarding classes to be included in, or excluded from, the match condition. Allows you to a remove forwarding class entry from the match condition.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include the forwarding class in the match condition. • Except—To exclude the forwarding class from the match condition and then select Add—To include the forwarding class in the match condition. • Delete—To remove a forwarding class from the match condition. 	<p>Specify a forwarding class by selecting a forwarding class from the list or entering a forwarding class, and then select an option.</p>

Table 258: Add IPv4 Firewall Filters Configuration Details (continued)

Field	Function	Action
IP Options	<p>Specifies IP options to be included in, or excluded from, the match condition. Allows you to remove an IP option from the match condition.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include the IP option in the match condition. • Except—To exclude the IP option from the match condition and then select Add—To include the IP option in the match condition. • Delete—To remove an IP option from the match condition. 	Specify option by selecting an IP option from the list or entering a text or numeric string identifying the option, and then select an option.
IPSec ESP SPI	<p>Specifies IPSec Encapsulating Security Payload security parameter index values to be included in, or excluded from, the match condition. Allows you to remove an ESP SPI value from the match condition.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include the value in the match condition. • Except—To exclude the value from the match condition and then select Add—To include the value in the match condition. • Delete—To remove an ESP SPI value from the match condition. 	Specify an ESP SPI value by entering a binary, hexadecimal, or decimal SPI value or range, and then select an option.
Action		
Nothing	Specifies that no action is performed. By default, a packet is accepted if it meets the match conditions of the term, and packets that do not match any conditions in the firewall filter are dropped.	Select Nothing .
Accept	Accepts a packet that meets the match conditions of the term.	Select Accept .
Discard	Discards a packet that meets the match conditions of the term. Names a discard collector for packets.	Select Discard .

Table 258: Add IPv4 Firewall Filters Configuration Details (continued)

Field	Function	Action
Reject	Rejects a packet that meets the match conditions of the term and returns a rejection message. Allows you to specify a message type that denotes the reason the packet was rejected. NOTE: To log and sample rejected packets, specify log and sample action modifiers in conjunction with this action.	Select Reject and then select a message type from the reason list.
Next Term	Evaluates a packet with the next term in the filter if the packet meets the match conditions in this term. This action makes sure that the next term is used for evaluation even when the packet matches the conditions of a term. When this action is not specified, the filter stops evaluating the packet after it matches the conditions of a term, and takes the associated action.	Select Next Term .
Routing Instance	Accepts a packet that meets the match conditions, and forwards it to the specified routing instance.	Select Routing Instance , and enter the routing instance name in the box next to Routing Instance .
Load Balance	Specifies a load-balance group, which you have already defined, to be used by packets that meet the match conditions. A load-balance group contains interfaces that use the same next-hop group to balance the traffic load.	Select Load Balance and enter the group name in the box next to Load Balance .
Action Modifiers		
Forwarding Class	Classifies the packet as a specific forwarding class.	Select Forwarding Class from the list.
Count	Counts the packets passing this term. Allows you to name a counter that is specific to this filter. This means that every time a packet transits any interface that uses this filter, it increments the specified counter.	Select Count and enter a 24-character string containing letters, numbers, or hyphens to specify a counter name.
Virtual Channel	Specifies the virtual channel to be set on a particular logical interface.	Enter a string identifying the virtual channel.
Log	Logs the packet header information in the routing engine.	Select Log .
Syslog	Records packet information in the system log.	Select Syslog .

Table 258: Add IPv4 Firewall Filters Configuration Details (continued)

Field	Function	Action
Sample	Samples traffic on the interface. <i>NOTE:</i> You must enable traffic sampling for this action to work.	Select Sample .
Loss Priority	Sets the loss priority of the packet. This is the priority of dropping a packet before it is sent, and it affects the scheduling priority of the packet.	Select Loss Priority from the list.

- See Also**
- [IPv6 Firewall Filters Configuration Page Options on page 450](#)
 - [Assign to Interfaces Configuration Page Options on page 461](#)

IPv6 Firewall Filters Configuration Page Options

1. Select **Configure>Security>Filters>IPv6 Firewall Filters** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Configure>Security>Firewall Filters>IPv6** in the J-Web user interface.

The IPv6 Firewall Filters configuration page appears.

2. Click one:
 - **Add**—Adds a new or duplicate IPv6 firewall filters configuration. Enter information as specified in [Table 259 on page 450](#).
 - **Edit**—Edits the selected IPv6 firewall filters configuration.
 - **Delete**—Deletes the selected IPv6 firewall filters configuration.
3. Click one:
 - **OK**—Saves the configuration and returns to the main configuration page.
 - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
 - **Cancel**—Cancels your entries and returns to the main configuration page.

Table 259: Add IPv6 Firewall Filters Configuration Details

Field	Function	Action
IPv6 Filter Summary		

Table 259: Add IPv6 Firewall Filters Configuration Details (continued)

Field	Function	Action
Action column	<p>Displays up and down arrows and an X, allowing you to delete or change the order of a filter or term. The order of an item is important because it determines the order in which corresponding actions are carried out.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • To move an item upward—Locate the item and click the up arrow from the same row. • To move an item downward—Locate the item and click the down arrow from the same row. • To delete an item—Locate the item and click the X from the same row. 	Select an option.
Filter Name	<p>Displays the name of the filter and, when expanded, lists the terms attached to the filter.</p> <p>Displays the match conditions and actions that are set for each term.</p> <p>Allows you to add more terms to a filter or to modify filter terms.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • To display the terms added to a filter—Click the plus sign next to the filter name. This also displays the match conditions and actions set for the term. • To edit a filter—Click the filter name. To edit a term, click the name of the term. 	Select an option.
Search		
Filter Name	<p>Searches for existing filters by filter name.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • To find a specific filter—Enter the name of the filter in the Filter Name box. • To list all filters with a common prefix or suffix—Use the wildcard character (*) when you enter the name of the filter. For example, te* lists all filters with a name starting with the characters te. 	Select an option.

Table 259: Add IPv6 Firewall Filters Configuration Details (continued)

Field	Function	Action
Term Name	<p>Searches for existing terms by name.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • To find a specific term—Enter the name of the term in the Term Name box. • To list all terms with a common prefix or suffix—Use the wildcard character (*) when typing the name of the term. For example, ra* lists all terms with a name starting with the characters ra. 	Select an option.
Number of Items to Display	Specifies the number of filters or terms to display on one page. Selects the number of items to be displayed on one page.	Select a number from the list.
Add New IPv6 Filter		
Name	<p>Positions the new filter in one of the following locations:</p> <ul style="list-style-type: none"> • After Final IPv4 Filter—At the end of all filters. • After IPv6 Filter—After a specified filter. • Before IPv6 Filter—Before a specified filter. 	Select an option.
Add	Adds a new filter name. Opens the term summary page for this filter allowing you to add new terms to this filter.	Click Add.
Add New IPv6 Term		
Name	<p>Positions the new term in one of the following locations:</p> <ul style="list-style-type: none"> • After Final IPv6 Filter—At the end of all terms. • After IPv6 Filter—After a specified term. • Before IPv6 Filter—Before a specified term. 	Select an option.
Add	Opens the Filter Term page, allowing you to define the match conditions and the action for this term.	Click Add.
Match Source		

Table 259: Add IPv6 Firewall Filters Configuration Details (continued)

Field	Function	Action
Source Address	<p>Specifies IP source addresses to be included in, or excluded from, the match condition. Allows you to remove source IP addresses from the match condition.</p> <p>If you have more than 25 addresses, this field displays a link that allows you to easily scroll through pages, change the order of addresses, and also search for them.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include the address in the match condition. • Except—To exclude the address from the match condition and then select Add -To include the address in the match condition. • Delete—To remove an IP source address from the match condition. 	Enter an IP source address and prefix length, and select an option.
Source Prefix List	<p>Specifies source prefix lists, which you have already defined, to be included in the match condition. Allows you to remove a prefix list from the match condition.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include a predefined source prefix list in the match condition, type the prefix list name. • Delete—To remove a prefix list from the match condition. 	Select an option.
Source Port	<p>Specifies the source port type to be included in, or excluded from, the match condition. Allows you to remove a source port type from the match condition.</p> <p>NOTE: This match condition does not check the protocol type being used on the port. Make sure to specify the protocol type (TCP or UDP) match condition in the same term.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include the port in the match condition. • Except—To exclude the port from the match condition and then select Add—To include the port in the match condition. • Delete—To remove a port type from the match condition. 	Select the port from the port name list; enter the port name, number, or range; and then select an option.
Match Destination		

Table 259: Add IPv6 Firewall Filters Configuration Details (continued)

Field	Function	Action
Destination Address	<p>Specifies destination addresses to be included in, or excluded from, the match condition. Allows you to remove a destination IP address from the match condition.</p> <p>If you have more than 25 addresses, this field displays a link that allows you to easily scroll through pages, change the order of addresses, and search for them.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include the address in the match condition. • Except —To exclude the address from the match condition and then select Add—To include the address in the match condition. • Delete—To remove an IP address from the match condition. 	Enter an IP destination address and prefix length, and select an option.
Destination Prefix List	<p>Specifies destination prefix lists, which you have already defined, to be included in the match condition. Allows you to remove a prefix list from the match condition.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include a predefined destination prefix list, enter the prefix list name. • Delete—To remove a prefix list from the match condition. 	Select an option.
Destination Port	<p>Specifies destination port types to be included in, or excluded from, the match condition. Allows you to remove a destination port type from the match condition.</p> <p>NOTE: This match condition does not check the protocol type being used on the port. Make sure to specify the protocol type (TCP or UDP) match condition in the same term.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include the port in the match condition. • Except—To exclude the port from the match condition and then select Add—To include the port in the match condition. • Delete—To remove a port type from the match condition. 	Select the port from the port name list; enter the port name, number, or range; and then select an option.

Match Source or Destination

Table 259: Add IPv6 Firewall Filters Configuration Details (continued)

Field	Function	Action
Address	<p>Specifies IP addresses to be included in, or excluded from, the match condition for a source or destination. Allows you to remove an IP address from the match condition.</p> <p>If you have more than 25 addresses, this field displays a link that allows you to easily scroll through pages, change the order of addresses and also search for them.</p> <p>NOTE: This address match condition cannot be specified in conjunction with the source address or destination address match conditions in the same term.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include the address in the match condition. • Except—To exclude the address from the match condition and then select Add—To include the address in the match condition. • Delete—To remove an IP address from the match condition. 	Enter an IP destination address and prefix length and select an option.
Prefix List	<p>Specifies prefix lists, which you have already defined, to be included in the match condition for a source or destination. Allows you to remove a prefix list from the match condition.</p> <p>NOTE: This prefix list match condition cannot be specified in conjunction with the source prefix list or destination prefix list match conditions in the same term.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include a predefined destination prefix list, type the prefix list name. • Delete—To remove a prefix list from the match condition. 	Select an option.

Table 259: Add IPv6 Firewall Filters Configuration Details (continued)

Field	Function	Action
Port	<p>Specifies a port type to be included in, or excluded from, a match condition for a source or destination. Allows you to remove a destination port type from the match condition.</p> <p>NOTE: This match condition does not check the protocol type being used on the port. Make sure to specify the protocol type (TCP or UDP) match condition in the same term.</p> <p>Also, this port match condition cannot be specified in conjunction with the source port or destination port match conditions in the same term.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include the port in the match condition. • Except—To exclude the port from the match condition and then select Add—To include the port in the match condition. • Delete—To remove a port type from the match condition. 	Select the port from the port name list; enter the port name, number, or range; and then select an option.
Match Interface		
Interface	<p>Specifies interfaces to be included in a match condition. Allows you to remove an interface from the match condition.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include an interface in a match condition. • Delete—To remove an interface from the match condition. 	Select a name from the interface name , or enter the interface name, and select an option.
Interface Set	<p>Specifies interface sets, which you have already defined, to be included in a match condition. Allows you to remove an interface set from the match condition.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include the group in the match condition. • Delete—To remove an interface group from the match condition. 	Enter the interface set name and select an option.

Table 259: Add IPv6 Firewall Filters Configuration Details (continued)

Field	Function	Action
Interface Group	<p>Specifies interface groups, which you have already defined, to be included in, or excluded from, a match condition. Allows you to remove an interface group from the match condition.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include the port in the match condition. • Except—To exclude the port from the match condition and then select Add—To include the port in the match condition. • Delete—To remove a port type from the match condition. 	Enter the name of the group and select an option.
Match Packet and Network		
TCP Established	<p>Matches all Transmission Control Protocol packets other than the first packet of a connection.</p> <p>NOTE: This match condition does not verify that the TCP is used on the port. Make sure to specify the TCP as a match condition in the same term.</p>	Select the check box.
TCP Initial	<p>Matches the first Transmission Control Protocol packet of a connection.</p> <p>NOTE: This match condition does not verify that the TCP is used on the port. Make sure to specify the TCP as a match condition in the same term.</p>	Select the check box.
TCP Flags	<p>Specifies Transmission Control Protocol flags to be included in the match condition.</p> <p>NOTE: This match condition does not verify that the TCP is used on the port. Make sure to specify the TCP as a match condition in the same term.</p>	Enter a text or numeric string defining the flag.

Table 259: Add IPv6 Firewall Filters Configuration Details (continued)

Field	Function	Action
ICMP Type	<p>Specifies Internet Control Message Protocol packet types to be included in, or excluded from, the match condition. Allows you to remove an ICMP packet type from the match condition.</p> <p>NOTE: This protocol does not verify that ICMP is used on the port. Make sure to specify an ICMP type match condition in the same term.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include the packet type in the match condition. • Except—To exclude the packet type from the match condition and then select Add—To include the packet type in the match condition. • Delete—To remove an ICMP packet type from the match condition. 	Select a packet type from the list or enter a packet type name or number, and select an option.
Next Header	<p>Specifies IPv6 protocol types to be included in, or excluded from, the match condition. Allows you to remove an IPv6 protocol type from the match condition.</p> <ul style="list-style-type: none"> • Add—To include the protocol in the match condition. • Except—To exclude the protocol from the match condition and then select Add—To include the protocol in the match condition. • Delete—To remove an IPv6 protocol type from the match condition. 	Select a protocol name from the list or enter the protocol name number, and select an option.
ICMP Code	<p>Specifies the Internet Control Message Protocol code to be included in, or excluded from, the match condition. Allows you to remove an ICMP code from the match condition.</p> <p>NOTE: The ICMP code is dependent on the ICMP type. Make sure to specify an ICMP type match condition in the same term.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include the packet type in the match condition. • Except—To exclude the packet type from the match condition and then select Add—To include the packet type in the match condition. • Delete—To remove an ICMP packet type from the match condition. 	Select a packet code from the list, or enter the packet code as text or a number, and select an option.

Table 259: Add IPv6 Firewall Filters Configuration Details (continued)

Field	Function	Action
Traffic Class	<p>Specifies the traffic class to be included in, or excluded from, the match condition. Allows you to remove a traffic class value from the match condition.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include the traffic class in the match condition. • Except—To exclude the traffic class from the match condition and then select Add—To include the traffic class in the match condition. • Delete—To remove a traffic class value from the match condition. 	Select a traffic class from the list or enter the traffic class as text number or a length by entering a value or range, and select an option.
Packet Length	<p>Specifies the length of received packets, in bytes, to be included in, or excluded from, the match condition. Allows you to remove a packet length value from the match condition.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include the packet length in the match condition. • Except—To exclude the packet length from the match condition and then select Add—To include the packet length in the match condition. • Delete—To remove a packet length value from the match condition. 	Specify a packet length by entering a value or range, and select an option.
Forwarding Class	<p>Specifies forwarding classes to be included in, or excluded from, the match condition. Allows you to a remove forwarding class entry from the match condition.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include the forwarding class in the match condition. • Except—To exclude the forwarding class from the match condition and then select Add—To include the forwarding class in the match condition. • Delete—To remove a forwarding class from the match condition. 	Specify a forwarding class by selecting a forwarding class from the list or entering a forward class, and then select an option.
Action		
Nothing	Specifies that no action is performed. By default, a packet is accepted if it meets the match conditions of the term, and packets that do not match any conditions in the firewall filter are dropped.	Select Nothing .

Table 259: Add IPv6 Firewall Filters Configuration Details (continued)

Field	Function	Action
Accept	Accepts a packet that meets the match conditions of the term.	Select Accept .
Discard	Discards a packet that meets the match conditions of the term. Names a discard collector for packets.	Select Discard .
Reject	Rejects a packet that meets the match conditions of the term and returns a rejection message. Allows you to specify a message type that denotes the reason the packet was rejected. NOTE: To log and sample rejected packets, specify log and sample action modifiers in conjunction with this action.	Select Reject and Select a message type from the reason list.
Next Term	Evaluates a packet with the next term in the filter if the packet meets the match conditions in this term. This action makes sure that the next term is used for evaluation even when the packet matches the conditions of a term. When this action is not specified, the filter stops evaluating the packet after it matches the conditions of a term, and takes the associated action.	Select Next Term .
Routing Instance	Accepts a packet that meets the match conditions, and forwards it to the specified routing instance.	Select Routing Instance and enter the routing instance name in the box next to Routing Instance .
Load Balance	Specifies a load-balance group, which you have already defined, to be used by packets that meet the match conditions. A load-balance group contains interfaces that use the same next-hop group to balance the traffic load.	Select Load Balance and enter the group name in the box next to Load Balance .
Action Modifiers		
Forwarding Class	Classifies the packet as a specific forwarding class.	Select Forwarding Class from the list.
Count	Counts the packets passing this term. Allows you to name a counter, which is specific to this filter. This means that every time a packet transits any interface that uses this filter, it increments the specified counter.	Select Count and then enter a 24-character string containing letters, numbers, or hyphens to specify a counter name.
Log	Logs the packet header information in the routing engine.	Select Log .
Syslog	Records packet information in the system log.	Select Syslog .

Table 259: Add IPv6 Firewall Filters Configuration Details (continued)

Field	Function	Action
Loss Priority	Sets the loss priority of the packet. This is the priority of dropping a packet before it is sent, and it affects the scheduling priority of the packet.	Select Loss Priority from the list.

- See Also**
- [IPv4 Firewall Filters Configuration Page Options on page 437](#)
 - [Assign to Interfaces Configuration Page Options on page 461](#)

Assign to Interfaces Configuration Page Options

1. Select **Configure>Filters>Assign to Interfaces** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Configure>Security>Firewall Filters>Assign to Interfaces** in the J-Web user interface.

The Assign to Interfaces configuration page appears.
2. Click one:
 - **Add**—Adds a new or duplicate assign to interfaces configuration. Enter information as specified in [Table 260 on page 461](#).
 - **Edit**—Edits the selected assign to interfaces configuration.
 - **Delete**—Deletes the selected assign to interfaces configuration.
3. Click one:
 - **OK**—Saves the configuration and returns to the main configuration page.
 - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
 - **Cancel**—Cancels your entries and returns to the main configuration page.

Table 260: Add Assign to Interfaces Configuration Details

Field	Function	Action
Firewall Filters		

Table 260: Add Assign to Interfaces Configuration Details (continued)

Field	Function	Action
Logical Interface Name	<p>Displays the logical interfaces on a router. Allows you to apply IPv4 and IPv6 firewall filters to packets received on the interface and packets transmitted from the interface.</p> <p>The options available are:</p> <ul style="list-style-type: none">• To apply an input firewall filter, follow instructions in the input firewall filters section.• To apply an output firewall filter, follow instructions in the ouput firewall filters section.	Select an interface name.
Link State	Displays the status of the logical interface.	—
Input Firewall Filters	Displays the input firewall filter applied on an interface. This filter evaluates all packets received on the interface.	—
Output Firewall Filters	Displays the output firewall filter applied on an interface. This filter evaluates all packets transmitted from the interface.	—
Input Firewall Filters		
IPv4 Input Filter	Allows you to apply an input firewall filter to an interface. This filter evaluates all packets received on the interface.	Select the name of the firewall filter from the list.
IPv6 Input Filter		
Output Firewall Filters		
IPv4 Output Filter	Allows you to apply an output firewall filter to an interface. This filter evaluates all packets received on the interface.	Select the name of the firewall filter from the list.
IPv6 Output Filter		

- See Also**
- [IPv4 Firewall Filters Configuration Page Options on page 437](#)
 - [IPv6 Firewall Filters Configuration Page Options on page 450](#)

ICAP Redirect

- [ICAP Redirect Profile Configuration Page Options on page 462](#)

ICAP Redirect Profile Configuration Page Options

The Internet Content Adaptation Protocol (ICAP) is a lightweight protocol used to extend transparent proxy servers, thereby freeing up resources and standardizing the way in which new features are implemented. ICAP is generally used to implement virus scanning and content filters in transparent HTTP proxy caches. It also concentrates on leveraging edge-based devices (caching proxies) to help deliver value-added services. At the core

of this process is a cache that will proxy all client transactions and will process them through ICAP web servers.

On SRX devices, the device works as SSL proxy and decrypts pass through traffic with proper SSL profile under the permission of policy. It decrypts the HTTPS traffic and redirects HTTP message to third party on premises DLP server using Internet Content Adaptation Protocol (ICAP) channel.

1. Select **Configure>Security>ICAP Redirect Profile** in the J-Web user interface.

The ICAP Redirect Profile configuration page appears.

2. Click one:

- **Server Status**—Fetches and displays the ICAP Redirect server details in a new window. It shows the ICAP profile name, server name, and its status.
- **Add**—Create a new ICAP Redirect profile configuration. Enter information as specified in [Table 261 on page 463](#).
- **Edit**—Edits the selected ICAP Redirect profile configuration.
- **Delete**—Deletes the selected assign to interfaces configuration.

3. Click one:

- **OK**—Saves the configuration and returns to the main configuration page.
- **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
- **Cancel**—Cancels your entries and returns to the main configuration page.

Table 261: Create-Edit ICAP Redirect Profile

Field	Function	Action
Firewall Filters		
Name	Displays the ICAP Service profile name.	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed; maximum length is 63 characters.
Timeout	Displays the server response timeout in milliseconds.	Enter the server response timeout in milliseconds. The range is between 100 milliseconds to 50000 milliseconds.
HTTP Redirect Option		
Request	Enables redirect service on HTTP request	Select to enable redirect service on HTTP request.
Response	Enables redirect service on HTTP response.	Select to enable redirect service on HTTP response.
ICAP Server		

Table 261: Create-Edit ICAP Redirect Profile (continued)

Field	Function	Action
You can configure ICAP Redirection server by the following options:		
Add —Create an ICAP Redirect server. Enter information as specified in Table 262 on page 464 .		
Edit —Edit an ICAP Redirect server configuration. Enter information as specified in Table 262 on page 464 .		
Fallback Option		
Timeout Action	Specifies the request timeout action when the request is sent to the server.	Select the timeout action from the dropdown list. The available options are: None, Permit, Log Permit, and Block.
Connectivity Action	Specifies that request cannot be sent out due to connection issues.	
Default Action	Specifies the default failure action to be taken when there are scenarios other than the above two mentioned ones.	

Table 262: Create-Edit ICAP Redirect Server

Field	Function	Action
Name	Displays the ICAP Redirect server name.	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed; maximum length is 63 characters.
Host Type*	Specifies whether the host type is a host name or host IP address..	Select Name or IP address.
Host	Specifies the host name or host IP address depending on what host type you chose as the Host Type.	Enter the host name or host IP address.
Port	Specifies the port in the server. This is the server listening post and the default port will be reached according to protocol defined.	Enter the port number. The range is between 1025 and 65534.
Sockets	Specifies the number of connections to be created.	Enter the number of connections. The range is between 1 and 64.
Authentication		
Authorization Type	Specifies the type of authentication.	

Table 262: Create-Edit ICAP Redirect Server (continued)

Field	Function	Action
Credential Type	Specifies the credentials for the server.	Select the credential type as ASCII or Base64.
Credentials		Based on the Credential Type that you choose, enter the ASCII string or Base64 string.
URL		
Request MOD	Specifies the reqmod uri that can be configured for ICAP server only.	Select to enable redirect service on HTTP request.
Response MOD	Specifies the respmod uri that can be configured for ICAP server only.	Select to enable redirect service on HTTP response.
Routing Instance	Specifies the virtual router that is used for launching.	Select the routing instance from the dropdown list.
SSL Initiation Profile	Specifies the TLS profile.	Select the SSL initiation profile from the dropdown list.

- See Also**
- [IPv4 Firewall Filters Configuration Page Options on page 437](#)
 - [IPv6 Firewall Filters Configuration Page Options on page 450](#)

DS-Lite

- [DS-Lite Configuration Page Options on page 465](#)

DS-Lite Configuration Page Options

1. Select **Configure>Security>DS-Lite** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Configure>Network>DS-Lite** in the J-Web user interface.

The DS-Lite configuration page appears. [Table 263 on page 466](#) explains the contents of this page.

2. Click one:
 - **Add** or **+**—Adds a new or duplicate DS-Lite configuration. Enter information as specified in [Table 264 on page 466](#).
 - **Edit** or **/**—Edits the selected DS-Lite configuration.
 - **Delete** or **X**—Deletes the selected DS-Lite configuration.
3. Click one:
 - **OK**—Saves the configuration and returns to the main configuration page.

- **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
- **Cancel**—Cancels your entries and returns to the main configuration page.

Table 263: DS-Lite Configuration Page

Field	Function
Name	Displays the name of the DS-Lite configuration.
Concentrator	Displays the name of the softwire concentrator.
Type	Displays the type of DS-Lite used.

Table 264: Add DS-Lite Configuration Details

Field	Function	Action
Name	Specifies the name of the DS-Lite configuration.	Enter a name for the DS-Lite configuration.
Concentrator	Specifies the IP address of the softwire concentrator.	Enter the IP address of the softwire concentrator.
Type	Specifies the softwire type.	Select the softwire type from the list.

See Also • [Monitoring DS-Lite on page 122](#)

Multi Tenancy

- [Configuring Multi Tenancy Logical Systems on page 466](#)
- [Configuring Multi Tenancy Resource Profiles on page 476](#)
- [Configuring Multi Tenancy Tenants on page 481](#)

Configuring Multi Tenancy Logical Systems

Logical system enables you to partition a single device in to secure contexts. It allows you to virtually divide a supported SRX Series devices, securing them from intrusion and attacks, and protecting them from false conditions outside their own context. Each logical system has its own discrete administrative domain, logical interfaces, routing interfaces, security firewall and other security features.

An SRX Series device with a multitenant logical systems device, can give various departments, organizations, customers, and partners a private use of the portion of its resource and a private view of the device. Using logical systems, you can share system and underlying physical machine resources among discrete user logical systems and the master logical system.

Root users can switch to Logical system context by navigating to **Configure>Multi tenancy>Logical systems** or **Tenants** page and selecting any one listed instance and clicking **Enter LSYS** or **Enter TENANT**,

Roles supported for Logical system and Tenant

J-Web supports the following roles with respect to Logical system and tenant.

- Root user in normal mode
- Root user entering into a Logical system
- Logical system administrator
- Logical system read-only user
- Root user entering as tenant
- Tenant administrator
- Tenant read-only user



NOTE: Tenant administrator and read-only users are created from Tenant wizard by selecting appropriate roles.

If you have opened J-Web in multiple tabs in the browser, and if in one of the tab you switch mode to Logical system or Tenant, then the other instances of J-Web in the other tabs will automatically switch to Logical system or Tenant.

J-Web maintains different session for different protocols, such as http or https.

When you refresh the screen, you will not be logged out; instead the screen is refreshed, and you will continue in the same session.

1. Select **Configure>Multi Tenancy>Logical Systems**.

The Logical Systems page appears. [Table 265 on page 468](#) explains the contents of this page.

2. Click one:

- **Enter LSYS** — Enter the selected logical system. [Table 266 on page 468](#) explains the content of this page.
- **More**— select this option to view the logical system details.
- **Add icon (+)**— Create a new logical system. Enter information as specified in [Table 267 on page 469](#).
- **Edit icon (/)**— Edit the selected logical system. Enter information as specified in [Table 267 on page 469](#).
- **Delete icon (X)**—Deletes the selected logical system.

- Search icon— Enables you to search a logical system in the grid.
 - Show Hide Column Filter icon —Enables you to show or hide a column in the grid.
3. Click Commit icon at the top of the J-Web page. The following commit options are displayed.
- **Commit**—Commits the configuration and returns to the main configuration page.
 - **Compare**—Enables you to compare the current configuration with the previous configuration.
 - **Discard**—Discards the configuration changes you performed in the J-Web.
 - **Preferences**—There are two tab:

Commit preferences—You can choose to just validate or validate and commit the changes.

Confirm commit timeout (in min) —You can select the commit timeout interval.



NOTE: During the report generation if you switch context, then a confirmation message is displayed. Click Yes to stop the report generation and to switch the context. Click No to continue to generate the report and not to switch context.

Table 265: Logical System profile page

Field	Function
Name	Displays the name of the logical system.
Resource Profile	Displays the name of the resource profile.
Users	Displays the logical system admin and users.
Assigned Interfaces	Displays the assigned logical interfaces.
Refresh	Displays manual refresh option must be used to refresh the above data.

Table 266: Enter LSYS page options

Field	Function	Action
Select Widget	Specifies the following widgets: <ul style="list-style-type: none"> • Logical System Profile. • Logical System CPU Profile. • Logical System FW No Hits. 	Drag and drop a widget to add it to your dashboard. Once widgets are added to the dashboard, they can be edited, refreshed, or removed by hovering over the widget header and selecting the option. The manual refresh option must be used to refresh the widget data.

Table 266: Enter LSYS page options (continued)

Field	Function	Action
Add Tabs	Specify to add the dashboards	Select (+) option to add a dashboard.

Table 267: Create-Edit the Logical System

Field	Function	Action
General		
Name	Displays the logical system name of a selected Resource Profile. Only one Resource Profile can be selected, per logical system.	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed; maximum length is 63 characters.
Create-Edit the security Profiles Click one: <ul style="list-style-type: none"> • Add icon (+)— Adds Resource Profiles. • Edit icon (/)— Edits the selected Resource Profiles. • Delete icon (X) — Deletes the selected Resource Profiles. • Search icon—Enables you to search a Resource Profile in the grid. • Filter icon — Enables you to filter the selected option in the grid. • Show Hide Column Filter icon—Enables you to show or hide a column in the grid. 		
Profile Name	Displays the name of the security profile.	Enter a unique string with an alphanumeric character and can include underscores; no spaces allowed; 31-character maximum.
IPS Policy	Specify the IPS Policy.	Select the IPS Policy
Resource Name		
nat-pat-portnum	Specify the maximum quantity and the reserved quantity of ports for the logical system as part of its security profile.	—
dslite-software-initiator	Specify the number of IPv6 dual-stack lite (DS-Lite) software initiators that can connect to the software concentrator configured in either a user logical system or the master logical system.	—
cpu	Specify the percentage of CPU utilization that is always available to a logical system.	—
appfw-rule	Specify the number of application firewall rule configurations that a master administrator can configure for a master logical system or user logical system when the security profile is bound to the logical systems.	—

Table 267: Create-Edit the Logical System (continued)

Field	Function	Action
nat-interface-port-ol	Specify the number of application firewall rule set configurations that a master administrator can configure for a master logical system or user logical system when the security profile is bound to the logical systems.	—
nat-rule-referenced-prefix	Specify the security NAT interface port overloading the quota of a logical system.	—
nat-port-ol-ipnumber	Specify the number of NAT port overloading IP number configurations that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.	—
nat-cone-binding	Specify the number of NAT cone binding configurations that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.	—
nat-static-rule	Specify the number of NAT static rule configurations that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.	—
nat-destination-rule	Specify the number of NAT destination rule configurations that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.	—
nat-source-rule	Specify the NAT source rule configurations that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.	—
nat-nopat-address	Specify the number of NAT without port address translation configurations that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.	—

Table 267: Create-Edit the Logical System (continued)

Field	Function	Action
nat-pat-address	Specify the number of NAT with port address translation (PAT) configurations that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.	—
nat-destination-pool	Specify the number of NAT destination pool configurations that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.	—
nat-source-pool	Specify the NAT source pool configurations that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.	—
flow-gate	Specify the number of flow gates, also known as pinholes that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.	—
flow-session	Specify the number of flow sessions that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.	—
policy	Specify the number of security policies with a count that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.	—
security-log-stream-number	Specify the Security log stream number quota of a logical system.	—
scheduler	Specify the number of schedulers that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.	—

Table 267: Create-Edit the Logical System (continued)

Field	Function	Action
zone	Specify the zones that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.	—
auth-entry	Specify the number of firewall authentication entries that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.	—
appfw-profile	Specify the application firewall profile quota of a logical system.	—
address-book	Specify the entries in the address book. Address book entries can include any combination of IPv4 addresses, IPv6 addresses, DNS names, wildcard addresses, and address range.	—
Reserved	Specify reserved quota that guarantees that the resource amount specified is always available to the logical system.	—
Maximum	Specify the maximum allowed quota.	—
Users Click one: <ul style="list-style-type: none"> • Add icon (+) — Create users. • Edit icon (/) — Edit the selected users. • Delete icon (X)— Delete the selected users. 		
Create-Edit users		
User Name	Displays the user name.	Maximum length is 64 characters.
Role	Specify the role of the user form the following options: <ul style="list-style-type: none"> • Logical System Administrator • Read only Access User <p>NOTE: LSYS Read Only user can only view the options but cannot modify them.</p>	Select any one option from the drop down list.
Password	Specify the password for the user.	Select a password which is more than 6 characters but less than 128 characters.
Confirm Password	Confirm the password.	Confirm the set password.

Table 267: Create-Edit the Logical System (continued)

Field	Function	Action
Interfaces Click One: <ul style="list-style-type: none"> • Enable/Disable — Enable or disable the physical interface. • Add icon (+) — Add logical interfaces. • Edit icon (/) —Edit the selected users. • Delete icon (X)— Delete the selected users. 		
Create-Edit logical interfaces		
Physical Interface Name	Displays the name of the Physical Interface.	Select a physical interface name from the grid.
Logical Interface Unit	Displays the logical Interface Unit	Enter the logical interface unit.
Description	Displays the description.	Enter the description.
VLAN ID	Displays the VLAN ID.	Enter the VLAN ID. VLAN ID is mandatory.
IPv4 Address	IPv4 Address	Enter a valid IP address.
Subnet Mask	Subnet Mask	Enter a valid subnet mask.
IPv6 Address	IPv6 Address	Enter a valid IP address.
Zones Click One: <ul style="list-style-type: none"> • Enable/Disable — Enable or disable the physical interface. • Add icon (+) — Create security zones. • Edit icon (/) —Edit the selected security zones. • Delete icon (X)— Delete the selected security zone. 		
Create-Edit Security Zones		
Name	Displays the name of the zones.	Enter a valid name of the zone.
Description	Displays the description of the zones.	Enter a description of the zone.
Application Tracking	Displays the application tracking support to the zone.	Enables the application tracking support.
Selected interface	Displays the selected interface.	Select an interface.

Table 267: Create-Edit the Logical System (continued)

Field	Function	Action
System service options		—

Table 267: Create-Edit the Logical System (continued)

Field	Function	Action
	<p>Select system services from the following options:</p> <ul style="list-style-type: none"> • all - Specify all system services. • any-service - Specify services on entire port range.. • appqoe- Specify the APPQOE active probe service. • bootp - Specify the Bootp and dhcp relay agent service. • dhcp - Specify the Dynamic Host Configuration Protocol. • dhcpv6- Enable Dynamic Host Configuration Protocol for IPV6. • dns- Specify the DNS service. • finger- Specify the finger service. • ftp- Specify the FTP protocol. • http – Specify the web management using HTTP. • https- Specify the web management using HTTP secured by SSL. • ident-reset- Specify the send back TCP RST IDENT request for port 113. • ike- Specify the Internet key exchange. • lsping-Specify the Label Switched Path ping service. • netconf- Specify the NETCONF Service. • ntp - Specify the network time protocol service. • ping – Specify the internet control message protocol. • r2cp-Enable Radio-Router Control Protocol service. • reverse-ssh-Specify the reverse SSH Service. • reverse-telnet-Specify the reverse telnet Service. • rlogin-Specify the Rlogin service • rpm-Specify the Real-time performance monitoring. • rsh-Specify the Rsh service. • snmp- Specify the Simple Network Management Protocol Service. • snmp-trap- Specify the Simple Network Management Protocol trap. • ssh-Specify the SSH service. • tcp-encap-Specify the TCP encapsulation service. • telnet-Specify the Telnet service. 	

Table 267: Create-Edit the Logical System (continued)

Field	Function	Action
	<ul style="list-style-type: none"> tftp-Specify the TFTP traceroute-Specify the traceroute service. webapi-clear-text-Specify the Webapi service using http. webapi-ssl-Specify the Webapi service using HTTP secured by SSL. xnm-clear-text-Specify the JUNOScript API for unencrypted traffic over TCP. xnm-ssl- Specify the JUNOScript API Service over SSL. 	
Protocols Options	<p>Select a protocol from the following options:</p> <ul style="list-style-type: none"> bfd - Bidirectional Forwarding Detection. bgp - Broder Gateway protocol. dvmp - Distance Vector Multicast Routing Protocol. igmp - Internet group management protocol. ldp - label Distribution Protocol. msdp- Multicast source discovery protocol. nhrp- Next Hop Resolution Protocol. ospf- Open shortest path first. ospf3- Open shortest path first version 3. pgm – Pragmatic General Multicast. pim- Protocol independent multicast. rip- Routing information protocol. ripng- Routing information protocol next generation. router-discovery- Router Discovery. rsvp- Resource reservation protocol. sap - Session Announcement Protocol. vrrp – Virtual Router redundancy protocol. 	—
Traffic Control Options	Specify the TCP Reset.	Send RST for NON-SYN packet not matching TCP session.

See Also • [Configuring Multi Tenancy Resource Profiles on page 476](#)

Configuring Multi Tenancy Resource Profiles

The Resource Profile page displays all the resource profiles or security profiles for the logical system along with the configured resources.

You can configure up to 32 security profiles on an SRX Series device running logical systems. When you reach the limit, you must delete a security profile and commit the configuration change before you can create and commit another security profile. In many cases fewer security profiles are needed because you might bind a single security profile to more than one logical system.

1. Select **Configure>Multi Tenancy>Resource Profiles**.

The Resource Profile page appears. [Table 268 on page 477](#) explains the content of this page.

2. Click one:

- **Global Settings**—Configures global options for the firewall policy. Enter information as specified in [Table 269 on page 478](#).

- **More**—Allows you to view a detailed view of the selected resource profile.

You can also view the details of a resource profile when you mouse over to the left of a resource profile and click on the Detailed View icon.

- Add icon (+)—Adds a new resource profile and IPS policy. Enter information as specified in [Table 270 on page 478](#).
- Edit icon (/)—Edits selected security profile. Enter information as specified in [Table 270 on page 478](#).
- Delete icon (X)—Deletes the selected security profile.
- Search icon—Enables you to search the security profile in the grid.
- Filter icon—Allows you to enter the desired Profile Name, Configured Resources, or Logical Systems/Tenants and display the matching results in the grid.
- Show Hide Column icon—Enables you to show or hide a column in the grid.

3. Click Commit icon at the top of the J-Web page. The following commit options are displayed.

- **Commit**—Commits the configuration and returns to the main configuration page.
- **Compare**—Enables you to compare the current configuration with the previous configuration.
- **Discard**—Discards the configuration changes you performed in the J-Web.
- **Preferences**—There are two tab:

Commit preferences—You can choose to just validate or validate and commit the changes.

Confirm commit timeout (in min) — You can select the time-out interval.

Table 268: Resource Profile page

Field	Function
Profile Name	Displays the Security Profile names.

Table 268: Resource Profile page (continued)

Field	Function
Configured Resource	Displays the configured resource.
Logical Systems/Tenants	Displays the logical system or tenants created.

Table 269: Global Settings option page

Field	Function	Action
Enable CPU limit	Specify the CPU control.	Enable or disable the CPU limit.
CPU Target	Specify the targeted CPU utilization allowed for the whole system (0..100 percent) .	Set a CPU target. You can enable disable this option to set the value. This will be applicable to all the logical system resource profiles. If u set 50 % here then none of the profile(s) can have a value more than this and all the profiles should share this 50% of the CPU.

Table 270: Create-Edit the Resource Profile:

Field	Function	Action
General		
Profile Name	Displays the name of the security profile.	Enter a unique string with an alphanumeric character and can include underscores; no spaces allowed; 31-character maximum.
IPS Policy	Specify the IPS Policy	Select the IPS Policy.
Resource Name		
nat-pat-portnum	Specify the maximum quantity and the reserved quantity of ports for the logical system as part of its security profile.	—
dslite-software-initiator	Specify the number of IPv6 dual-stack lite (DS-Lite) software initiators that can connect to the software concentrator configured in either a user logical system or the master logical system.	—
cpu	Specify the percentage of CPU utilization that is always available to a logical system.	—
appfw-rule	Specify the number of application firewall rule configurations that a master administrator can configure for a master logical system or user logical system when the security profile is bound to the logical systems.	—

Table 270: Create-Edit the Resource Profile: (continued)

Field	Function	Action
nat-interface-port-ol	Specify the number of application firewall rule set configurations that a master administrator can configure for a master logical system or user logical system when the security profile is bound to the logical systems.	—
nat-rule-referenced-prefix	Specify the security NAT interface port overloading the quota of a logical system.	—
nat-port-ol-ipnumber	Specify the number of NAT port overloading IP number configurations that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.	—
nat-cone-binding	Specify the number of NAT cone binding configurations that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.	—
nat-static-rule	Specify the number of NAT static rule configurations that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.	—
nat-destination-rule	Specify the number of NAT destination rule configurations that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.	—
nat-source-rule	Specify the NAT source rule configurations that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.	—
nat-nopat-address	Specify the number of NAT without port address translation configurations that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.	—

Table 270: Create-Edit the Resource Profile: (continued)

Field	Function	Action
nat-pat-address	Specify the number of NAT with port address translation (PAT) configurations that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.	—
nat-destination-pool	Specify the number of NAT destination pool configurations that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.	—
nat-source-pool	Specify the NAT source pool configurations that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.	—
flow-gate	Specify the number of flow gates, also known as pinholes that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.	—
flow-session	Specify the number of flow sessions that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.	—
policy	Specify the number of security policies with a count that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.	—
security-log-stream-number	Specify the security log stream number.	—
scheduler	Specify the number of schedulers that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.	—
zone	Specify the zones that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.	—

Table 270: Create-Edit the Resource Profile: (continued)

Field	Function	Action
auth-entry	Specify the number of firewall authentication entries that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.	—
appfw-profile	Specify the application firewall profile quota of a logical system.	—
address-book	Define entries in the address book. Address book entries can include any combination of IPv4 addresses, IPv6 addresses, DNS names, wildcard addresses, and address range.	—
Reserved	A reserved quota that guarantees that the resource amount specified is always available to the logical system.	—
Maximum	A maximum allowed quota.	—
Range	The minimum and maximum range permitted for each corresponding resource name.	—

See Also • [Configuring Multi Tenancy Logical Systems on page 466](#)

Configuring Multi Tenancy Tenants

The Tenants profile page displays the resource profile, users, assigned interfaces, zones, and routing instance of the configured tenant systems.

Tenant systems are used when you need to separate departments, organization, or customers and each of them can be limited to one virtual router. The main difference between a logical system and a tenant system is that a logical system supports advanced routing functionality using multiple routing instances. In comparison, a tenant system supports only one routing instance, but supports the deployment of significantly more tenants per system. A master administrator creates a tenant system and assigns an administrator for managing the tenant system. A tenant system can have multiple administrators.

Root users can switch to tenant context by navigating to Configure>Multi tenancy>Tenants page and selecting any one listed instance and clicking Enter TENANT respectively.

Roles supported for Tenant

J-Web supports the following roles with respect to tenant.

- Root user in normal mode
- Root user entering as tenant
- Tenant administrator
- Tenant read-only user



NOTE: Tenant administrator and read-only users are created from Tenant wizard by selecting appropriate roles.

If you have opened J-Web in multiple tabs in the browser, and if in one of the tab you switch mode to logical system or tenant, then the other instances of J-Web in the other tabs will automatically switch to logical system or tenant.

J-Web maintains different session for different protocols, such as http or https.

When you refresh the screen, you will not be logged out; instead the screen is refreshed, and you will continue in the same session.

1. Select **Configure>Multi Tenancy>Tenants**.

The Tenants page appears. [Table 271 on page 483](#) explains the contents of this page.

2. Click one:

- **Enter Tenant** —Select a tenant from the list and enter its system.
- **More**—Select this option to view the details of a selected tenant.
- **Add icon (+)**—Create a new tenant. Enter information as specified in [Table 272 on page 483](#).
- **Edit icon (/)**—Edit the selected tenant. Enter information as specified in [Table 272 on page 483](#).
- **Delete icon (X)**—Deletes the selected tenant system.
- **Search icon**— Enables you to search for a tenant system in the grid.
- **Filter icon** —Enables you to filter and display the list of tenants based on a column in the grid.
- **Show Hide Column icon** —Enables you to show or hide a column in the grid.

3. Click Commit icon at the top of the J-Web page. The following commit options are displayed.

- **Commit**—Commits the configuration and returns to the main configuration page.
- **Compare**—Enables you to compare the current configuration with the previous configuration.

- **Confirm Commit**—Commits the configuration; and after 10 minutes, the changes will be rolled back, and the previous configuration is restored.
- **Discard**—Discards the configuration changes you performed in the J-Web.
- **Preferences**—There are two tabs:

Commit preferences—You can choose to just validate or validate and commit the changes.

Confirm commit timeout (in min) —You can select the commit timeout interval.



NOTE: During report generation if you switch context, then a confirmation message is displayed. Click **Yes** to stop the report generation and to switch the context. Click **No** to continue to generate the report and not to switch context.

Table 271: Tenants Profile Page

Field	Function
Name	Displays the name of the tenant system.
Resource Profile	Displays the name of the resource profile.
Users	Displays the tenant system admin and users, and its associated permissions.
Assigned Interfaces	Displays the assigned logical interfaces.
Zones	Displays the zones for the tenant.
Routing Instance	Displays the routing instance that is explicitly assigned to the tenant system.

Table 272: Create-Edit Tenant System

Field	Function	Action
Tenant - General Details		
Name	Enter a name for the tenant.	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed; maximum length is 63 characters.
Routing Instance	By default the tenant name is taken as the routing instance name.	
Tenant Resource Profile		

Table 272: Create-Edit Tenant System (continued)

Field	Function	Action
Profile Name	Displays the name of the resource profile.	Enter a unique string with an alphanumeric character and can include underscores; no spaces allowed; 31-character maximum.
Configured Resources	Displays the resources and its reserved or maximum quantity assigned for this resource profile.	
Logical Systems/Tenants	Displays other logical systems and/or tenants using this resource profile.	

Click one:

- Add icon (+)—Adds resource profiles.
- Edit icon (/)—Edits the selected resource profiles.
- Search icon—Enables you to search a resource profile in the grid.
- Filter icon—Enables you to filter the selected option in the grid.
- Show Hide Column Filter icon—Enables you to show or hide a column in the grid.

Create-Edit Tenant Resource Profile

See [“Configuring Multi Tenancy Resource Profiles” on page 476](#) for details on creating and editing resource profile.

User Details

You can define tenant administrators and users.

Click one:

- Add icon (+)—Create users.
- Edit icon (/)—Edit the selected users.
- Delete icon—Delete the selected users.

Create-Edit users

User Name	Enter/displays user name.	Maximum length is 64 characters.
Role	Specify the role of the user from the following options: <ul style="list-style-type: none"> • Tenant Administrator • Read only Access User <p>NOTE: Logical system or tenant Read Only user can only view the options but cannot modify them.</p>	Select any one option from the drop down list.
Password	Specify the password for the user.	Select a password which is more than 6 characters but less than 128 characters.
Confirm Password	Confirm the password.	Confirm the set password.

Table 272: Create-Edit Tenant System (continued)

Field	Function	Action
Assign Interfaces		
Only one logical interface can be part of one tenant, whereas, a tenant can have multiple logical interfaces.		
Click One:		
<ul style="list-style-type: none"> • Enable/Disable —Enable or disable the physical interface. • Add icon (+)—Add logical interfaces. • Edit icon (/)—Edit the selected users. • Delete icon—Delete the selected users. 		
Create-Edit logical interfaces		
Physical Interface Name	Displays the name of the physical interface.	Select a physical interface name from the grid.
Logical Interface Unit	Displays the logical interface unit.	Enter the logical interface unit.
Description	Displays the description.	Enter the description.
VLAN ID	Displays the VLAN ID.	Enter the VLAN ID. VLAN ID is mandatory.
IPv4 Address	Displays the IPv4 address.	Enter a valid IP address.
Subnet Mask	Displays the subnet mask.	Enter a valid subnet mask.
IPv6 Address	Displays the IPv6 address.	Enter a valid IP address.
Zone Configuration		
Click One:		
<ul style="list-style-type: none"> • Enable/Disable — Enable or disable the physical interface. • Add icon (+) — Create security zones. • Edit icon (/) —Edit the selected security zones. • Delete icon (X)—Delete the selected security zone. 		
Create-Edit Security Zones		
Name	Displays the name of the zones.	Enter a valid name of the zone.
Description	Displays the description of the zones.	Enter a description of the zone.
Application Tracking	Displays the application tracking support to the zone.	Enables the application tracking support.
Selected interface	Displays the selected interface.	Select an interface.

Table 272: Create-Edit Tenant System (continued)

Field	Function	Action
System service options		—

Table 272: Create-Edit Tenant System (continued)

Field	Function	Action
	<p>Select system services from the following options:</p> <ul style="list-style-type: none"> all - Specify all system services. any-service - Specify services on entire port range.. appqoe- Specify the APPQOE active probe service. bootp - Specify the Bootp and dhcp relay agent service. dhcp - Specify the Dynamic Host Configuration Protocol. dhcpx6- Enable Dynamic Host Configuration Protocol for IPV6. dns- Specify the DNS service. finger- Specify the finger service. ftp- Specify the FTP protocol. http – Specify the web management using HTTP. https- Specify the web management using HTTP secured by SSL. ident-reset- Specify the send back TCP RST IDENT request for port 113. ike- Specify the Internet key exchange. lsping-Specify the Label Switched Path ping service. netconf- Specify the NETCONF Service. ntp - Specify the network time protocol service. ping – Specify the internet control message protocol. r2cp-Enable Radio-Router Control Protocol service. reverse-ssh-Specify the reverse SSH Service. reverse-telnet-Specify the reverse telnet Service. rlogin-Specify the Rlogin service rpm-Specify the Real-time performance monitoring. rsh-Specify the Rsh service. snmp- Specify the Simple Network Management Protocol Service. snmp-trap- Specify the Simple Network Management Protocol trap. ssh-Specify the SSH service. tcp-encap-Specify the TCP encapsulation service. telnet-Specify the Telnet service. 	

Table 272: Create-Edit Tenant System (continued)

Field	Function	Action
	<ul style="list-style-type: none"> • tftp-Specify the TFTP • traceroute-Specify the traceroute service. • webapi-clear-text-Specify the Webapi service using http. • webapi-ssl-Specify the Webapi service using HTTP secured by SSL. • xnm-clear-text-Specify the JUNOScript API for unencrypted traffic over TCP. • xnm-ssl- Specify the JUNOScript API Service over SSL. 	
Protocols Options	<p>Select a protocol from the following options:</p> <ul style="list-style-type: none"> • bfd - Bidirectional Forwarding Detection. • bgp - Broder Gateway protocol. • dvmrp - Distance Vector Multicast Routing Protocol. • igmp - Internet group management protocol. • ldp - label Distribution Protocol. • msdp- Multicast source discovery protocol. • nhrp- Next Hop Resolution Protocol. • ospf- Open shortest path first. • ospf3- Open shortest path first version 3. • pgm – Pragmatic General Multicast. • pim- Protocol independent multicast. • rip- Routing information protocol. • ripng- Routing information protocol next generation. • router-discovery- Router Discovery. • rsvp- Resource reservation protocol. • sap - Session Announcement Protocol. • vrrp – Virtual Router redundancy protocol. 	—
Traffic Control Options	Specify the TCP Reset.	Send RST for NON-SYN packet not matching TCP session.

See Also • [Configuring Multi Tenancy Resource Profiles on page 476](#)

Chassis Cluster

- [Chassis Cluster Configuration Page Options on page 489](#)
- [Chassis Cluster Setup Configuration Page Options on page 496](#)

Chassis Cluster Configuration Page Options

1. Select **Configure>Chassis Cluster>Cluster Configuration**.
The Chassis Cluster Configuration page appears. There are two tabs on this page—Node Settings and HA Cluster Settings. By default, the Node Settings tab is selected. [Table 273 on page 489](#) explains the contents of the Chassis Cluster Configuration page.
2. **Global Settings**—Starting Junos 18.1R1, if you are using a SRX4600 device, Global Settings option is available, using which you can change the speed of the control ports of the SRX4600 device.
 - Click Global Settings. The Global Settings window appears.
 - Select the speed from the dropdown. The options available are 1 Gbps and 10 Gbps.
3. Click one:
 - **Add**—Adds a new or duplicate chassis cluster configuration. Enter information as specified in [Table 274 on page 490](#).
 - **Edit**—Edits the selected chassis cluster configuration. Enter information as specified in [Table 275 on page 492](#).
 - **Delete**—Deletes the selected chassis cluster configuration.
4. Click one:
 - **OK**—Saves the configuration and returns to the main configuration page.
 - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
 - **Cancel**—Cancels your entries and returns to the main configuration page.

Table 273: Chassis Cluster Configuration Page

Field	Function
Node Settings	
Node ID	Displays the node ID.
Cluster ID	Displays the cluster ID configured for the node.
Host Name	Displays the name of the node.
Backup Router	Displays the IP address used while booting.

Table 273: Chassis Cluster Configuration Page (continued)

Field	Function
Management Interface	Displays the management interface of the node.
IP Address	Displays the management IP address of the node.
Status	Displays the state of the redundancy group. <ul style="list-style-type: none"> • Primary—Redundancy group is active. • Secondary—Redundancy group is passive.
HA Cluster Settings>Interfaces	
Name	Displays the physical interface name.
Member Interfaces/IP Address	Displays the member interface name or IP address configured for an interface.
Redundancy Group	Displays the redundancy group.
HA Cluster Settings>Redundancy Group	
Group	Displays the redundancy group identification number.
Preempt	Displays the selected Preempt option. <ul style="list-style-type: none"> • True—Mastership can be preempted based on priority. • False—Mastership cannot be preempt based on priority.
Gratuitous ARP Count	Displays the number of gratuitous ARP requests that a newly elected primary device in a chassis cluster sends out to announce its presence to the other network devices.
Node Priority	Displays the assigned priority for the redundancy group on that node. The eligible node with the highest priority is elected as primary for the redundant group.

Table 274: Add Node Setting Configuration Details

Field	Function	Action
Fabric Link > Fabric Link 0 (fab0)		
Interface	Specifies fabric link 0.	Enter the interface IP fabric link 0.
Add	Adds fabric interface 0.	Click Add.
Delete	Deletes fabric interface 0.	Click Delete.
Fabric Link > Fabric Link 1 (fab1)		
Interface	Specifies fabric link 1.	Enter the interface IP for fabric link 1.
Add	Adds fabric interface 1.	Click Add.

Table 274: Add Node Setting Configuration Details (continued)

Field	Function	Action
Delete	Deletes fabric interface 1.	Click Delete.
Redundant Ethernet		
Interface	Specifies a logical interface consisting of two physical Ethernet interfaces, one on each chassis.	Enter the logical interface.
IP	Specifies redundant Ethernet IP address.	Enter redundant Ethernet IP address.
Redundancy Group	Specifies redundancy group ID number in the chassis cluster.	Select one of the redundancy group from the list.
Add	Adds redundant Ethernet IP address.	Click Add.
Delete	Deletes redundant Ethernet IP address.	Click Delete.
Add Redundancy Group		
Redundancy Group	Specifies the redundancy group name.	Enter the redundancy group name.
Allow preemption of primaryship	Allows a node with a better priority to initiate a failover for a redundancy group. NOTE: By default, this feature is disabled. When disabled, a node with a better priority does not initiate a redundancy group failover (unless some other factor, such as faulty network connectivity identified for monitored interfaces, causes a failover).	—
Gratuitous ARP Count	Specifies the number of gratuitous Address Resolution Protocol requests that a newly elected master sends out on the active redundant Ethernet interface child links to notify network devices of a change in mastership on the redundant Ethernet interface links. The range is through 1 to 16. The default is 4.	Enter a value.
node0 priority	Specifies the priority value of node0 for a redundancy group.	Enter the node priority number as 0.
node1 priority	Specifies the priority value of node1 for a redundancy group.	Select the node priority number as 1.
Interface Monitor		
Interface	Specifies the number of redundant Ethernet interfaces to be created for the cluster.	Select the interface from the list.
Weight	Specifies the weight for the interface to be monitored. The ranges is from 1 through 125.	Enter a value.

Table 274: Add Node Setting Configuration Details (continued)

Field	Function	Action
Add	Adds interfaces to be monitored by the redundancy group and their respective weights.	Click Add.
Delete	Deletes interfaces to be monitored by the redundancy group along with their respective weights.	Select the interface from the configured list and click Delete.
IP Monitoring		
Weight	Specifies the weight for IP monitoring.	Enter a value.
Threshold	Specifies the global threshold for IP monitoring. The range is from 0 through 255.	Enter a value.
Retry Count	Specifies the number of retries needed to declare reachability failure. The range is from 5 through 15.	Enter a value.
Retry Interval	Specifies the time interval in seconds between retries. The range is from 1 through 30.	Enter a value.
IPv4 Addresses to Be Monitored		
IP	Specifies the IPv4 addresses to be monitored for reachability.	Enter the IPv4 addresses.
Weight	Specifies the weight for the redundancy group interface to be monitored.	Enter the weight.
Interface	Specifies the logical interface through which to monitor this IP address.	Enter the logical interface address.
Secondary IP address	Specifies the source address for monitoring packets on a secondary link.	Enter the secondary IP address.
Add	Adds the IPv4 addresses to be monitored.	Click Add.
Delete	Delete the IPv4 address.	Select the item from the list and click Delete.

Table 275: Edit Node Setting Configuration Details

Field	Function	Action
Node Settings		
Host Name	Specifies the name of the host.	Enter the name of the host.
Backup Router	Specifies the backup router to be used during failover.	Enter the backup router address.

Table 275: Edit Node Setting Configuration Details (continued)

Field	Function	Action
Destination		
IP	Specifies the destination IP address.	Enter the destination IP address.
Add	Adds the destination address.	Click Add.
Delete	Deletes the destination address.	Click Delete.
Interface		
Interface	Specifies the interfaces available for the router. <i>NOTE:</i> Allows you to add and edit two interfaces for each fabric link.	Select an option.
IP	Specifies the interface IP address.	Enter the interface IP address.
Add	Adds the interface.	Click Add.
Delete	Deletes the interface.	Click Delete.

Table 276: Add HA Cluster Setting Configuration Details

Field	Function	Action
Fabric Link > Fabric Link 0 (fab0)		
Interface	Specifies fabric link 0.	Enter the interface IP fabric link 0.
Add	Adds fabric interface 0.	Click Add.
Delete	Deletes fabric interface 0.	Click Delete.
Fabric Link > Fabric Link 1 (fab1)		
Interface	Specifies fabric link 1.	Enter the interface IP for fabric link 1.
Add	Adds fabric interface 1.	Click Add.
Delete	Deletes fabric interface 1.	Click Delete.
Redundant Ethernet		
Interface	Specifies a logical interface consisting of two physical Ethernet interfaces, one on each chassis.	Enter the logical interface.
IP	Specifies the redundant Ethernet IP address.	Enter the redundant Ethernet IP address.
Redundancy Group	Specifies redundancy group ID number in the chassis cluster.	Select one of the redundancy groups from the list.

Table 276: Add HA Cluster Setting Configuration Details (continued)

Field	Function	Action
lacp	Specifies the mode in which Link Aggregation Control Protocol (LACP) packets are exchanged between the interfaces. The modes are: <ul style="list-style-type: none"> • Active—Indicates that the interface initiates transmission of LACP packets. • Passive—Indicates that the interface only responds to LACP packets. 	Select an option.
periodic	Specifies the periodicity mode in which LACP packets are exchanged between the interfaces. The modes are: <ul style="list-style-type: none"> • fast—Indicates that the interface initiates a faster transmission of LACP packets. • slow—Indicates that the interface only responds to LACP packets. 	
Add	Adds the redundant Ethernet IP address.	Click Add.
Delete	Deletes the redundant Ethernet IP address.	Click Delete.
Add Redundancy Group		
Redundancy Group	Specifies the redundancy group name.	Enter the redundancy group name.
Allow preemption of primaryship	Allows a node with a better priority to initiate a failover for a redundancy group. <p>NOTE: By default, this feature is disabled. When disabled, a node with a better priority does not initiate a redundancy group failover (unless some other factor, such as faulty network connectivity identified for monitored interfaces, causes a failover).</p>	—
Gratuitous ARP Count	Specifies the number of gratuitous Address Resolution Protocol requests that a newly elected master sends out on the active redundant Ethernet interface child links to notify network devices of a change in mastership on the redundant Ethernet interface links. <p>The range is from 1 through 16. The default is 4.</p>	Enter a value.
node0 priority	Specifies the priority value of node0 for a redundancy group.	Enter the node priority number as 0.
node1 priority	Specifies the priority value of node1 for a redundancy group.	Select the node priority number as 1.

Table 276: Add HA Cluster Setting Configuration Details (continued)

Field	Function	Action
Interface Monitor		
Interface	Specifies the number of redundant Ethernet interfaces to be created for the cluster.	Select the interface from the list.
Weight	Specifies the weight for the interface to be monitored. The range is from 1 through 125.	Enter a value.
Add	Adds interfaces to be monitored by the redundancy group and their respective weights.	Click Add.
Delete	Deletes interfaces to be monitored by the redundancy group along with their respective weights.	Select the interface from the configured list and click Delete.
IP Monitoring		
Weight	Specifies the global threshold for IP monitoring. The range is from 0 through 255.	Enter a value.
Threshold	Specifies the global threshold for IP monitoring. The range is from 0 through 255.	Enter a value.
Retry Count	Specifies the number of retries needed to declare reachability failure. The range is from 5 through 15.	Enter a value.
Retry Interval	Specifies the time interval in seconds between retries. The range is from 1 through 30.	Enter a value.
IPv4 Addresses to be monitored		
IP	Specifies the IPv4 addresses to be monitored for reachability.	Enter the IPv4 addresses.
Weight	Specifies the weight for the redundancy group interface to be monitored.	Enter the weight.
Interface	Specifies the logical interface through which to monitor this IP address.	Enter the logical interface address.
Secondary IP address	Specifies the source IPv4 address for monitoring packets on a secondary link.	Enter the secondary IP address.
Add	Adds the IPv4 addresses to be monitored.	Click Add.
Delete	Delete the IPv4 address.	Select the item from the list and click Delete.

See Also • [Chassis Cluster Setup Configuration Page Options on page 496](#)

Chassis Cluster Setup Configuration Page Options

1. Select **Configure>Chassis Cluster>Setup**.

The Chassis Cluster Setup configuration page appears. [Table 277 on page 496](#) explains the contents of this page.

2. Click one:

- **Enable**—Enables cluster mode on the node.
 - **Enable and Reboot**—Enables cluster mode and reboots the node.
 - **Enable and No Reboot**—Enables cluster mode without rebooting the node.
- **Disable**—Disables the cluster mode on the node.
 - **Disable and Reboot**—Disables cluster mode and reboots the node.
 - **Disable and No Reboot**—Disables cluster mode without rebooting the node.
- **Reset**—Resets your entries to the original value.

3. Click one:

- **OK**—Saves the configuration and returns to the main configuration page.
- **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
- **Cancel**—Cancels your entries and returns to the main configuration page.

Table 277: Add Chassis Cluster Setup Configuration Details

Field	Function	Action
Cluster ID	Specifies the number by which a cluster is identified.	Enter a number from 0 through 15.
Node		
Node ID	Specifies the number by which a node is identified.	Enter a number from 0 through 1.
Node Management IP Address (fxp0.0)	Specifies the management IP address of a node.	Enter a valid IP address for the management interface.
Control Link		
Fpc	Specifies the FPC control link.	Select the FPC number from the list.
Port	Specifies the port to configure for the control link.	Enter a number from 0 through 2.

See Also • [Chassis Cluster Configuration Page Options on page 489](#)

CLI Tools

- [CLI Viewer Configuration Page Options on page 497](#)
- [CLI Editor Configuration Page Options on page 498](#)
- [Point and Click Configuration Page Options on page 498](#)

CLI Viewer Configuration Page Options

1. Select **Configure>CLI Tools>CLI Viewer**.

The CLI Viewer page appears, showing the current configuration running on the device.



NOTE:

- The configuration statements appear in a fixed order irrespective of the order in which you configured the routing platform. The top of the configuration displays a timestamp indicating when the configuration was last changed and the current version.
- Each level in the hierarchy is indented to indicate each statement's relative position in the hierarchy. Each level is generally set off with braces, using an open brace ({) at the beginning of each hierarchy level and a closing brace (}) at the end. If the statement at a hierarchy level is empty, the braces are not displayed. Each leaf statement ends with a semicolon (;), as does the last statement in the hierarchy.
- The indented representation is used when the configuration is displayed or saved as an ASCII file. However, when you load an ASCII configuration file, the format of the file is not so strict. The braces and semicolons are required, but the indentation and use of new lines are not required in ASCII configuration files.

2. Click one:

- **OK**—Saves the configuration and returns to the main configuration page.
- **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
- **Cancel**—Cancels your entries and returns to the main configuration page.

- See Also**
- [CLI Editor Configuration Page Options on page 498](#)
 - [Point and Click Configuration Page Options on page 498](#)

CLI Editor Configuration Page Options

1. Select **Configure>CLI Tools>CLI Editor**.

The CLI Editor configuration page appears. This page allows you to configure all routing platform services that you can configure from the Junos CLI.

2. Navigate to the hierarchy level you want to edit. Edit the candidate configuration using standard text editor operations—insert lines (with the Enter key), delete lines, modify, copy, and paste text.
3. Click **Commit** to load and commit the configuration. This saves the edited configuration, which replaces the existing configuration. The device checks the configuration for the correct syntax before committing it. If any errors occur when the configuration is loading or committed, they are displayed and the previous configuration is restored.
4. Click one:
 - **OK**—Saves the configuration and returns to the main configuration page.
 - **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
 - **Cancel**—Cancels your entries and returns to the main configuration page.



NOTE: When you edit the ASCII configuration file, you can add comments of one or more lines. Comments must precede the statement they are associated with. If you place the comments in other places in the file, such as on the same line after a statement or on a separate line following a statement, they are removed when you click Commit. Comments must begin and end with special characters. For more information, see the *Junos OS CLI User Guide*.

- See Also**
- [Point and Click Configuration Page Options on page 498](#)
 - [CLI Viewer Configuration Page Options on page 497](#)

Point and Click Configuration Page Options

1. Select **Configure>CLI Tools>Point and Click CLI**.

The Configuration page appears. [Table 278 on page 499](#) explains how to edit the configuration on a series of pages of clickable options that step you through the hierarchy. [Table 279 on page 499](#) lists key J-Web configuration editor tasks and their functions.



NOTE: Options changes for each device. For a device, if a feature is not yet configured, you have the option to first configure the feature. If the feature is already configured, you have the option to edit or delete the feature on that particular device.

2. Click one:

- **Refresh**—Refreshes and updates the display with any changes to the configuration made by other users.
- **Commit**—Verifies edits and applies them to the current configuration file running on the device.
- **Discard**—Removes edits applied to, or deletes existing statements or identifiers from, the candidate configuration.

3. Click one:

- **OK**—Saves the configuration and returns to the main configuration page.
- **Commit Options>Commit**—Commits the configuration and returns to the main configuration page.
- **Cancel**—Cancels your entries and returns to the main configuration page.

Table 278: Point and Click Configuration Details

Field	Function	Action
Configuration	<p>Specifies that you can edit the selected configuration on a series of pages of clickable options that step you through the hierarchy. The options available are:</p> <ul style="list-style-type: none"> • Expand all—Expands the hierarchy of all statements. • Hide all—Hides the hierarchy of all statements. • (+)—Expands an individual statement in the hierarchy. • (-)—Hides an individual statement in the hierarchy. 	Click one option.

Table 279: J-Web Configuration Editor Page Details

Field	Function	Action
Access	<p>Specifies that you can edit or delete access and user authentication methods to the device. The options available are:</p> <ul style="list-style-type: none"> • Edit—Edits the feature. • Delete—Deletes the feature. 	Click an option.

Table 279: J-Web Configuration Editor Page Details (continued)

Field	Function	Action
Accounting options	Specifies that you can configure accounting options such as log data about basic system operations and services on the device. The option available is: <ul style="list-style-type: none"> • Configure—Configures the feature. 	Click the option.
Applications	Specifies that you can edit or delete applications functions of the Junos OS and their properties on the device. The options available are: <ul style="list-style-type: none"> • Edit—Edits the feature • Delete—Deletes the feature. 	Click an option.
Chassis	Specifies that you can configure alarms and other chassis properties on the device. The option available is: <ul style="list-style-type: none"> • Configure—Configures the feature. 	Click the option.
Class of service	Specifies that you can edit or delete the Class-of-Service feature. The options available are: <ul style="list-style-type: none"> • Edit—Edits the feature • Delete—Deletes the feature. 	Click one option.
Ethernet switching options	Specifies that you can configure Ethernet switching options on the device. The option available is: <ul style="list-style-type: none"> • Configure—Configures the feature. 	Click the option.
Event options	Specifies that you can configure diagnostic event policies and actions associated with each policy. The option available is: <ul style="list-style-type: none"> • Configure—Configures the feature. 	Click the option.
Firewall	Specifies that you can configure stateless firewall filters—also known as ACLs—on the device. The option available is: <ul style="list-style-type: none"> • Configure—Configures the feature. 	Click the option.
Forwarding options	Specifies that you can configure forwarding option protocols, including flow monitoring, accounting properties, and packet capture. The option available is: <ul style="list-style-type: none"> • Configure—Configures the feature. 	Click the option.

Table 279: J-Web Configuration Editor Page Details (continued)

Field	Function	Action
Interfaces	Specifies that you can edit or delete interfaces on the device. The options available are: <ul style="list-style-type: none"> • Edit—Edits the feature. • Delete—Deletes the feature. 	Click an option.
Multicast snooping options	Specifies that you can configure multicast snooping options. The option available is: <ul style="list-style-type: none"> • Configure—Configures the feature. 	Click the option.
Poe	Specifies that you can edit or delete Power over Ethernet options on the device. The options available are: <ul style="list-style-type: none"> • Edit—Edits the feature. • Delete—Deletes the feature. 	Click an option.
Policy options	Specifies that you can configure routing policies that control information from routing protocols that the device imports into its routing table and exports to its neighbors. The option available is: <ul style="list-style-type: none"> • Configure—Configures the feature. 	Click the option.
Protocols	Specifies that you can edit or delete routing protocols, including Intermediate System-to-Intermediate System (IS-IS), OSPF, RIP, Routing Information Protocol Next Generation (RIPng), and BGP. The options available are: <ul style="list-style-type: none"> • Edit—Edits the feature. • Delete—Deletes the feature. 	Click an option.
Routing instances	Specifies that you can configure a hierarchy to configure routing instances. The options available are: <ul style="list-style-type: none"> • Configure—Configures the feature. 	Click the option.
Routing options	Specifies that you can edit or delete protocol-independent routing properties. The options available are: <ul style="list-style-type: none"> • Edit—Edits the feature. • Delete—Deletes the feature. 	Click an option.
Schedulers	Specifies that you can determine the day and time when security policies are in effect. The option available is: <ul style="list-style-type: none"> • Configure—Configures the feature. 	Click the option.

Table 279: J-Web Configuration Editor Page Details (continued)

Field	Function	Action
Security	<p>Specifies that you can edit or delete the rules for the transit traffic and the actions that need to take place on the traffic as it passes through the firewall; and to monitor the traffic attempting to cross from one security zone to another. The options available are:</p> <ul style="list-style-type: none"> • Edit—Edits the feature. • Delete—Deletes the feature. 	Click an option.
Services	<p>Specifies that you can configure real-time performance monitoring (RPM) on the device. The option available is:</p> <ul style="list-style-type: none"> • Configure—Configures the feature. 	Click an option.
Smtp	<p>Specifies that you can configure Simple Mail Transfer Protocol. The option available is:</p> <ul style="list-style-type: none"> • Configure—Configures the feature. 	Click the option.
Snmp	<p>Specifies that you can configure Simple Network Management Protocol for monitoring router operation and performance. The option available is:</p> <ul style="list-style-type: none"> • Configure—Configures the feature. 	Click an option.
System	<p>Specifies that you can edit or delete system management functions, including the device's hostname, address, and domain name; the addresses of the DNS servers; user login accounts, including user authentication and the root-level user account; time zones and NTP properties; and properties of the device's auxiliary and console ports. The options available are:</p> <ul style="list-style-type: none"> • Edit—Edits the feature. • Delete—Deletes the feature. 	Click one option.
Vlans	<p>Specifies that you can edit or delete a virtual LAN. The options available are:</p> <ul style="list-style-type: none"> • Edit—Edits the feature. • Delete—Deletes the feature. 	Click one option.
Wlan	<p>Specifies that you can configure a wireless local area network. The option available is:</p> <ul style="list-style-type: none"> • Configure—Configures the feature. 	Click the option.
Access profile		
Access profile name	Specifies the access profile name.	Enter an access profile name.

Table 279: J-Web Configuration Editor Page Details (continued)

Field	Function	Action
Advanced		
Add new entry	Specifies that you can add a new identifier to a statement.	Click Add new entry to add a new identifier.

- See Also**
- [CLI Viewer Configuration Page Options on page 497](#)
 - [CLI Editor Configuration Page Options on page 498](#)

Reports

- [Reports on page 505](#)

Reports

Purpose Use the Reports menu to generate reports on demand. There are several predefined reports listed in this page, see [Table 280 on page 506](#). The generated report is displayed in HTML format. You can group multiple reports and generate a consolidated report.

Starting in Junos OS Release 18.1R1, the following predefined group of reports are available.

- Application and User Usage
- Top Talkers
- IPS Threat Environment
- URL Report
- Viruses Blocked



NOTE: A few pre-existing reports that were available in the previous Junos OS releases are grouped within these reports.

Starting in Junos OS Release 18.4R1, Threat Assessment Report is available as a predefined group of reports.



NOTE: Starting in Junos OS Release 19.1R1, Threat Assessment report content will support the following charts:

- Top Web Categories for Security High—Displays only high severities and top 10 web categories.
- Top Web Categories—Displays top 10 web categories.
- Top Users Accessing Risky Websites—Displays top 10 values.
- Top URL Categories for Security Risk (High and Medium)—Displays both high and medium severities and top 10 values.
- Top URL Categories for Productivity Loss—Displays top 10 values.
- Top URL Categories for Legal Liability—Displays top 10 values.

Table 280 on page 506 lists the predefined group reports and the supported users.



NOTE: Starting in Junos OS Release 19.1R1, logical system and tenant support the reports listed in Table 280 on page 506 only for SRX1500, SRX4100, SRX4200, and SRX4600.

Table 280: Predefined Group Reports and Supported Users

Report Name	Report Content	Root	Logical System	Tenant
Threat Assessment Report	Executive Summary	Yes	Yes	Yes
	Application Risk Assessment	Yes	Yes	Yes
	Threat & Malware Assessment	Yes	Yes	Yes
	User and Web Access Assessment	Yes	Yes	Yes

Table 280: Predefined Group Reports and Supported Users (continued)

Report Name	Report Content	Root	Logical System	Tenant
Application and User Usage	Top High Risk Applications by Bandwidth	Yes	Yes	Yes
	Top High Risk Applications By Count	Yes	Yes	Yes
	Top Categories By Bandwidth	Yes	Yes	Yes
	Top Applications By Bandwidth	Yes	Yes	Yes
	Top Categories By Count	Yes	Yes	Yes
	Top Applications By Count	Yes	Yes	Yes
	Top Users Of High Risk Applications By Bandwidth	Yes	Yes	Yes
	Top Users By Bandwidth	Yes	Yes	Yes
	High Risk Applications Allowed Per User	Yes	Yes	Yes
	High Risk Applications Blocked Per User	Yes	Yes	Yes

Table 280: Predefined Group Reports and Supported Users (continued)

Report Name	Report Content	Root	Logical System	Tenant
Top Talkers	Top Source IPs by Bandwidth	Yes	Yes	Yes
	Top Destination IPs by Bandwidth	Yes	Yes	Yes
	Top Source IPs by Session	Yes	Yes	Yes
	Top Destination IPs by Session	Yes	Yes	Yes
	Top Users By Bandwidth	Yes	Yes	Yes
	Top Users By Count	Yes	Yes	Yes
IPS Threat Environment	IPS Attacks by Severity Over Time	Yes	Yes	No
	Total IPS Attacks by Severity	Yes	Yes	No
	Top IPS Categories Blocked	Yes	Yes	No
	Top IPS Attacks Blocked	Yes	Yes	No
	Top Targeted Hosts by IP	Yes	Yes	No
	Top Targeted Hosts by User	Yes	Yes	No

Table 280: Predefined Group Reports and Supported Users (continued)

Report Name	Report Content	Root	Logical System	Tenant
URL Report	Top URLs by Bandwidth	Yes	Yes	No
	Top URLs by Count	Yes	Yes	No
	Top URL Categories by Bandwidth	Yes	Yes	No
	Top URL Categories by Count	Yes	Yes	No
	Total URLs Blocked Over Time	Yes	Yes	No
	Top Blocked URLs	Yes	Yes	No
	Top Blocked URL Categories by Count	Yes	Yes	No
	Users With Most Blocked URLs	Yes	Yes	No
Viruses Blocked	Total Viruses Blocked Over Time	Yes	Yes	No
	Top Viruses Blocked	Yes	Yes	No
Virus: Top Blocked	Virus: Top Blocked	Yes	Yes	No
Top Firewall Events	Top Firewall Events	Yes	Yes	Yes
Top Firewall Deny Destinations	Top Firewall Deny Destinations	Yes	Yes	Yes
Top Firewall Service Deny	Top Firewall Service Deny	Yes	Yes	Yes
Top Firewall Denies	Top Firewall Denies	Yes	Yes	Yes

Table 280: Predefined Group Reports and Supported Users (continued)

Report Name	Report Content	Root	Logical System	Tenant
Top IPS Events	Top IPS Events	Yes	Yes	No
Top Anti-spam Detected	Top Anti-spam Detected	Yes	Yes	No
Top Screen Attackers	Top Screen Attackers	Yes	Yes	Yes
Top Screen Victims	Top Screen Victims	Yes	Yes	Yes
Top Screen Hits	Top Screen Hits	Yes	Yes	Yes
Top Firewall Rules	Top Firewall Rules	Yes	Yes	Yes
Top Firewall Deny Sources	Top Firewall Deny Sources	Yes	Yes	Yes
Top IPS Attack Sources	Top IPS Attack Sources	Yes	Yes	No
Top IPS Attack Destinations	Top IPS Attack Destinations	Yes	Yes	No
Top IPS Rules	Top IPS Rules	Yes	Yes	No
Top Web Apps	Top Web Apps	Yes	Yes	No
Top Roles	Top Roles	Yes	Yes	No
Top Applications Blocked	Top Applications Blocked	Yes	Yes	No
Top URLs by User	Top URLs by User	Yes	Yes	No
Top Source Zone by Volume	Top Source Zone by Volume	Yes	Yes	Yes
Top Applications by User	Top Applications by User	Yes	Yes	Yes
Top Botnet Threats By Source Address via IDP Logs	Top Botnet Threats By Source Address via IDP Logs	Yes	Yes	No

Table 280: Predefined Group Reports and Supported Users (continued)

Report Name	Report Content	Root	Logical System	Tenant
Top Botnet Threats by Destination Address via IDP Logs	Top Botnet Threats by Destination Address via IDP Logs	Yes	Yes	No
Top Botnet Threats by Threat Severity via IDP Logs	Top Botnet Threats by Threat Severity via IDP Logs	Yes	Yes	No
Top Malware Threats by Source Address via IDP Logs	Top Malware Threats by Source Address via IDP Logs	Yes	Yes	No
Top Malware Threats by Destination Address via IDP Logs	Top Malware Threats by Destination Address via IDP Logs	Yes	Yes	No
Top Malware Threats by Threat Severity via IDP Logs	Top Malware Threats by Threat Severity via IDP Logs	Yes	Yes	No
Top Blocked Applications via Webfilter Logs	Top Blocked Applications via Webfilter Logs	Yes	Yes	No
Top Permitted Application Subcategories by Volume via Webfilter Logs	Top Permitted Application Subcategories by Volume via Webfilter Logs	Yes	Yes	No
Top Permitted Application Subcategories by Count via Webfilter Logs	Top Permitted Application Subcategories by Count via Webfilter Logs	Yes	Yes	No

Action To view and download reports, click **Reports** in the top level menu.

Predefined report names, their description, and type is listed in a grid format.

You can select single or multiple report names or all the predefined report names and generate a consolidated report.

After you select the report names, click **Generate Report**.

The Report Title popup window opens.

Enter a Name for your report. You may enter a description. You must select the number of records you want in the report by selecting a number in **Show Top**.

In the **Show Details** section, Select All or Top Selected to display all the details or only the top selected details in the report.

Starting in Junos OS Release 18.1R1, you can select a predefined time span. In the Time Span list, select the predefined time span from where you want the report generated. You may also enter a custom time span by selecting Custom from the list.

You can order your reports by clicking the arrow next to **Sorting Options**. You may select to display reports from Largest to Smallest or Smallest to Largest details.

Click **Save**. The report is generated in HTML format and prompts you to save the file.

You can view the report by opening it from the location where you saved it or by opening it from the file icon listed at the bottom of the Reports page.

The opening page of the report shows the time when it was generated. A table of contents is generated if you have selected multiple reports. Each report displays information in a bar graph and tabular format. If there is no data to be represented, the report says **-No Data Available-**.

Release History Table

Release	Description
19.1R1	Starting in Junos OS Release 19.1R1, Threat Assessment report content will support the following charts:
19.1R1	Starting in Junos OS Release 19.1R1, logical system and tenant support the reports listed in Table 280 on page 506 only for SRX1500, SRX4100, SRX4200, and SRX4600.
18.4R1	Starting in Junos OS Release 18.4R1, Threat Assessment Report is available as a predefined group of reports.
18.1R1	Starting in Junos OS Release 18.1R1, the following predefined group of reports are available.
18.1R1	Starting in Junos OS Release 18.1R1, you can select a predefined time span.

Related Documentation

- [Traffic Monitoring Report](#)
- [Monitoring Address Pools on page 20](#)

CHAPTER 5

Administration

- [Devices on page 513](#)
- [License Management on page 524](#)
- [Certificate Management on page 527](#)
- [Ping Host on page 550](#)
- [Ping MPLS on page 553](#)
- [Traceroute on page 557](#)
- [Network Monitoring on page 560](#)
- [RPM on page 566](#)
- [Packet Capture on page 574](#)
- [CLI Terminal on page 578](#)
- [SKY ATP Enrollment on page 580](#)

Devices

- [Maintaining Files on page 513](#)
- [Maintaining Reboot Schedule on page 515](#)
- [Maintaining System Snapshots on page 517](#)
- [Software on page 519](#)
- [Config Management on page 521](#)

Maintaining Files

1. Select **Maintain>Files** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platform.

Or

Select **Administration>Devices>Files** in the J-Web user interface.

The Files page appears. [Table 281 on page 514](#) explains the contents of this page.

2. Click **Clean Up Files**. The device rotates log files and identifies the files that can be safely deleted.

The J-Web interface displays the files that you can delete and the amount of space that will be freed on the file system.

3. Click one:

- **OK** — Deletes the files and returns to the Files page.
- **Cancel** — Cancels your entries and returns to the list of files in the directory.

Enter the information specified in [Table 281 on page 514](#) to maintain the secure router.

Table 281: Clean Up Files Maintenance Options

Field	Function	Action
Clean Up Files		
Rotates log files	Indicates all information in the current log files is archived and fresh log files are created.	—
Deletes log files in /var/log	Indicates any files that are not currently being written to are deleted.	—
Deletes temporary files in /var/tmp	Indicates any files that have not been accessed within two days are deleted.	—
Deletes all crash files in /var/crash	Indicates any core files that the device has written during an error are deleted.	—
Deletes all software images (*.tgz files) in /var/sw/pkg	Indicates any software image copied to this directory during software upgrades are deleted.	—
Download and Delete Files		
Log Files	<p>Lists the log files located in the /var/log directory on the device.</p> <p>The available options are:</p> <ul style="list-style-type: none"> • Delete—Deletes files. • Download—Downloads files. 	Select an option.
Temporary Files	<p>Lists the temporary files located in the /var/tmp directory on the device.</p> <p>The available options are:</p> <ul style="list-style-type: none"> • Delete—Deletes files. • Download—Downloads files. 	Select an option.

Table 281: Clean Up Files Maintenance Options (continued)

Jailed Temporary Files	<p>Lists the jailed temporary files located in the <code>/var/jail/tmp</code> directory on the device.</p> <p>The available options are:</p> <ul style="list-style-type: none"> • Delete—Deletes files. • Download—Downloads files. 	Select an option.
Old JUNOS Software	<p>Lists the software images located in the <code>/var/sw/pkg (*.tgz files)</code> directory on the device.</p> <p>The available options are:</p> <ul style="list-style-type: none"> • Delete—Deletes files. • Download—Downloads files. 	Select an option.
Crash (Core) File	<p>Lists the core files located in the <code>/var/crash</code> directory on the device.</p> <p>The available options are:</p> <ul style="list-style-type: none"> • Delete—Deletes files. • Download—Downloads files. 	Select an option.
Database Files	<p>Lists the database files located in the <code>/var/db</code> directory on the device.</p> <p>The available options are:</p> <ul style="list-style-type: none"> • Delete—Deletes files. • Download—Downloads files. 	Select an option.
Delete Backup JUNOS Package		
Delete backup Junos package	<p>Reviews the backup image information listed.</p> <p>The available options are:</p> <ul style="list-style-type: none"> • OK—Deletes the backup image and returns to the Files page. • Cancel—Cancels the deletion of the backup image and returns to the Files page. 	<p>Click Delete backup JUNOS package and then select an option.</p> <p>NOTE: Delete backup option is hidden if the router is in dual-root partitioning scheme</p>

- See Also**
- [Maintaining Configuration Management Upload Files on page 521](#)
 - [Maintaining Reboot Schedule on page 515](#)

Maintaining Reboot Schedule

Select **Maintain>Reboot** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.

Or

Select **Administration>Devices>Reboot** in the J-Web user interface.

The Reboot maintain page appears.

Provide the information specified in [Table 282 on page 516](#) to maintain the secure router.

Table 282: Reboot Schedule Maintenance Options

Field	Function	Action
Reboot Immediately	Reboots the device immediately.	Select this option to reboot the device immediately.
Reboot in <i>number of</i> minutes	Reboots the device in the number of minutes from the current time.	Select this option to reboot the device after the specified number of minutes from the current time.
Reboot when the system time is <i>hour:minute</i>	Reboots the device at the absolute time that you specify, on the current day.	Select a two-digit hour in 24-hour format and a two-digit minute.
Halt Immediately	Stops the device software immediately. After the software has stopped, you can access the device through the console port only.	Select this option to stop the device immediately.
Reboot From Media	Reboots the device from the specified media type.	Choose the boot device from the Reboot From Media list: <ul style="list-style-type: none"> • internal—Reboots from the internal media (default). • usb—Reboots from the USB storage device.
Message	Displays a message to the user on the device before the reboot occurs.	Type a message to be displayed to the user on the device before the reboot occurs.

Table 282: Reboot Schedule Maintenance Options (continued)

Field	Function	Action
Schedule	Schedules a reboot based on the information specified in the previous fields.	<p>Select this option to schedule a reboot. The J-Web interface requests confirmation to perform the reboot or to halt. Click:</p> <ul style="list-style-type: none"> • OK— Confirms the operation. <ul style="list-style-type: none"> • 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 interface Reboot page. • If 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. <p>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 lights during startup and remains steadily green when the device is operating normally.</p> • Cancel—Cancels your entries and returns to the main configuration page.

- See Also**
- [Maintaining Licenses on page 524](#)
 - [Maintaining System Snapshots on page 517](#)

Maintaining System Snapshots

1. Select **Maintain>Snapshot** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platform.
- Or

Select **Administration>Devices>Snapshot** in the J-Web user interface.

The Snapshot page appears. [Table 283 on page 518](#) explains the contents of this page.

2. Click **Snapshot** — Creates a boot device on an alternate medium.
3. Click one :
 - **OK** — Performs the system snapshot to an medium.
 - **Cancel** — Cancels the system snapshot to another medium.

Enter the information specified in [Table 283 on page 518](#) to maintain the secure router.

Table 283: Snapshot Maintenance Options

Field	Function	Action
Target Media	<p>Specifies the boot device to copy the snapshot to.</p> <p>NOTE: You cannot copy software to the active boot device.</p> <p>The available options for a boot device that is not the active boot device:</p> <ul style="list-style-type: none"> • internal — Copies software to the internal media. • usb — Copies software to the device connected to the USB port. 	Select an option.
Factory	<p>Copies only the 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.</p> <p>NOTE: After a boot device is created with the default factory configuration, it can operate only in an internal media slot.</p>	Select the check box.
Partition	Partitions the medium. This process is usually necessary for boot devices that do not already have software installed on them.	Select the check box.

- See Also**
- [Maintaining Configuration Management Upload Files on page 521](#)
 - [Maintaining Reboot Schedule on page 515](#)

Software

- [Maintaining Software Upload Packages on page 519](#)
- [Maintaining Software Install Packages on page 519](#)
- [Maintaining Software Downgrades on page 520](#)

Maintaining Software Upload Packages

1. Select **Maintain>Software>Upload Package** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platform.

Or

Select **Administration>Devices>Software>Upload Package** in the J-Web user interface.

The Upload Package maintain page appears.
2. Enter the information specified in [Table 284 on page 519](#) to maintain the secure router.
3. Click **Upload and Install Package**. The software is activated after the device has rebooted.

Table 284: Upload Package Maintenance Options

Field	Function	Action
File to Upload	Specifies the location of the software package on the local system.	Enter the location of the software package, or click Choose File to navigate to the location.
Reboot If Required	Specifies that the device is automatically rebooted when the upgrade is complete.	Select the check box for 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.	Select the check box 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.	Select the check box to format the internal media with dual-root partitioning.

- See Also**
- [Maintaining Software Install Packages on page 519](#)
 - [Maintaining Software Downgrades on page 520](#)

Maintaining Software Install Packages

1. Select **Maintain>Software>Install Package** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platform.

Or

Select **Administration>Devices>Software>Install Package** in the J-Web user interface.

The Install Package maintain page appears.

2. Enter the information specified in [Table 285 on page 520](#) to maintain the secure router.
3. Click **Fetch and Install Package**. The software is activated after the device reboots.

Table 285: Install Package Maintenance Options

Field	Function	Action
Package Location	Specifies the FTP or HTTP server, file path, and software package name.	Enter the full address of the software package location on the FTP or HTTP server. For example, use one of the following format: <i>ftp://hostname/pathname/package-name</i> <i>http://hostname/pathname/package-name</i>
User	Specifies the username to use on a remote server.	Enter the username.
Password	Specifies the password to use on a remote server.	Enter the password.
Reboot If Required	Specifies that the device is automatically rebooted when the upgrade is complete.	Select the check box for 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.	Select the check box 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.	Select the check box to format the internal media with dual-root partitioning.

- See Also**
- [Maintaining Software Upload Packages on page 519](#)
 - [Maintaining Software Downgrades on page 520](#)

Maintaining Software Downgrades

1. Select **Maintain>Software>Downgrade** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platform.

Or

Select **Administration>Devices>Software>Downgrade** in the J-Web user interface.

The Downgrade maintain page appears. The image of the previous version (if any) is displayed on this page.

2. Click **Downgrade** to downgrade to the previous version of the software.



NOTE: This operation cannot be undone.

3. Reboot the device when the downgrade process is complete and for the new software to take effect. To reboot, perform the steps in “[Maintaining Reboot Schedule](#)” on [page 515](#).



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

- See Also**
- [Maintaining Software Upload Packages on page 519](#)
 - [Maintaining Software Install Packages on page 519](#)

Config Management

- [Maintaining Configuration Management Upload Files on page 521](#)
- [Maintaining Configuration Management History on page 522](#)
- [Maintaining the Rescue Configuration on page 524](#)

Maintaining Configuration Management Upload Files

1. Select **Maintain>Config Management>Upload** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platform.

Or

Select **Administration>Devices>Config Management>Upload** in the J-Web user interface.

The Upload Files page appears.

2. Enter the absolute path and filename in the **File to Upload** box.



NOTE: You can also click **Browse** to navigate to the file location and select it.

3. Click **Upload and Commit** to upload and commit the configuration.

The device checks the configuration for the correct syntax before committing it.

- See Also**
- [Maintaining Configuration Management History on page 522](#)
 - [Maintaining the Rescue Configuration on page 524](#)

Maintaining Configuration Management History

1. Select **Maintain>Config Management>History** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platform.

Or

Select **Administration>Devices>Config Management>History** in the J-Web user interface.

The History page appears. [Table 286 on page 522](#) explains the contents of this page.

2. Click one:

- **Number** — Displays a configuration .
- **Compare** — Compares two configurations files that you select.

The main pane displays the differences between the two configuration files at each hierarchy level as follows:

- Lines that have changed are highlighted side by side in green.
- Lines that exist only in the most recent configuration file are displayed in red on the left.
- Lines that exist only in the least recent configuration file are displayed in blue on the right.

- **Download** — Downloads a configuration file to your local system.

Select the options on your Web browser to save the configuration file to a target directory on your local system.

The file is saved as an ASCII file.

- **Rollback** — Rolls back the configuration to any of the previous versions stored on the device.

The main pane displays the results of the rollback operation.



NOTE: Click Rollback to load the device and download the selected configuration. This behavior is different from entering the rollback configuration mode command from the CLI, where the configuration is loaded, but not committed.

Enter the information specified in [Table 286 on page 522](#) to maintain the secure router.

Table 286: History Maintenance Options

Field	Function	Action
Number	Indicates the version of the configuration file.	–

Table 286: History Maintenance Options (continued)

Date/Time	Indicates the date and time the configuration was committed.	—
User	Indicates the name of the user who committed the configuration.	—
Client	<p>Indicates the method by which the configuration was committed.</p> <p>The available options are:</p> <ul style="list-style-type: none"> • cli—A user entered a Junos OS CLI command. • junoscript—A Junos XML management protocol client performed the operation. Commit operations performed by users through the J-Web interface are identified in this way. • snmp—An SNMP set request started the operation. • button—The CONFIG button on the router was pressed to commit the rescue configuration (if set) or to clear all configurations except the factory configuration. • autoinstall—Autoinstallation is performed. • other—Another method was used to commit the configuration. 	—
Comment	Indicates comments.	—
Log Message	<p>Indicates the method used to edit the configuration.</p> <ul style="list-style-type: none"> • Imported via paste—Configuration was edited and loaded with the Configure>CLI Tools>CLI Editor option. • Imported upload [filename]—Configuration was uploaded with the Configuration>View and Edit>Upload Configuration File option. • Modified via quick-configuration—Configuration was modified with the specified version of the J-Web user interface. • Rolled back via user-interface—Configuration was rolled back to a previous version through the user interface specified by <i>user-interface</i>, which can be Web Interface or CLI. 	—

Table 286: History Maintenance Options (continued)

Action	Indicates action to perform with the configuration file.	Select an option.
	The available options are:	
	<ul style="list-style-type: none"> • Download—Downloads a file. • Rollback—Rolls back a file. 	

- See Also**
- [Maintaining Configuration Management Upload Files on page 521](#)
 - [Maintaining Reboot Schedule on page 515](#)

Maintaining the Rescue Configuration

1. Select **Maintain>Config Management>Rescue** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platform.

Or

Select **Administration>Devices>Config Management>Rescue** in the J-Web user interface.

The Rescue page appears.
2. Click one:
 - **View rescue configuration** — Displays the current rescue configuration (if it exists).
 - **Set rescue configuration** — Sets the current running configuration as the rescue configuration. Click **OK** to confirm or **Cancel** to cancel.
 - **Delete rescue configuration** — Deletes the current rescue configuration. Click **OK** to confirm or **Cancel** to cancel.

- See Also**
- [Maintaining Configuration Management Upload Files on page 521](#)
 - [Maintaining Configuration Management History on page 522](#)

License Management

- [Maintaining Licenses on page 524](#)

Maintaining Licenses

1. Select **Maintain>Licenses** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platform.

Or

Select **Administration>License Management** in the J-Web user interface.

The Licenses maintain page appears. [Table 287 on page 525](#) explains the contents of this page.

2. Click one:

- **OK**—Saves the configuration and returns to the main configuration page.
- **Cancel**—Cancels your entries and returns to the main configuration page.

Enter the information specified in [Table 287 on page 525](#) to maintain the secure router.

Table 287: License Maintenance Options

Field	Function	Action
Feature	Displays the name of the licensed feature. Available options are: <ul style="list-style-type: none"> • Features—Software feature licenses. • All features—All-inclusive licenses. 	—
Licenses Used	Displays the 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.	—
Licensed Installed	Displays the number of licenses installed on the device for the particular feature.	—
Licenses Needed	Displays the 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.	—
License Expires on	Displays the expiry details on the license feature.	—
Licenses > Installed Licenses		

Table 287: License Maintenance Options (continued)

Add	Adds a new license key with the J-Web license manager.	<p>Perform one of the following, using a blank line to separate multiple license keys:</p> <ol style="list-style-type: none"> 1. Enter the full URL to the destination file containing the license key to be added in License File URL. <p>NOTE: Use this option 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.</p> <ol style="list-style-type: none"> 2. Paste the license key text, in plain-text format, for the license to be added in License Key. <p>NOTE: Use this option to activate a perpetual license directly on the device. (Most feature licenses are perpetual.)</p> <p>Click OK to add the license key.</p> <p>NOTE: If you added the SRX100 Memory Upgrade license, the device reboots immediately and comes back up as a high-memory device.</p>
Delete	Deletes one or more license keys with the J-Web license manager.	<ol style="list-style-type: none"> 1. Select the check box of the license or licenses you want to delete. 2. Click Delete. <p>NOTE: If you deleted the SRX100 Memory Upgrade license, the device reboots immediately and comes back up as a low-memory device.</p>
Update	Allows to send license update to the License Management Server (LMS).	Click Update to send license update to LMS.
Update Trial	Allows to send license update to the LMS and updates the trial licenses.	Click Update Trial to update trial licenses.
Display Keys	Displays the license keys installed on the device with the J-Web license manager.	Click Display Keys to display all of the license keys installed on the device.
Download Keys	Downloads the license keys installed on the device with the J-Web license manager.	<ol style="list-style-type: none"> 1. Click Download Keys to download all of the license keys installed on the device to a single file. 2. Select Save it to disk and specify the file to which the license keys are to be written.

Software Feature Licenses

Each feature license is tied to exactly one software feature, and that license is valid for exactly one device. [Table 288 on page 527](#) describes the Junos OS features that require licenses.

Table 288: Junos OS Services Feature Licenses

Junos OS License Requirements	Device								
Feature	J Series	SRX100	SRX210	SRX220	SRX240	SRX650	SRX1000 Line	SRX3000 Line	SRX5000 Line
Access Manager			X		X				
BGP Route Reflectors	X		X		X	X			
Dynamic VPN		X	X	X	X	X			
IDP Signature Update	X	X *	X *	X *	X *	X	X	X	X
Application Signature Update (Application Identification)							X	X	X
Juniper-Kaspersky Anti-Virus	X	X	X	X	X	X			
Juniper-Sophos Anti-Spam	X	X	X	X	X	X			
Juniper-Websense Integrated Web Filtering	X	X	X	X	X	X			
SRX100 Memory Upgrade		X							
UTM	X		X *		X *	X			

- See Also**
- [Maintaining Reboot Schedules](#)
 - [Maintaining Software Downgrades on page 520](#)
 - [Maintaining Software Install Packages on page 519](#)
 - [Maintaining Software Downgrades on page 520](#)
 - [Maintaining System Snapshots on page 517](#)

Certificate Management

- [Managing Certificates on page 528](#)
- [Managing Device Certificates on page 532](#)

- [Managing Trusted Certificate Authority on page 540](#)
- [Managing Certificate Authority Group on page 547](#)

Managing Certificates

1. Select **Administration>Certificate Management**.

The Certificate Management page appears. This page displays the number of certificates currently being used on the device. Usage is determined by the configuration on the device. [Table 289 on page 529](#) explains the contents of this page.

2. Click any of the following options:

- **Upload**—Uploads the selected CSR signed certificate or externally generated certificate to the device. The options are:
 - a. If you select **CSR Signed Certificate**, the Upload CSR Signed Certificate popup window appears.

Select the certificate content from the two options presented. If you select **File Path on device for Certificate**, add the path of the certificate file in **File path on device for Certificate** text box.

If you select **Paste Certificate Content**, paste the contents of the certificate in the text box.
 - b. If you select **Externally Generated Certificate**, the Upload Externally Generated Certificate popup window appears.

Enter the Certificate ID, File path on device for key pair where the key file is located, and Passphrase, if the key is encrypted using passphrase.

Select the certificate content from the two options. If you select **File Path on device for Certificate**, add the path of the certificate file (pim) in **File path on device for Certificate** text box.

If you select **Paste Certificate Content**, paste the contents of the certificate in the text box.
- Click **Upload**.
- **Download**—Downloads the selected CSR or signed certificate.
- Add icon **(+)**—Create a new certificate. A certificate can be Certificate Signing Request (CSR) or a self-signed certificate. After you create a CSR, you need to download it, get it signed by a CA, and use that certificate in the device. Self-signed certificates allow for use of SSL-based services without requiring you obtain an identity certificate signed by a CA. Self-signed certificates are usually used for internal purpose. All these steps can be managed in the Certificate Management page. There are two steps to generate a certificate:
 1. Generate Key Pair
 2. Generate Certificate

[Table 290 on page 530](#) lists the details involved while creating a certificate.

- Delete icon (X)—Delete the certificate that you have selected in the grid.
- **More**—The available options are:
 - Generate Trusted CAs—Generates default CAs provided by Juniper Networks, which is necessary while creating SSL Proxy profile. It may takes several minutes for generation. It is a one time activity.
 - View Trusted CAs—View all the default trusted CAs
 - Clear All Selections—Clears all selections made in the grid
- Search icon—Enables you to search for the certificate that you enter in the search criteria
- Show Hide column icon—Enables you to show or hide the columns to be displayed in the grid

Enter the information specified in [Table 289 on page 529](#) to maintain the secure router.

Table 289: Certificate Management Page

Field	Description
Certificate ID	Displays the certificate ID
Serial Number	Displays the serial number of the certificate.
Issuer	Displays the issuer of the certificate.
Subject	Displays the subject details such as Organizational Unit, Organization Name and so on.
Domain Name	Displays the domain name of the user.
Email	Displays the email ID of the user of the certificate.
IPv4 Address	Displays the IPv4 address of the user.
IPv6 Address	Displays the IPv6 address of the user.
Validity From	Displays the start date of the validity of the certificate.
Validity To	Displays the end date of the validity of the certificate.
Key Length	Displays the length of the key pair of the certificate.
Key Algorithm	Displays whether the key algorithm of the certificate is RSA or ECDSA encryption.
Signature Algorithm	Displays whether the signature algorithm is SHA-1, SHA-256, or SHA-384 digest.
Status	Displays whether the status of the certificate is signed or in CSR stage.

Table 290: Creating Certificate

Field	Function	Action
Generate Key Pair		
Certificate ID	Certificate ID is a unique value across the device. This will be used to create a key pair along with the algorithm to associate with the key.	Enter a unique value for the certificate ID.
Size	The bit length size of the RSA, DSA, or ECDSA key.	<p>Select the size from the list. The options available are: 1024 bits (RSA/DSA only), 2048 bits (RSA/DSA only), 256 bits (ECDSA only), 384 bits (ECDSA only), 4096 bits (RSA/DSA only), and 521 bits (ECDSA only).</p> <p>Starting in Junos OS Release 19.1R1, the bit length size supports 521 bits (ECDSA only).</p>
Type	The type of key encryption.	<p>Select the type of key from the dropdown list. The option are: RSA/DSA if size is selected as either 1024 bits, 2048 bits, or 4096 bits.</p> <p>ECDSA if size is selected as 256 bits, 384 bits or 521 bits. Starting in Junos OS Release 19.1R1, the bit length size supports 521 bits.</p> <p>NOTE: The certificate cannot be used in SSL Proxy profile if it is generated using type DSA.</p>
	Generate the key pair.	Click Generate.
Generate Certificate		
Certificate Signing Details		
Type	<p>A certificate can be Certificate Signing Request (CSR) or a self-signed local certificate. After the CA is generated it must be signed by a CA server and then you upload the signed CSR back to the device using the same certificate ID.</p> <p>Self-signed certificates allow for use of SSL-based services without requiring you obtain an identity certificate signed by a CA. Self-signed certificates are usually used for internal purpose.</p>	Select the type of certificate from the options—Certificate Signing Request (CSR) or Self-signed local-certificate.
Certificate ID	Displays the certificate ID that is created in the previous screen.	—

Table 290: Creating Certificate (continued)

Digest	Displays the digests available.	<p>Select the digest from the dropdown list.</p> <p>If Key pair is generated with RSA/DSA:</p> <ul style="list-style-type: none"> For CSR the options are: The options are: SHA-1 digests (RSA/DSA only) or SHA-256 digests (RSA/ECDSA only). For self-signed local certificate, the options are: SHA-1 digests or SHA-256 digests. <p>If key pair is generated with ECDSA:</p> <ul style="list-style-type: none"> For CSR, the options are: SHA-256 digests (RSA/ECDSA only) or SHA-384 digests (ECDSA only). For self-signed local certificate, the options are: SHA-1 digests or SHA-256 digests.
Domain Name	Allows you to enter a domain name that you want to associate with this certificate.	Enter a Domain Name.
Email	Allows you to enter the email address.	Enter an email address.
IP Address	Allows you to enter the IPv4 address of the system from where you are creating this certificate.	Enter IPv4 address.
Add CA Constraint	This option is available only for Self-Signed Local-Certificate.	Select the checkbox to add CA constraint to this certificate.
IPv6 Address	Allows you to enter the IPv6 address of the system from where you are creating this certificate.	Enter IPv6 address.
<p>NOTE: This appears only if you selected the Type of certificate as Certificate Signing Request (CSR).</p>		
Collapse the Subject (Any one field is mandatory)		
Domain Component	Allows you to enter the domain component that you want to be associated with this certificate. This will be displayed under the Subject in the Certificate Management page.	Enter the domain component.
Common Name	Allows you to enter a common name with this certificate.	Enter a common name.
Organizational Unit	Allows you to enter your organizational unit that you want to be associated with this certificate.	Enter the organizational unit.

Table 290: Creating Certificate (continued)

Organizational Name	Allows you to enter your organizational name that you want to be associated with this certificate. This will be displayed under the Subject in the Certificate Management page.	Enter the organizational name.
Serial Number	Allows you to enter serial number for the certificate.	Enter a serial number.
Locality	Allows you to enter the locality from where you are creating this certificate.	Enter the locality name.
State	Allows you to enter the state or region from where you are creating this certificate.	Enter the state name.
Country	Allows you to enter the country from where you are creating this certificate.	Enter the country name.

- See Also**
- [Maintaining Software Downgrades on page 520](#)
 - [Maintaining Software Install Packages on page 519](#)
 - [Maintaining Software Downgrades on page 520](#)
 - [Maintaining System Snapshots on page 517](#)

Managing Device Certificates

Starting in Junos OS 19.2R1 Release, Device Certificates page is available and you can navigate to this page from **Administration > Certificate Management > Device Certificates**.

Manage the device certificates to authenticate Secure Socket Layer (SSL). 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.

[Table 291 on page 532](#) provides the details of the fields of the Device Certificates page.

Table 291: Fields on Device Certificates Page

Field	Description
Certificate ID	Displays the certificate ID. Certificate ID is a unique value across the device. This will be used to create a key pair along with the algorithm to associate with the key.
Issuer Org	Displays the details of the authority that issued the certificate.
Status	Displays whether the status of the certificate is valid, expired, and so on.

Table 291: Fields on Device Certificates Page (continued)

Field	Description
Expiration Date	Displays certificate expiration date.
Encryption Type	Displays whether the algorithm of the certificate is RSA, DSA, or ECDSA encryption.
Signature Status	Displays whether the status of the certificate is signed or in certificate signing request (CSR) stage.

You can perform the following tasks:

- Import a certificate to manually load externally generated certificates. See [“Importing a Certificate” on page 533](#).



NOTE: You must obtain the private key, passphrase, and the signed certificate from certificate authority (CA) server.

- Export a local certificate or CSR from the default location to a specific location within the device. See [“Exporting a Certificate” on page 534](#).
- View the details of a certificate. See [“Viewing the Details of a Certificate” on page 535](#).
- Generate a certificate. See [“Generating a Certificate” on page 537](#).
- Delete a certificate. See [“Deleting a Certificate” on page 539](#).
- Search for text in a device certificate table. See [“Search Text in Device Certificates Table” on page 539](#).
- Filter the device certificates information based on select criteria. To do this, select the filter icon at the top right-hand corner of the table. The columns in the grid change to accept filter options. Type the filter options; the table displays only the data that fits the filtering criteria.
- Show or hide columns in the Device Certificates table. To do this, use the Show Hide Columns icon in the top right corner of the page and select the options you want to show or deselect to hide options on the page

Importing a Certificate

To import a device certificate:

1. Select **Administration > Certificate Management > Device Certificates**.
2. Click **Import**.

The Import Certificate page appears.

3. Complete the configuration according to the guidelines provided in [Table 292 on page 534](#).

4. Click **OK** to import the certificate.

You are taken to the Device Certificates page. If the certificate content that you imported is validated successfully, a confirmation message is displayed; if not, an error message is displayed.

After importing a certificate, you can use it when you create an SSL proxy profile and for IPSec VPN peers authentication.

Table 292: Fields on the Import Certificate Page

Field	Action
Type	Select an option to specify whether the certificate that you are importing is an Externally Generated Certificate or a CSR.
Certificate ID	Enter a unique value for the certificate ID for an externally generated certificate. Select an option from the list to specify the certificate ID for a CSR.
File path for Certificate	Click Browse to navigate to the path from where you want to import the certificate.
File path for Private Key	Click Browse to navigate to the path from where you want to import the private key.
Passphrase	Enter the passphrase used to protect the private key or key pair of the certificate file.

Exporting a Certificate

To export a device certificate:

1. Select **Administration > Certificate Management > Device Certificates**.

2. Click **Export**.

The Export Certificate page appears.

3. Complete the configuration according to the guidelines provided in [Table 293 on page 535](#).

4. Click **OK** to export the certificate.

Once you save or download the exported file(s), a confirmation message is displayed; if not, an error message is displayed.

Table 293: Fields on the Export Certificate Page

Field	Action
Type	Select an option from the list to specify whether the certificate that you are exporting is a Local Certificate or a CSR.
Certification Name	Select an option from the list for the local certificate name.
Certificate ID	This option is available only for CSR. Select an option from the list for the CSR certificate ID.
Format	Select an option from the list to specify whether the exporting certificate format is Privacy-Enhanced Mail (PEM) or Distinguished Encoding Rules (DER).
Key Pair	Enable or disable exporting key pair of a certificate.
Passphrase	Enter the passphrase to protect the private key or key pair of the certificate file.

Viewing the Details of a Certificate

To view the details of a device certificate:

1. Select **Administration > Certificate Management > Device Certificates**.
2. Select an existing certificate.
3. Select **More > Detailed View**.

The View Certificate page appears with the details of the certificate.



NOTE: When you hover over the certificate ID, a Detailed View icon appears before the certificate ID. You can also use this icon to view the certificate details.

4. Click **OK** after viewing the certificate details.

[Table 294 on page 535](#) provides the field details of the certificate on the View Certificate page.

Table 294: Fields on the View Certificate Page

Field	Action
Certificate Details	
Certificate ID	Displays the certificate ID.
Certificate Version	Displays the certificate revision number.

Table 294: Fields on the View Certificate Page (continued)

Field	Action
Certificate Type	Displays the certificate type. For example, Signed.
Encryption Type	Displays the encryption type. For example, RSA.
Key Size	Displays the key size of the encryption type.
Serial Number	Displays the unique serial number of the certificate.
Subject	
Domain Component	Displays the domain component associated with the certificate.
Common Name	Displays the common name associated with the certificate.
Organizational Unit Name	Displays the organizational unit associated with the certificate.
Organizational Name	Displays the organizational name associated with this certificate.
Serial Number	Displays the serial number of the device.
Locality	Displays the locality name.
State	Displays the state name.
Country	Displays the country name.
Subject Alt Name	
Domain Name	Displays the Fully Qualified Domain Name (FQDN).
Email	Displays the email ID of the certificate holder.
IPv4 Address	Displays the IPv4 address.
IPv6 Address	Displays the IPv6 address.
Issuer Information	
Common Name	Displays the issuer common name associated with the certificate.
Domain Component	Displays the issuer domain component associated with the certificate.
Organization Name	Displays the issuer organizational name.
Organization Unit Name	Displays the issuer organizational unit.
Locality Name	Displays the issuer locality name.
State or Province Name	Displays the issuer state or region name.

Table 294: Fields on the View Certificate Page (continued)

Field	Action
Validity	
Not Before	Displays the start time when the certificate becomes valid.
Not After	Displays the end time when the certificate becomes invalid.
Auto Re Enrollment	
Status	Displays whether the auto re enrollment is enabled or disabled.
Next Trigger Time	Displays the how long auto-reenrollment should be initiated before expiration.
Fingerprint	
MD5	Displays the MD5 fingerprints to identify the certificate.
SHA1	Displays the SHA-1 fingerprints to identify the certificate.
Signature Algorithm	
Algorithm	Displays whether the signature algorithm is SHA-1, SHA-256, or SHA-384 digest.
Distribution CRL	
URL	Displays the URL of the certificate revocation list (CRL) server.
LDAP	Displays the name of the location from which the CRL is retrieved through Lightweight Directory Access Protocol (LDAP).
Authority Information Access OCSP	
URL	Displays the URL of the Online Certificate Status Protocol (OCSP) server.

Generating a Certificate

To generate a device certificate:

1. Select **Administration > Certificate Management > Device Certificates**.
2. Click the add icon (+).
The Generate Certificate page appears.
3. Complete the configuration according to the guidelines provided in [Table 295 on page 538](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.
If you click **OK**, a new certificate with the provided configuration is created.

Table 295: Fields on the Generate Certificate Page

Field	Action
Certificate Details	
Certificate Type	<p>Select one of the certificate type from the list that you want to generate:</p> <ul style="list-style-type: none"> Local Self-Signed—Allows for use of SSL-based (Secure Sockets Layer) services without requiring that the user or administrator to undertake the considerable task of obtaining an identity certificate signed by a CA. Self-signed certificates are usually used for internal purpose. Local Certificate—Validates the identity of the security device. A local certificate imports or references an SSL certificate.
CA Profile Name	<p>This option is available for a local certificate.</p> <p>Select one of the CA profile name from the list or click Create to add a CA Profile. For details on adding a CA profile, see the table in the <i>Adding a Certificate Authority Profile</i> section.</p>
Certificate ID	Enter a unique value for the certificate ID.
Encryption Type	<p>Select one of the type of encryption from the list:</p> <ul style="list-style-type: none"> RSA Encryption DSA Encryption <p>NOTE: The certificate cannot be used in SSL Proxy profile if it is generated using type DSA.</p> <ul style="list-style-type: none"> ECDSA Encryption
Key Size	<p>Select one of the key size from the list:</p> <ul style="list-style-type: none"> RSA encryption supports 1024 bits, 2048 bits, or 4096 bits. DSA encryption supports 1024 bits, 2048 bits, or 4096 bits. ECDSA encryption supports 256 bits, 384 bits, or 521 bits.
Subject (Minimum of one field required)	
Domain Component	Enter the domain component that you want to be associated with the certificate.
Common Name	Enter a common name with the certificate.
Organizational Unit Name	Enter the organizational unit that you want to be associated with the certificate.
Organizational Name	Enter the organizational name that you want to be associated with this certificate.
Serial Number	Enter a serial number of the device.
Locality	Enter the locality name.
State	Enter the state name.
Country	Enter the country name.

Table 295: Fields on the Generate Certificate Page (continued)

Field	Action
Subject Alt Name	
NOTE: For a local certificate, any one field is mandatory	
Domain Name	Enter a Domain Name that you want to associate with the certificate.
Email	Enter an user email address.
IPv4 Address	Enter the IPv4 address of the device.
IPv6 Address	This option is available for a local certificate. Enter the IPv6 address of the device.
Advanced	
Digest	Select the digest from the list: <ul style="list-style-type: none"> For local Self-signed certificate (RSA/DSA/ECDSA) options are: None, SHA-1 digests, or SHA-256 digests. For local certificate options are: <ul style="list-style-type: none"> RSA/DSA: None, SHA-1 digests, or SHA-256 digests ECDSA: None, SHA-256 digests, or SHA-384 digests.
Signing Certificate	Enable or disable specifies that the certificate is used to sign other certificates.

Deleting a Certificate

To delete a device certificate:

1. Select **Administration > Certificate Management > Device Certificates**.
2. Select the certificate you want to delete.
3. On the upper right side of the Device Certificates page, click the delete icon to delete.
A confirmation window appears.
4. Click **Yes** to delete.

Search Text in Device Certificates Table

You can use the search icon in the top right corner of a page to search for text containing letters and special characters on that page.

To search for text:

1. Enter partial text or full text of the keyword in the search bar and click the search icon.

The search results are displayed.

2. Click **X** next to a search keyword or click **Clear All** to clear the search results.

- See Also**
- [Managing Trusted Certificate Authority on page 540](#)
 - [Managing Certificate Authority Group on page 547](#)

Managing Trusted Certificate Authority

Starting in Junos OS 19.2R1 Release, Trusted Certificate Authority page is available and you can navigate to this page from **Administration > Certificate Management > Trusted Certificate Authority**.

SSL forward proxy ensures secure transmission of data between a client and a server. Before establishing a secure connection, SSL forward proxy checks certificate authority (CA) certificates to verify signatures on server certificates. For this reason, a reasonable list of trusted CA certificates is required to effectively authenticate servers.

[Table 296 on page 540](#) provides the details of the fields of the Trusted Certificate Authority Page

Table 296: Fields on Trusted Certificate Authority Page

Field	Description
CA Profile	Displays the name of the CA profile.
Certificate ID	Displays the CA certificate ID.
Issuer Org	Displays the issuer organizational name.
Status	Displays the status of the CA certificate. For example: <ul style="list-style-type: none">• Valid.• Expires in number of day(s).• Expired.• Download Required. This status is for a CA profile with manual enrollment.• Enrollment Required. This status is for a CA profile with automatic enrollment.
Expiration Date	Displays CA certificate expiration date.
Encryption Type	Displays whether the algorithm of the certificate is RSA, DSA, or ECDSA encryption.

You can perform the following tasks:

- Generate default trusted CAs—For SSL forward proxy, you need to load trusted CA certificates on your system. By default, Junos OS provides a list of trusted CA certificates that include default certificates used by common browsers. To generate default Trusted CA profiles with default name as Local, click **Generate Default Trusted CAs** and then click **Continue**. This process may take several minutes.
- Enroll a CA certificate using the Simple Certificate Enrollment Process (SCEP) or Certificate Management Protocol (CMPv2). With SCEP or CMPv2, you can configure Juniper Network device to obtain a local certificate online and start the online enrollment for the specified certificate ID. See [“Enrolling a Certificate Authority Certificate” on page 541](#).
- Import a CA certificate to manually load CA certificates and CRL. See [“Importing a Certificate Authority Certificate” on page 542](#).
- Add a CA profile. See [“Adding a Certificate Authority Profile” on page 543](#).
- Edit a CA profile. See [“Editing a Certificate Authority Profile” on page 545](#).
- Delete a CA profile. See [“Deleting a Certificate Authority Profile” on page 546](#).
- Search for text in a Trusted Certificate Authority table. See [“Search Text in Trusted Certificate Authority Table” on page 546](#).
- Filter the trusted CA information based on select criteria. To do this, select the filter icon at the top right-hand corner of the table. The columns in the grid change to accept filter options. Type the filter options; the table displays only the data that fits the filtering criteria.
- Show or hide columns in the trusted CA table. To do this, use the Show Hide Columns icon in the top right corner of the page and select the options you want to show or deselect to hide options on the page.

Enrolling a Certificate Authority Certificate

To import a trusted CA group:

1. Select **Administration > Certificate Management > Trusted Certificate Authority**.
2. Click **Enroll**.
The Enroll CA Certificate page appears.
3. Complete the configuration according to the guidelines provided in [Table 297 on page 541](#).
4. Click **OK** to enroll the CA certificate.

Table 297: Fields on the Enroll CA Certificate Page

Field	Action
CA Profile Name	Select a CA profile name from the list that you want to enroll.

Table 297: Fields on the Enroll CA Certificate Page (continued)

Field	Action
Protocol	Select a protocol from the list for the CA certificate that you want to enroll. <ul style="list-style-type: none"> • SCEP—Simple Certificate Enrollment Protocol (SCEP) • CMPV2—Certificate Management Protocol version 2 (CMPv2)
NOTE: The following fields are available only if you select CMPv2 protocol. All the fields are mandatory.	
CA Secret	Enter the out-of-band secret value received from the CA server.
CA Reference	Enter the out-of-band reference value received from the CA server.
CA Dn	Enter the distinguished name (DN) of the CA enrolling the EE certificate. NOTE: This optional parameter is mandatory if the CA certificate is not already enrolled. If the CA certificate is already enrolled, the subject DN is extracted from the CA certificate.
Certificate Details	Click Add to generate a new certificate inline.

Importing a Certificate Authority Certificate

To import a CA certificate:

1. Select **Administration > Certificate Management > Trusted Certificate Authority**.
2. Click **Import**.

The Import CA Certificate page appears.

3. Complete the configuration according to the guidelines provided in [Table 298 on page 542](#).
4. Click **OK** to import the CA certificate.

You are taken to the Trusted Certificate Authority page. If the CA certificate content that you imported is validated successfully, a confirmation message is displayed; if not, an error message is displayed.

Table 298: Fields on the Import CA Certificate Page

Field	Action
CA Profile Name	Select a CA profile name from the list that you want to import.
File path for CA Certificate	Click Browse to navigate to the path from where you want to import the CA certificate.
File path for CRL	Click Browse to navigate to the path from where you want to import the Certificate Revocation List (CRL).

Adding a Certificate Authority Profile

To add a CA group:

1. Select **Administration > Certificate Management > Trusted Certificate Authority**.

2. Click the add icon (+).

The Add CA Profile page appears.

3. Complete the configuration according to the guidelines provided in [Table 299 on page 543](#).

4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

If you click **OK**, a new CA profile with the provided configuration is created.

Table 299: Fields on the Add CA Profile Page

Field	Action
Profile Details	
CA Profile Name	Enter a unique CA profile name.
CA Identity	Enter a CA identity name.
Revocation Check	Select an option from the list: <ul style="list-style-type: none"> • Disable—Disables verification of status of digital certificates. • OCSP—Online Certificate Status Protocol (OCSP) checks the revocation status of a certificate. • CRL—A CRL is a time-stamped list identifying revoked certificates, which is signed by a CA and made available to the participating IPsec peers on a regular periodic basis.
URL	For OCSP, enter HTTP addresses for OCSP responders. For CRL, enter the name of the location from which to retrieve the CRL through HTTP or Lightweight Directory Access Protocol (LDAP).
On Connection Failure	Enable this option to skip the revocation check if the OCSP responder is not reachable. NOTE: This option is applicable only for OCSP.
Disable Responder Revocation Check	Enable this option to disable revocation check for the CA certificate received in an OCSP response. NOTE: This option is applicable only for OCSP.
Accept Unknown Status	When set to enable, accepts the certificate with unknown status. NOTE: This option is applicable only for OCSP.

Table 299: Fields on the Add CA Profile Page (continued)

Field	Action
Nonce Payload	<p>Disable the option—Explicitly disable the sending of a nonce payload.</p> <p>Enable the option—Enable the sending of a nonce payload. This is the default.</p> <p>NOTE: This option is applicable only for OCSP.</p>
CRL Refresh Interval	<p>Enter the time interval (in hours) between CRL updates.</p> <p>Range: 0 through 8784 hours.</p> <p>NOTE: This option is applicable only for CRL.</p>
Password	Enter the password for authentication with the server.
Disable on Download Failure	<p>Enable this option to override the default behavior and permit certificate verification even if the CRL fails to download.</p> <p>NOTE: This option is applicable only for CRL.</p>
Enrollment	
CA Certificate	Select an option whether you want to enroll the CA certificate manually or automatically.
File path for Certificate	Click Browse to navigate to the path from where you want to enroll the CA certificate.
URL	Enter the URL from where you want to enroll the CA certificate automatically.
Retry	Number of enrollment retry attempts before aborting. Range: 0 - 1080.
Retry-interval	Interval in seconds between the enrollment retries. Range: 0 - 3600.
Advanced	
Administrator	Enter an administrator e-mail address to which the certificate request is sent.
Source Address	Enter a source IPv4 or IPv6 address to be used instead of the IP address of the egress interface for communications with external servers.
Auto Re Enrollment	Enable this option to request that the issuing CA replace a certificate before its specified expiration date.
Re Generate Key Pair	Enable this option to automatically generate a new key pair when auto-reenrolling a device certificate.
Protocol	Select an option from the list: Simple Certificate Enrollment Protocol (SCEP) or Certificate Management Protocol version 2 (CMPv2).
Challenge Password	Enter the challenge password used by the certificate authority (CA) for certificate enrollment and revocation. This challenge password must be the same used when the certificate was originally configured.

Table 299: Fields on the Add CA Profile Page (continued)

Field	Action
Trigger Time	Enter the percentage for the reenroll trigger time before expiration. Range: 1 through 99 percent
Digest	Select an option from the list: None, SHA-1 digest (default), or MD5-digest. NOTE: This option is applicable only when you select SCEP protocol.
Encryption	Select an option from the list: None, DES, DES 3. NOTE: This option is applicable only when you select SCEP protocol.
Routing Instance	Select an option from the list of configured routing instances.
Proxy Profile	Select an option from the list. Or To create a new proxy profile inline: 1. Click Create . Create Proxy Profile page appears. 2. Enter the following details: <ul style="list-style-type: none"> • Profile Name—Enter a unique proxy profile name. • Connection Type: <ul style="list-style-type: none"> • Server IP—Enter the IP address of the server. • Host Name—Enter the host name. • Port Number—Select the port number by using top/down arrows. Range: 0 through 65535 3. Click OK .

Editing a Certificate Authority Profile

To edit a CA profile:

1. Select **Administration > Certificate Management > Trusted Certificate Authority**.
2. Select a CA profile.
3. On the upper right side of the Trusted Certificate Authority page, click the pencil icon.
See [Table 299 on page 543](#) for the options available for editing on the Edit CA Profile page.



NOTE: When you select a CA profile to edit, you cannot edit the following fields:

- CA Profile Name
- Revocation Check
- Enrollment > CA Certificate
- Advanced > Auto Re Enrollment
- Advanced > Protocol

4. Click **OK**

Deleting a Certificate Authority Profile

To delete a CA profile:

1. Select **Administration > Certificate Management > Trusted Certificate Authority**.
2. Select a CA profile.
3. On the upper right side of the Trusted Certificate Authority page, click the delete icon to delete.
A confirmation window appears.
4. Click **Yes** to delete.

Search Text in Trusted Certificate Authority Table

You can use the search icon in the top right corner of a page to search for text containing letters and special characters on that page.

To search for text:

1. Enter partial text or full text of the keyword in the search bar and click the search icon.
The search results are displayed.
2. Click **X** next to a search keyword or click **Clear All** to clear the search results.

- See Also**
- [Managing Device Certificates on page 532](#)
 - [Managing Certificate Authority Group on page 547](#)

Managing Certificate Authority Group

Starting in Junos OS 19.2R1 Release, Certificate Authority Group page is available and you can navigate to this page from **Administration > Certificate Management > Certificate Authority Group**.

For SSL forward proxy, you need to load trusted CA certificates on your system. By default, Junos OS provides a list of trusted CA certificates that include default certificates used by common browsers. Alternatively, you can define your own list of trusted CA certificates and import them on to your system.

[Table 300 on page 547](#) provides the details of the fields of the Certificate Authority Group Page

Table 300: Fields on Certificate Authority Group Page

Field	Description
Group Name	Displays a Name for the CA profile group.
CA Profiles	Displays the name of CA profiles.
Used For	Displays whether the CA profile group is used for IPsec VPN or for SSL proxy.

You can perform the following tasks:

- Import a CA group to manually load the CA group. See [“Importing a Trusted Certificate Authority Group” on page 548](#).
- Add a CA group. See [“Adding a Certificate Authority Group” on page 548](#).



NOTE: You can group up to maximum of 20 CA profiles in a single trusted CA group. A minimum of one CA profile is a must to create a trusted CA group.

- Edit a CA group. See [“Editing a Certificate Authority Group” on page 549](#).
- Delete a CA group. See [“Deleting a Certificate Authority Group” on page 549](#).
- Search for text in a CA group table. See [“Search Text in Certificate Authority Group Table” on page 549](#).
- Filter the CA group information based on select criteria. To do this, select the filter icon at the top right-hand corner of the table. The columns in the grid change to accept filter options. Type the filter options; the table displays only the data that fits the filtering criteria.
- Show or hide columns in the CA group table. To do this, use the Show Hide Columns icon in the top right corner of the page and select the options you want to show or deselect to hide options on the page.

Importing a Trusted Certificate Authority Group

To import a trusted CA group:

1. Select **Administration > Certificate Management > Certificate Authority Group**.

2. Click **Import**.

The Import Trusted CA Group page appears.

3. Complete the configuration according to the guidelines provided in [Table 301 on page 548](#).

4. Click **OK** to import the CA group.

You are taken to the Certificate Authority Group page. If the CA group content that you imported is validated successfully, a confirmation message is displayed; if not, an error message is displayed.

After importing a CA profile group, you can use it when you create a SSL proxy.

Table 301: Fields on the Import Trusted CA Group Page

Field	Action
CA Group Name	Enter the name of a CA group.
File path for CA Group	Click Browse to navigate to the path from where you want to import the CA group. NOTE: Only .pem format is supported.

Adding a Certificate Authority Group

To add a CA group:

1. Select **Administration > Certificate Management > Certificate Authority Group**.

2. Click the add icon (+).

The Add CA Group page appears.

3. Complete the configuration according to the guidelines provided in [Table 302 on page 549](#).

4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

If you click **OK**, a new CA group with the provided configuration is created.

After added a CA group, you can use it for IPSec VPN.

Table 302: Fields on the Add CA Group Page

Field	Action
CA Group Name	Enter an unique CA group name.
CA Profiles	<p>Select a CA profile name from the list in the Available column and then click the right arrow to move it to the Selected column.</p> <p>NOTE: You can add up to maximum of 20 CA profiles per trusted CA group.</p>

Editing a Certificate Authority Group

To edit a CA group:

1. Select **Administration > Certificate Management > Certificate Authority Group**.
2. Select a CA group.
3. On the upper right side of the Certificate Authority Group page, click the pencil icon.
See [Table 302 on page 549](#) for the options available for editing on the Edit CA Group page.
4. Click **OK**

Deleting a Certificate Authority Group

To delete a CA group:

1. Select **Administration > Certificate Management > Certificate Authority Group**.
2. Select a CA group.
3. On the upper right side of the Certificate Authority Group page, click the delete icon to delete.
A confirmation window appears.
4. Click **Yes** to delete.

Search Text in Certificate Authority Group Table

You can use the search icon in the top right corner of a page to search for text containing letters and special characters on that page.

To search for text:

1. Enter partial text or full text of the keyword in the search bar and click the search icon.
The search results are displayed.

2. Click **X** next to a search keyword or click **Clear All** to clear the search results.

- See Also**
- [Managing Device Certificates on page 532](#)
 - [Managing Trusted Certificate Authority on page 540](#)

Ping Host

- [Troubleshooting Ping Host on page 550](#)

Troubleshooting Ping Host

Problem **Description:** You can ping a host to verify that the host can be reached over the network. The output is useful for diagnosing host and network connectivity problems. The J Series device sends a series of ICMP echo (ping) requests to a specified host and receives ICMP echo responses.

Solution To use the ping host tool:

1. Select **Troubleshoot>Ping Host** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platform.

Or

Select **Administration>Ping Host** in the J-Web user interface.

2. Click the expand icon next to Advanced options.
3. Enter the information specified in [Table 303 on page 550](#) to troubleshoot the issue. The Remote Host field is the only required field.
4. Click **Start**.

The results of the ping operation are displayed in the main pane. If no options are specified, each ping response is in the following format:

```
bytes bytes from ip-address: icmp_seq=number ttl=number time=time
```

5. Click **OK** to stop the ping operation before it is complete.

Table 303: Ping Host Troubleshooting Options

Field	Function	Action
Remote Host	Identifies the host to ping.	Type the hostname or IP address of the host to ping.

Advanced Options

Table 303: Ping Host Troubleshooting Options (continued)

Field	Function	Action
Don't Resolve Addresses	Determines whether or not to display hostnames of the hops along the path.	<ul style="list-style-type: none"> To suppress the display of the hop hostnames, select the check box. To display the hop hostnames, clear the check box.
Interface	Specifies the interface on which the ping requests are sent.	From the list, select the interface on which ping requests are sent. If you select any , the ping requests are sent on all interfaces.
Count	Specifies the number of ping requests to send.	From the list, select the number of ping requests to send.
Don't Fragment	Specifies the don't fragment (DF) bit in the IP header of the ping request packet.	<ul style="list-style-type: none"> To set the DF bit, select the check box. To clear the DF bit, clear the check box.
Record Route	Sets the record route option in the IP header of the ping request packet. The path of the ping request packet is recorded within the packet and displayed in the main pane.	<ul style="list-style-type: none"> To record and display the path of the packet, select the check box. To suppress the recording and display of the path of the packet, clear the check box.
Type-of-Service	Specifies the type-of-service (ToS) value in the IP header of the ping request packet.	From the list, select the decimal value of the ToS field.
Routing Instance	Specifies the name of the routing instance for the ping attempt.	From the list, select the routing instance name.
Interval	Specifies the interval, in seconds, between the transmission of each ping request.	From the list, select the interval.
Packet Size	Specifies the size of the ping request packet.	Type the size, in bytes, of the packet. The size can be from 0 through 65468. The device adds 8 bytes to the size of the ICMP header.
Source Address	Specifies the source address of the ping request packet.	Type the source IP address.
Time-to-Live	Specifies the time-to-live (TTL) hop count for the ping request packet.	From the list, select the TTL.

Table 303: Ping Host Troubleshooting Options (continued)

Field	Function	Action
Bypass Routing	<p>Determines whether or not ping requests are routed by means of the routing table.</p> <p>If the routing table is not used, ping requests are sent only to hosts on the interface specified in the Interface box. If the host is not on that interface, ping responses are not sent.</p>	<ul style="list-style-type: none"> To bypass the routing table and send the ping requests to hosts on the specified interface only, select the check box. To route the ping requests using the routing table, clear the check box.
Ping Host Results and Output Summary		
<i>bytes</i> bytes from <i>ip-address</i>	<ul style="list-style-type: none"> bytes—Size of ping response packet, which is equal to the value you entered in the Packet Size box, plus 8. ip-address—IP address of destination host that sent the ping response packet. 	—
icmp_seq=0 icmp_seq= <i>number</i>	number —Sequence Number field of the ping response packet. You can use this value to match the ping response to the corresponding ping request.	—
ttl= <i>number</i>	number —TTL hop-count value of the ping response packet.	—
time= <i>time</i>	time —Total time between the sending of the ping request packet and the receiving of the ping response packet, in milliseconds. This value is also called round-trip time.	—
<i>number</i> packets transmitted	number —Number of ping requests (probes) sent to host.	—
<i>number</i> packets received	number —Number of ping responses received from host.	—
<i>percentage</i> packet loss	percentage —Number of ping responses divided by the number of ping requests, specified as a percentage.	—
round-trip min/avg/max/stddev = <i>min-time</i> / <i>avg-time</i> / <i>max-time</i> / <i>std-dev</i> ms	<ul style="list-style-type: none"> min-time—Minimum round-trip time (see time=time field in this table). avg-time—Average round-trip time. max-time—Maximum round-trip time. std-dev—Standard deviation of the round-trip times. 	—

Table 303: Ping Host Troubleshooting Options (continued)

Field	Function	Action
Output = Packet loss of 100 percent	<p>If the device does not receive ping responses from the destination host (the output shows a packet loss of 100 percent), one of the following explanations might apply:</p> <ul style="list-style-type: none"> • The host is not operational. • There are network connectivity problems between the device and the host. • The host might be configured to ignore ICMP echo requests. • The host might be configured with a firewall filter that blocks ICMP echo requests or ICMP echo responses. • The size of the ICMP echo request packet exceeds the MTU of a host along the path. • The value you selected in the TTL box was less than the number of hops in the path to the host, in which case the host might reply with an ICMP error message. <p>For more information about ICMP, see RFC 792, <i>Internet Control Message Protocol</i>.</p>	—

See Also • [Troubleshooting Ping MPLS on page 553](#)

Ping MPLS

- [Troubleshooting Ping MPLS on page 553](#)

Troubleshooting Ping MPLS

Problem Description: Before using the ping MPLS tool, make sure that the receiving interface on the VPN or LSP remote endpoint has MPLS enabled, and that the loopback interface on the egress node is configured as **127.0.0.1**. The source address for MPLS probes must be a valid address on the J Series device.

Solution To use the ping MPLS tool:

1. Select **Troubleshoot>Ping MPLS** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platform.

Or

Select **Administration>Ping MPLS** in the J-Web user interface.

2. Click the expand icon next to the ping MPLS option you want to use.

3. Enter information specified in [Table 304 on page 554](#) to troubleshoot the issue.
4. Click **Start**.
5. Click **OK** to stop the ping operation before it is complete.

Table 304: Ping MPLS Troubleshooting Options

Field	Function	Action
Ping RSVP-signaled LSP		
LSP Name	Identifies the LSP to ping.	Type the name of the LSP to ping.
Source Address	Specifies the source address of the ping request packet.	Type the source IP address—a valid address configured on a J Series device interface.
Count	Specifies the number of ping requests to send.	From the list, select the number of ping requests to send. The default is 5 requests.
Detailed Output	Requests the display of extensive rather than brief ping output.	Select the check box to display detailed output.
Ping LDP-signaled LSP		
FEC Prefix	Identifies the LSP to ping.	Type the forwarding equivalence class (FEC) prefix and length of the LSP to ping.
Source Address	Specifies the source address of the ping request packet.	Type the source IP address—a valid address configured on a J Series device interface.
Count	Specifies the number of ping requests to send.	From the list, select the number of ping requests to send. The default is 5 requests.
Detailed Output	Requests the display of extensive rather than brief ping output.	Select the check box to display detailed output.
Ping LSP to Layer 3 VPN prefix		
Layer 3 VPN Name	Identifies the Layer 3 VPN to ping.	Type the name of the VPN to ping.
Count	Specifies the number of ping requests to send.	From the list, select the number of ping requests to send. The default is 5 requests.
Detailed Output	Requests the display of extensive rather than brief ping output.	Select the check box to display detailed output.
VPN Prefix	Identifies the IP address prefix and length of the Layer 3 VPN to ping.	Type the IP address prefix and length of the VPN to ping.
Source Address	Specifies the source address of the ping request packet.	Type the source IP address—a valid address configured on a J Series device interface.

Table 304: Ping MPLS Troubleshooting Options (continued)

Field	Function	Action
Locate LSP using interface name		
Interface	Specifies the interface on which the ping requests are sent. (See the interface naming conventions in the Junos OS Interfaces Configuration Guide for Security Devices .)	From the list, select the J Series device interface on which ping requests are sent. If you select any , the ping requests are sent on all interfaces.
Source Address	Specifies the source address of the ping request packet.	Type the source IP address—a valid address configured on a J Series device interface.
Count	Specifies the number of ping requests to send.	From the list, select the number of ping requests to send. The default is 5 requests.
Detailed Output	Requests the display of extensive rather than brief ping output.	Select the check box to display detailed output.
Instance to which this connection belongs		
Layer 2VPN Name	Identifies the Layer 2 VPN to ping.	Type the name of the VPN to ping.
Remote Site Identifier	Specifies the remote site identifier of the Layer 2 VPN to ping.	Type the remote site identifier for the VPN.
Source Address	Specifies the source address of the ping request packet.	Type the source IP address—a valid address configured on a J Series device interface.
Local Site Identifier	Specifies the local site identifier of the Layer 2 VPN to ping.	Type the local site identifier for the VPN.
Count	Specifies the number of ping requests to send.	From the list, select the number of ping requests to send. The default is 5 requests.
Detailed Output	Requests the display of extensive rather than brief ping output.	Select the check box to display detailed output.
Locate LSP from interface name		
Interface	Specifies the interface on which the ping requests are sent.	From the list, select the J Series device interface on which ping requests are sent. If you select any , the ping requests are sent on all interfaces.
Source Address	Specifies the source address of the ping request packet.	Type the source IP address—a valid address configured on a J Series device interface.
Count	Specifies the number of ping requests to send.	From the list, select the number of ping requests to send. The default is 5 requests.
Detailed Output	Requests the display of extensive rather than brief ping output.	Select the check box to display detailed output.

Table 304: Ping MPLS Troubleshooting Options (continued)

Field	Function	Action
Locate LSP from virtual circuit information		
Remote Neighbor	Identifies the remote neighbor (PE router) within the virtual circuit to ping.	Type the IP address of the remote neighbor within the virtual circuit.
Circuit Identifier	Specifies the virtual circuit identifier for the Layer 2 circuit to ping.	Type the virtual circuit identifier for the Layer 2 circuit.
Source Address	Specifies the source address of the ping request packet.	Type the source IP address—a valid address configured on a J Series device interface.
Count	Specifies the number of ping requests to send.	From the list, select the number of ping requests to send.
Detailed Output	Requests the display of extensive rather than brief ping output.	Select the check box to display detailed output.
Ping endpoint of LSP		
VPN Prefix	Identifies the LSP endpoint to ping.	Type either the LDP FEC prefix and length or the RSVP LSP endpoint address for the LSP to ping.
Source Address	Specifies the source address of the ping request packet.	Type the source IP address—a valid address configured on a J Series device interface.
Count	Specifies the number of ping requests to send.	From the list, select the number of ping requests to send.
Detailed Output	Requests the display of extensive rather than brief ping output.	Select the check box to display detailed output.
Ping MPLS Results and Output Summary		
Exclamation point (!)	Echo reply was received.	—
Period (.)	Echo reply was not received within the timeout period.	—
x	Echo reply was received with an error code. Errored packets are not counted in the received packets count and are accounted for separately.	—
number packets transmitted	number —Number of ping requests (probes) sent to a host.	—
number packets received	number —Number of ping responses received from a host.	—
percentage packet loss	percentage —Number of ping responses divided by the number of ping requests, specified as a percentage.	—

Table 304: Ping MPLS Troubleshooting Options (continued)

Field	Function	Action
time	For Layer 2 circuits only, the number of milliseconds required for the ping packet to reach the destination. This value is approximate, because the packet has to reach the Routing Engine.	–
Output = Packet loss of 100 percent	<p>If the device does not receive ping responses from the destination host (the output shows a packet loss of 100 percent), one of the following explanations might apply:</p> <ul style="list-style-type: none"> • The host is not operational. • There are network connectivity problems between the device and the host. • The host might be configured to ignore echo requests. • The host might be configured with a firewall filter that blocks echo requests or echo responses. • The size of the echo request packet exceeds the MTU of a host along the path. • The outbound node at the remote endpoint is not configured to handle MPLS packets. • The remote endpoint's loopback address is not configured to 127.0.0.1. 	–

See Also • [Troubleshooting Ping Host on page 550](#)

Traceroute

- [Troubleshooting Traceroute on page 557](#)

Troubleshooting Traceroute

Problem **Description:** You can use the traceroute diagnostic tool to display a list of routers between the device and a specified destination host. The output is useful for diagnosing a point of failure in the path from the device to the destination host, and for addressing network traffic latency and throughput problems.

The device generates the list of routers by sending a series of ICMP traceroute packets in which the time-to-live (TTL) value in the messages sent to each successive router is incremented by 1. (The TTL value of the first traceroute packet is set to 1.) In this manner, each router along the path to the destination host replies with a Time Exceeded packet from which the source IP address can be obtained.

Solution To use the traceroute tool:

1. Select **Troubleshoot>Traceroute** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platform.

Or

Select **Administration>Traceroute** in the J-Web user interface.

2. Click the expand icon next to Advanced options.
3. Enter information in the Traceroute page as described in [Table 305 on page 558](#).

The Remote Host field is the only required field.

4. Click **Start**.

The results of the traceroute operation are displayed in the main pane. If no options are specified, each line of the traceroute display is in the following format:

```
hop-number host (ip-address) [as-number] time1 time2 time3
```

The device sends a total of three traceroute packets to each router along the path and displays the round-trip time for each traceroute operation. If the device times out before receiving a Time Exceeded message, an asterisk (*) is displayed for that round-trip time.

5. Click **OK** to stop the traceroute operation before it is complete.

Table 305: Ping Traceroute Troubleshooting Options

Field	Function	Action
Remote Host	Identifies the destination host of the traceroute.	Type the hostname or IP address of the destination host.
Advanced Options		
Don't Resolve Addresses	Determines whether or not hostnames of the hops along the path are displayed, in addition to IP addresses.	<ul style="list-style-type: none"> • To suppress the display of the hop hostnames, select the check box. • To display the hop hostnames, clear the check box.
Gateway	Specifies the IP address of the gateway to route through.	Type the gateway IP address.
Source Address	Specifies the source address of the outgoing traceroute packets.	Type the source IP address.
Bypass Routing	<p>Determines whether or not traceroute packets are routed by means of the routing table.</p> <p>If the routing table is not used, traceroute packets are sent only to hosts on the interface specified in the Interface box. If the host is not on that interface, traceroute responses are not sent.</p>	<ul style="list-style-type: none"> • To bypass the routing table and send the traceroute packets to hosts on the specified interface only, select the check box. • To route the traceroute packets by means of the routing table, clear the check box.

Table 305: Ping Traceroute Troubleshooting Options (continued)

Field	Function	Action
Interface	Specifies the interface on which the traceroute packets are sent.	From the list, select the interface on which traceroute packets are sent. If you select any , the traceroute requests are sent on all interfaces.
Time-to-Live	Specifies the maximum time-to-live (TTL) hop count for the traceroute request packet.	From the list, select the TTL.
Type-of-Service	Specifies the type-of-service (ToS) value to include in the IP header of the traceroute request packet.	From the list, select the decimal value of the ToS field.
Resolve AS Numbers	Determines whether or not the autonomous system (AS) number of each intermediate hop between the device and the destination host is displayed.	<ul style="list-style-type: none"> To display the AS numbers, select the check box. To suppress the display of the AS numbers, clear the check box.
Ping Traceroute Results and Output Summary		
hop-number	Number of the hop (router) along the path.	—
host	Hostname, if available, or IP address of the router.	To suppress the display of the hostname, select the Don't Resolve Addresses check box.
ip-address	IP address of the router.	—
as-number	AS number of the router.	—
time1	Round-trip time between the sending of the first traceroute packet and the receiving of the corresponding Time Exceeded packet from that particular router.	—
time2	Round-trip time between the sending of the second traceroute packet and the receiving of the corresponding Time Exceeded packet from that particular router.	—
time3	Round-trip time between the sending of the third traceroute packet and the receiving of the corresponding Time Exceeded packet from that particular router.	—

Table 305: Ping Traceroute Troubleshooting Options (continued)

Field	Function	Action
Output = Complete path to the destination host not displayed	<p>If the device does not display the complete path to the destination host, one of the following explanations might apply:</p> <ul style="list-style-type: none"> • The host is not operational. • There are network connectivity problems between the device and the host. • The host, or a router along the path, might be configured to ignore ICMP traceroute messages. • The host, or a router along the path, might be configured with a firewall filter that blocks ICMP traceroute requests or ICMP time exceeded responses. • The value you selected in the Time Exceeded box was less than the number of hops in the path to the host. In this case, the host might reply with an ICMP error message. <p>For more information about ICMP, see RFC 792, <i>Internet Control Message Protocol</i>.</p>	—

- See Also**
- [Troubleshooting RPM Setup on page 566](#)
 - [Troubleshooting Packet Capture on page 574](#)

Network Monitoring

- [Alarm on page 560](#)

Alarm

- [Monitoring Chassis Alarm on page 560](#)
- [Monitoring System Alarm on page 563](#)

Monitoring Chassis Alarm

Problem Description: You can view the RPM configuration to verify the following information:

- The RPM configuration is within the expected values.
- The RPM probes are functioning and the RPM statistics are within expected values.
- The device is configured to receive and transmit TCP and UDP RPM probes on the correct ports.

In addition to the RPM statistics for each RPM test, the J-Web interface displays the round-trip times and cumulative jitter graphically. In the graphs, the round-trip time and jitter values are plotted as a function of the system time. Large spikes in round-trip time or jitter indicate a slower outbound (egress) or inbound (ingress) time for the probe sent at that particular time.

Solution To view RPM information:

1. Select **Administration>Network Monitoring>Alarm>Chassis Alarm** in the J-Web user interface.
2. Enter the information specified in [Table 309 on page 572](#) to troubleshoot the issue.

Table 306: RPM Information Troubleshooting Options

Field	Function	Additional Information
Currently Running Tests		
Graph		Click the Graph link to display the graph (if it is not already displayed) or to update the graph for a particular test.
Owner	Configured owner name of the RPM test.	—
Test Name	Configured name of the RPM test.	—
Probe Type	Type of RPM probe configured for the specified test. Following are valid probe types: <ul style="list-style-type: none"> • http-get • http-get-metadata • icmp-ping • icmp-ping-timestamp • tcp-ping • udp-ping 	—
Target Address	IP address or URL of the remote server that is being probed by the RPM test.	—
Source Address	Explicitly configured source address that is included in the probe packet headers.	If no source address is configured, the RPM probe packets use the outgoing interface as the source address, and the Source Address field is empty.
Minimum RTT	Shortest round-trip time from the J Series device to the remote server, as measured over the course of the test.	—
Maximum RTT	Longest round-trip time from the J Series device to the remote server, as measured over the course of the test.	—
Average RTT	Average round-trip time from the J Series device to the remote server, as measured over the course of the test.	—
Standard Deviation RTT	Standard deviation of round-trip times from the J Series device to the remote server, as measured over the course of the test.	—

Table 306: RPM Information Troubleshooting Options (continued)

Field	Function	Additional Information
Probes Sent	Total number of probes sent over the course of the test.	—
Loss Percentage	Percentage of probes sent for which a response was not received.	—
Round-Trip Time for a Probe		
Samples	Total number of probes used for the data set.	The J Series device maintains records of the most recent 50 probes for each configured test. These 50 probes are used to generate RPM statistics for a particular test.
Earliest Sample	System time when the first probe in the sample was received.	—
Latest Sample	System time when the last probe in the sample was received.	—
Mean Value	Average round-trip time for the 50-probe sample.	—
Standard Deviation	Standard deviation of the round-trip times for the 50-probe sample.	—
Lowest Value	Shortest round-trip time from the device to the remote server, as measured over the 50-probe sample.	—
Time of Lowest Sample	System time when the lowest value in the 50-probe sample was received.	—
Highest Value	Longest round-trip time from the J Series device to the remote server, as measured over the 50-probe sample.	—
Time of Highest Sample	System time when the highest value in the 50-probe sample was received.	—
Cumulative Jitter for a Probe		
Samples	Total number of probes used for the data set.	The J Series device maintains records of the most recent 50 probes for each configured test. These 50 probes are used to generate RPM statistics for a particular test.
Earliest Sample	System time when the first probe in the sample was received.	—
Latest Sample	System time when the last probe in the sample was received.	—

Table 306: RPM Information Troubleshooting Options (continued)

Field	Function	Additional Information
Mean Value	Average jitter for the 50-probe sample.	—
Standard Deviation	Standard deviation of the jitter values for the 50-probe sample.	—
Lowest Value	Smallest jitter value, as measured over the 50-probe sample.	—
Time of Lowest Sample	System time when the lowest value in the 50-probe sample was received.	—
Highest Value	Highest jitter value, as measured over the 50-probe sample.	—
Time of Highest Sample	System time when the highest jitter value in the 50-probe sample was received.	—

See Also • [Troubleshooting RPM Setup on page 566](#)

Monitoring System Alarm

Problem **Description:** You can view the RPM configuration to verify the following information:

- The RPM configuration is within the expected values.
- The RPM probes are functioning and the RPM statistics are within expected values.
- The device is configured to receive and transmit TCP and UDP RPM probes on the correct ports.

In addition to the RPM statistics for each RPM test, the J-Web interface displays the round-trip times and cumulative jitter graphically. In the graphs, the round-trip time and jitter values are plotted as a function of the system time. Large spikes in round-trip time or jitter indicate a slower outbound (egress) or inbound (ingress) time for the probe sent at that particular time.

Solution To view RPM information:

1. Select **Administration>Network Monitoring>Alarm>System Alarm** in the J-Web user interface.
2. Enter the information specified in [Table 309 on page 572](#) to troubleshoot the issue.

Table 307: RPM Information Troubleshooting Options

Field	Function	Additional Information
Currently Running Tests		
Graph		Click the Graph link to display the graph (if it is not already displayed) or to update the graph for a particular test.
Owner	Configured owner name of the RPM test.	—
Test Name	Configured name of the RPM test.	—
Probe Type	Type of RPM probe configured for the specified test. Following are valid probe types: <ul style="list-style-type: none"> • http-get • http-get-metadata • icmp-ping • icmp-ping-timestamp • tcp-ping • udp-ping 	—
Target Address	IP address or URL of the remote server that is being probed by the RPM test.	—
Source Address	Explicitly configured source address that is included in the probe packet headers.	If no source address is configured, the RPM probe packets use the outgoing interface as the source address, and the Source Address field is empty.
Minimum RTT	Shortest round-trip time from the J Series device to the remote server, as measured over the course of the test.	—
Maximum RTT	Longest round-trip time from the J Series device to the remote server, as measured over the course of the test.	—
Average RTT	Average round-trip time from the J Series device to the remote server, as measured over the course of the test.	—
Standard Deviation RTT	Standard deviation of round-trip times from the J Series device to the remote server, as measured over the course of the test.	—
Probes Sent	Total number of probes sent over the course of the test.	—
Loss Percentage	Percentage of probes sent for which a response was not received.	—

Table 307: RPM Information Troubleshooting Options (continued)

Field	Function	Additional Information
Round-Trip Time for a Probe		
Samples	Total number of probes used for the data set.	The J Series device maintains records of the most recent 50 probes for each configured test. These 50 probes are used to generate RPM statistics for a particular test.
Earliest Sample	System time when the first probe in the sample was received.	—
Latest Sample	System time when the last probe in the sample was received.	—
Mean Value	Average round-trip time for the 50-probe sample.	—
Standard Deviation	Standard deviation of the round-trip times for the 50-probe sample.	—
Lowest Value	Shortest round-trip time from the device to the remote server, as measured over the 50-probe sample.	—
Time of Lowest Sample	System time when the lowest value in the 50-probe sample was received.	—
Highest Value	Longest round-trip time from the J Series device to the remote server, as measured over the 50-probe sample.	—
Time of Highest Sample	System time when the highest value in the 50-probe sample was received.	—
Cumulative Jitter for a Probe		
Samples	Total number of probes used for the data set.	The J Series device maintains records of the most recent 50 probes for each configured test. These 50 probes are used to generate RPM statistics for a particular test.
Earliest Sample	System time when the first probe in the sample was received.	—
Latest Sample	System time when the last probe in the sample was received.	—
Mean Value	Average jitter for the 50-probe sample.	—
Standard Deviation	Standard deviation of the jitter values for the 50-probe sample.	—

Table 307: RPM Information Troubleshooting Options (continued)

Field	Function	Additional Information
Lowest Value	Smallest jitter value, as measured over the 50-probe sample.	—
Time of Lowest Sample	System time when the lowest value in the 50-probe sample was received.	—
Highest Value	Highest jitter value, as measured over the 50-probe sample.	—
Time of Highest Sample	System time when the highest jitter value in the 50-probe sample was received.	—

See Also • [Troubleshooting RPM Setup on page 566](#)

RPM

- [Troubleshooting RPM Setup on page 566](#)
- [Troubleshooting RPM Information on page 571](#)

Troubleshooting RPM Setup

Problem **Description:** You can configure RPM parameters to monitor real-time performance through the J-Web interface.

Solution To configure RPM parameters:

1. Select **Troubleshoot>RPM>Setup RPM** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platform.
Or
Select **Administration>RPM>Setup RPM** in the J-Web user interface.
2. Enter the information specified in [Table 308 on page 567](#) to troubleshoot the issue.
3. From the main RPM configuration page, click one:
 - **Apply**—Applies the configuration and stays on the RPM configuration page.
 - **OK**—Applies the configuration and returns to the RPM configuration page.
 - **Cancel**—Cancels your entries and returns to the RPM configuration page.

Table 308: RPM Setup Troubleshooting Options

Field	Function	Action
Probe Owners		
Identification		
Owner Name	Specifies an RPM owner for which one or more RPM tests are configured. In most implementations, the owner name identifies a network on which a set of tests is being run (a particular customer, for example).	Type the name of the RPM owner.
Performance Probe Tests		
Identification		
Test name	Specifies a unique name to identify the RPM test.	Type the name of the RPM test.
Target (Address or URL)	Specifies an IP address or a URL of a probe target.	Type the IP address, in dotted decimal notation, or the URL of the probe target. If the target is a URL, type a fully formed URL that includes http:// .
Source Address	Specifies an IP address to be used as the probe source address.	Type the source address to be used for the probe. If the source IP address is not one of the device's assigned addresses, the packet uses the outgoing interface's address as its source.
Routing Instance	Specifies a routing instance over which the probe is sent.	Type the routing instance name. The routing instance applies only to probes of type icmp and icmp-timestamp . The default routing instance is inet.0 .
History Size	Specifies the number of probe results saved in the probe history.	Type a number between 0 and 255. The default history size is 50 probes.
Request Information		
Probe Type	Specifies the type of probe to send as part of the test.	Select the desired probe type from the list: <ul style="list-style-type: none"> • http-get • http-get-metadata • icmp-ping • icmp-ping-timestamp • tcp-ping • udp-ping
Interval	Specifies the wait time (in seconds) between each probe transmission.	Type a number between 1 and 255 (seconds).
Test Interval	Specifies the wait time (in seconds) between tests.	Type a number between 0 and 86400 (seconds).

Table 308: RPM Setup Troubleshooting Options (continued)

Field	Function	Action
Probe Count	Specifies the total number of probes to be sent for each test.	Type a number between 1 and 15.
Moving Average Size	Specifies the number of samples used for a moving average.	Type a number between 0 and 225.
Destination Port	Specifies the TCP or UDP port to which probes are sent. To use TCP or UDP probes, you must configure the remote server as a probe receiver. Both the probe server and the remote server must be Juniper Networks devices configured to receive and transmit RPM probes on the same TCP or UDP port.	Type the number 7—a standard TCP or UDP port number—or a port number from 49152 through 65535.
DSCP Bits	Specifies the Differentiated Services code point (DSCP) bits. This value must be a valid 6-bit pattern. The default is 000000 .	Type a valid 6-bit pattern.
Data Size	Specifies the size of the data portion of the ICMP probes.	Type a size (in bytes) between 0 and 65507.
Data Fill	Specifies the contents of the data portion of the ICMP probes.	Type a hexadecimal value between 1 and 800h to use as the contents of the ICMP probe data.
Hardware Timestamp		
One Way Hardware Timestamp	Specifies the hardware timestamps for one-way measurements.	To enable one-way timestamping, select the check box.
Hardware Timestamp	Specifies timestamping of RPM probe messages. You can timestamp the following RPM probes to improve the measurement of latency or jitter: <ul style="list-style-type: none"> • ICMP ping • ICMP ping timestamp • UDP ping—destination port UDP-ECHO (port 7) only • UDP ping timestamp—destination port UDP-ECHO (port 7) only 	To enable timestamping, select the check box.
Destination Interface	Specifies the name of an output interface for probes.	Select the interface from the drop-down list.
Maximum Probe Thresholds		

Table 308: RPM Setup Troubleshooting Options (continued)

Field	Function	Action
Successive Lost Probes	Specifies the total number of probes that must be lost successively to trigger a probe failure and generate a system log message.	Type a number between 0 and 15.
Lost Probes	Specifies the total number of probes that must be lost to trigger a probe failure and generate a system log message.	Type a number between 0 and 15.
Round Trip Time	Specifies the total round-trip time (in microseconds), from the device to the remote server, that triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds).
Jitter	Specifies the total jitter (in microseconds) for a test that triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds).
Standard Deviation	Specifies the maximum allowable standard deviation (in microseconds) for a test, which, if exceeded, triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds).
Egress Time	Specifies the total one-way time (in microseconds), from the device to the remote server, that triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds).
Ingress Time	Specifies the total one-way time (in microseconds), from the remote server to the device, that triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds).
Jitter Egress Time	Specifies the total outbound-time jitter (in microseconds) for a test that triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds).
Jitter Ingress Time	Specifies the total inbound-time jitter (in microseconds) for a test that triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds).
Egress Standard Deviation	Specifies the maximum allowable standard deviation of outbound times (in microseconds) for a test, which, if exceeded, triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds).

Table 308: RPM Setup Troubleshooting Options (continued)

Field	Function	Action
Ingress Standard Deviation	Specifies the maximum allowable standard deviation of inbound times (in microseconds) for a test, which, if exceeded, triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds).
Traps		
Egress Jitter Exceeded	Generates SNMP traps when the threshold for jitter in outbound time is exceeded.	<ul style="list-style-type: none"> To enable SNMP traps for this condition, select the check box. To disable SNMP traps, clear the check box.
Egress Standard Deviation Exceeded	Generates SNMP traps when the threshold for standard deviation in outbound times is exceeded.	<ul style="list-style-type: none"> To enable SNMP traps for this condition, select the check box. To disable SNMP traps, clear the check box.
Egress Time Exceeded	Generates SNMP traps when the threshold for maximum outbound time is exceeded.	<ul style="list-style-type: none"> To enable SNMP traps for this condition, select the check box. To disable SNMP traps, clear the check box.
Ingress Jitter Exceeded	Generates SNMP traps when the threshold for jitter in inbound time is exceeded.	<ul style="list-style-type: none"> To enable SNMP traps for this condition, select the check box. To disable SNMP traps, clear the check box.
Ingress Standard Deviation Exceeded	Generates SNMP traps when the threshold for standard deviation in inbound times is exceeded.	<ul style="list-style-type: none"> To enable SNMP traps for this condition, select the check box. To disable SNMP traps, clear the check box.
Ingress Time Exceeded	Generates traps when the threshold for maximum inbound time is exceeded.	<ul style="list-style-type: none"> To enable SNMP traps for this condition, select the check box. To disable SNMP traps, clear the check box.
Jitter Exceeded	Generates traps when the threshold for jitter in round-trip time is exceeded.	<ul style="list-style-type: none"> To enable SNMP traps for this condition, select the check box. To disable SNMP traps, clear the check box.
Probe Failure	Generates traps when the threshold for the number of successive lost probes is reached.	<ul style="list-style-type: none"> To enable SNMP traps for this condition, select the check box. To disable SNMP traps, clear the check box.
RTT Exceeded	Generates traps when the threshold for maximum round-trip time is exceeded.	<ul style="list-style-type: none"> To enable SNMP traps for this condition, select the check box. To disable SNMP traps, clear the check box.
Standard Deviation Exceeded	Generates traps when the threshold for standard deviation in round-trip times is exceeded.	<ul style="list-style-type: none"> To enable SNMP traps for this condition, select the check box. To disable SNMP traps, clear the check box.
Test Completion	Generates traps when a test is completed.	<ul style="list-style-type: none"> To enable SNMP traps for this condition, select the check box. To disable SNMP traps, clear the check box.

Table 308: RPM Setup Troubleshooting Options (continued)

Field	Function	Action
Test Failure	Generates traps when the threshold for the total number of lost probes is reached.	<ul style="list-style-type: none"> To enable SNMP traps for this condition, select the check box. To disable SNMP traps, clear the check box.
Maximum Number of Concurrent Probes		
Maximum Number of Concurrent Probes	Specifies the maximum number of concurrent probes allowed.	Type a number between 1 and 500.
Probe Server		
TCP Probe Server	Specifies the port on which the device is to receive and transmit TCP probes.	Type number 7, or a port number from 49160 through 65535.
UDP Probe Server	Specifies the port on which the device is to receive and transmit UDP probes.	Type number 7, or a port number from 49160 through 65535.

See Also • [Troubleshooting RPM Information on page 571](#)

Troubleshooting RPM Information

Problem **Description:** You can view the RPM configuration to verify the following information:

- The RPM configuration is within the expected values.
- The RPM probes are functioning and the RPM statistics are within expected values.
- The device is configured to receive and transmit TCP and UDP RPM probes on the correct ports.

In addition to the RPM statistics for each RPM test, the J-Web interface displays the round-trip times and cumulative jitter graphically. In the graphs, the round-trip time and jitter values are plotted as a function of the system time. Large spikes in round-trip time or jitter indicate a slower outbound (egress) or inbound (ingress) time for the probe sent at that particular time.

Solution To view RPM information:

- Select **Troubleshoot>RPM>View RPM** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platform.
Or
Select **Administration>RPM>View RPM** in the J-Web user interface.
- Enter the information specified in [Table 309 on page 572](#) to troubleshoot the issue.

Table 309: RPM Information Troubleshooting Options

Field	Function	Additional Information
Currently Running Tests		
Graph		Click the Graph link to display the graph (if it is not already displayed) or to update the graph for a particular test.
Owner	Configured owner name of the RPM test.	—
Test Name	Configured name of the RPM test.	—
Probe Type	Type of RPM probe configured for the specified test. Following are valid probe types: <ul style="list-style-type: none"> • http-get • http-get-metadata • icmp-ping • icmp-ping-timestamp • tcp-ping • udp-ping 	—
Target Address	IP address or URL of the remote server that is being probed by the RPM test.	—
Source Address	Explicitly configured source address that is included in the probe packet headers.	If no source address is configured, the RPM probe packets use the outgoing interface as the source address, and the Source Address field is empty.
Minimum RTT	Shortest round-trip time from the J Series device to the remote server, as measured over the course of the test.	—
Maximum RTT	Longest round-trip time from the J Series device to the remote server, as measured over the course of the test.	—
Average RTT	Average round-trip time from the J Series device to the remote server, as measured over the course of the test.	—
Standard Deviation RTT	Standard deviation of round-trip times from the J Series device to the remote server, as measured over the course of the test.	—
Probes Sent	Total number of probes sent over the course of the test.	—
Loss Percentage	Percentage of probes sent for which a response was not received.	—

Table 309: RPM Information Troubleshooting Options (continued)

Field	Function	Additional Information
Round-Trip Time for a Probe		
Samples	Total number of probes used for the data set.	The J Series device maintains records of the most recent 50 probes for each configured test. These 50 probes are used to generate RPM statistics for a particular test.
Earliest Sample	System time when the first probe in the sample was received.	—
Latest Sample	System time when the last probe in the sample was received.	—
Mean Value	Average round-trip time for the 50-probe sample.	—
Standard Deviation	Standard deviation of the round-trip times for the 50-probe sample.	—
Lowest Value	Shortest round-trip time from the device to the remote server, as measured over the 50-probe sample.	—
Time of Lowest Sample	System time when the lowest value in the 50-probe sample was received.	—
Highest Value	Longest round-trip time from the J Series device to the remote server, as measured over the 50-probe sample.	—
Time of Highest Sample	System time when the highest value in the 50-probe sample was received.	—
Cumulative Jitter for a Probe		
Samples	Total number of probes used for the data set.	The J Series device maintains records of the most recent 50 probes for each configured test. These 50 probes are used to generate RPM statistics for a particular test.
Earliest Sample	System time when the first probe in the sample was received.	—
Latest Sample	System time when the last probe in the sample was received.	—
Mean Value	Average jitter for the 50-probe sample.	—
Standard Deviation	Standard deviation of the jitter values for the 50-probe sample.	—

Table 309: RPM Information Troubleshooting Options (continued)

Field	Function	Additional Information
Lowest Value	Smallest jitter value, as measured over the 50-probe sample.	—
Time of Lowest Sample	System time when the lowest value in the 50-probe sample was received.	—
Highest Value	Highest jitter value, as measured over the 50-probe sample.	—
Time of Highest Sample	System time when the highest jitter value in the 50-probe sample was received.	—

See Also • [Troubleshooting RPM Setup on page 566](#)

Packet Capture

- [Troubleshooting Packet Capture on page 574](#)

Troubleshooting Packet Capture

Problem **Description:** You can use the J-Web packet capture diagnostic tool to quickly capture and analyze router control traffic on a device. You can capture traffic destined for or originating from the Routing Engine, and you can compose expressions with various matching criteria to specify the packets that you want to capture. You can either choose to decode and view the captured packets as they are captured, or to save the captured packets to a file and analyze them offline using packet analyzers such as Ethereal. J-Web packet capture does not capture transient traffic.

To capture transient traffic and entire IPv4 data packets for offline analysis, you must configure packet capture with the J-Web or CLI configuration editor.

Solution To use J-Web packet capture:

1. Select **Troubleshoot>Packet Capture** in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platform.
- Or
Select **Administration>Packet Capture** in the J-Web user interface.
2. Enter the information specified in [Table 310 on page 575](#) to troubleshoot the issue.
3. Save the captured packets to a file or specify other advanced options by clicking the expand icon next to Advanced options.

4. Click **Start**.

The captured packet headers are decoded and displayed in the Packet Capture display.

5. Click one:

- **Stop Capturing**—Stops capturing the packets and stays on the same page while the decoded packet headers are being displayed.
- **OK**—Stops capturing packets and returns to the Packet Capture page.

Table 310: Packet Capture Troubleshooting Options

Field	Function	Action
Interface	<p>Specifies the interface on which the packets are captured.</p> <p>If you select default, packets on the Ethernet management port 0 are captured.</p>	From the list, select an interface—for example, ge-0/0/0 .
Detail level	<p>Specifies the extent of details to be displayed for the packet headers.</p> <ul style="list-style-type: none"> • Brief—Displays the minimum packet header information. This is the default. • Detail—Displays packet header information in moderate detail. • Extensive—Displays the maximum packet header information. 	From the list, select Detail .
Packets	<p>Specifies the number of packets to be captured. Values range from 1 to 1000. Default is 10. Packet capture stops capturing packets after this number is reached.</p>	From the list, select the number of packets to be captured—for example, 10 .
Addresses	<p>Specifies the addresses to be matched for capturing the packets using a combination of the following parameters:</p> <ul style="list-style-type: none"> • Direction—Matches the packet headers for IP address, hostname, or network address of the source, destination, or both. • Type—Specifies if packet headers are matched for host address or network address. <p>You can add multiple entries to refine the match criteria for addresses.</p>	<p>Select address-matching criteria. For example:</p> <ol style="list-style-type: none"> 1. From the Direction list, select source. 2. From the Type list, select host. 3. In the Address box, type 10.1.40.48. 4. Click Add.

Table 310: Packet Capture Troubleshooting Options (continued)

Field	Function	Action
Protocols	Matches the protocol for which packets are captured. You can choose to capture TCP, UDP, or ICMP packets or a combination of TCP, UDP, and ICMP packets.	From the list, select a protocol—for example, tcp .
Ports	Matches the packet headers containing the specified source or destination TCP or UDP port number or port name.	Select a direction and a port. For example: 1. From the Type list, select src . 2. In the Port box, type 23 .
Advanced Options		
Absolute TCP Sequence	Displays the absolute TCP sequence numbers for the packet headers.	<ul style="list-style-type: none"> To display absolute TCP sequence numbers in the packet headers, select this check box. To stop displaying absolute TCP sequence numbers in the packet headers, clear this check box.
Layer 2 Headers	Displays the link-layer packet headers.	<ul style="list-style-type: none"> To include link-layer packet headers while capturing packets, select this check box. To exclude link-layer packet headers while capturing packets, clear this check box.
Non-Promiscuous	<p>Does not place the interface in promiscuous mode so that the interface reads only packets addressed to it.</p> <p>In promiscuous mode, the interface reads every packet that reaches it.</p>	<ul style="list-style-type: none"> To read all packets that reach the interface, select this check box. To read only packets addressed to the interface, clear this check box.
Display Hex	Displays packet headers, except link-layer headers, in hexadecimal format.	<ul style="list-style-type: none"> To display the packet headers in hexadecimal format, select this check box. To stop displaying the packet headers in hexadecimal format, clear this check box.
Display ASCII and Hex	Displays packet headers in hexadecimal and ASCII formats.	<ul style="list-style-type: none"> To display the packet headers in ASCII and hexadecimal formats, select this check box. To stop displaying the packet headers in ASCII and hexadecimal formats, clear this check box.
Header Expression	<p>Specifies the match condition for the packets to be captured.</p> <p>The match conditions you specify for Addresses, Protocols, and Ports are displayed in expression format in this field.</p>	Enter match conditions directly in this field in expression format or modify the expression composed from the match conditions you specified for Addresses, Protocols, and Ports. If you change the match conditions specified for Addresses, Protocols, and Ports again, packet capture overwrites your changes with the new match conditions.

Table 310: Packet Capture Troubleshooting Options (continued)

Field	Function	Action
Packet Size	Specifies the number of bytes to be displayed for each packet. If a packet header exceeds this size, the display is truncated for the packet header. The default value is 96 bytes.	Type the number of bytes you want to capture for each packet header—for example, 256 .
Don't Resolve Addresses	Specifies that IP addresses are not to be resolved into hostnames in the packet headers displayed.	<ul style="list-style-type: none"> To prevent packet capture from resolving IP addresses to hostnames, select this check box. To resolve IP addresses into hostnames, clear this check box.
No Timestamp	Suppresses the display of packet header timestamps.	<ul style="list-style-type: none"> To stop displaying timestamps in the captured packet headers, select this check box. To display the timestamp in the captured packet headers, clear this check box.
Write Packet Capture File	<p>Writes the captured packets to a file in PCAP format in /var/tmp. The files are named with the prefix jweb-pcap and the extension .pcap.</p> <p>If you select this option, the decoded packet headers are not displayed on the packet capture page.</p>	<ul style="list-style-type: none"> To save the captured packet headers to a file, select this check box. To decode and display the packet headers on the J-Web page, clear this check box.

Packet Capture Results and Output Summary

timestamp	<p>Displays the time when the packet was captured. The timestamp 00:45:40.823971 means 00 hours (12.00 a.m.), 45 minutes, and 40.823971 seconds.</p> <p>NOTE: The time displayed is local time.</p>	—
direction	<p>Displays the direction of the packet. Specifies whether the packet originated from the Routing Engine (Out) or was destined for the Routing Engine (In).</p>	—
protocol	<p>Displays the protocol for the packet.</p> <p>In the sample output, IP indicates the Layer 3 protocol.</p>	—

Table 310: Packet Capture Troubleshooting Options (continued)

Field	Function	Action
<i>source address</i>	Displays the hostname, if available, or IP address and the port number of the packet's origin. If the Don't Resolve Addresses check box is selected, only the IP address of the source is displayed. NOTE: When a string is defined for the port, the packet capture output displays the string instead of the port number.	—
<i>destination address</i>	Displays the hostname, if available, or IP address of the packet's destination with the port number. If the Don't Resolve Addresses check box is selected, only the IP address of the destination and the port are displayed. NOTE: When a string is defined for the port, the packet capture output displays the string instead of the port number.	—
<i>protocol</i>	Displays the protocol for the packet. In the sample output, TCP indicates the Layer 4 protocol.	—
<i>data size</i>	Displays the size of the packet (in bytes).	—

- See Also**
- [Troubleshooting RPM Information on page 571](#)
 - [Understanding the J-Web CLI Terminal on page 578](#)

CLI Terminal

- [Understanding the J-Web CLI Terminal on page 578](#)

Understanding the J-Web CLI Terminal

The J-Web CLI terminal provides access to the Junos OS command-line interface (CLI) through the J-Web interface. The functionality and behavior of the CLI available through the CLI terminal page is the same as the Junos OS CLI available through the routing platform console. The CLI terminal supports all CLI commands and other features such as CLI Help and autocompletion. Using the CLI terminal page you can fully configure, monitor, and manage your routing platform.

This topic includes the following sections:

- [CLI Terminal Requirements on page 579](#)
- [CLI Overview on page 579](#)

CLI Terminal Requirements

To access the CLI through the J-Web interface, your management device requires the following features:

- **SSH access**—Secure shell (SSH) provides a secured method of logging in to the routing platform to encrypt traffic so that it is not intercepted. If SSH is not enabled on your system, the CLI terminal page displays an error and provides a link to the Set Up Quick Configuration page where you can enable SSH.



NOTE: Starting in Junos Release 19.2R1, the following changes are made to the Quick Setup wizard:

- The initial configuration summary page is not be available as you cannot configure any of the fields from this page.
- For SRX300 line of devices, the Set Device Password option is removed if the root password is already set through Skip to JWeb from phone home during the factory default settings. This will avoid setting up the password again.

- **Java applet support**—Your Web browser must support Java applets.
- **JRE installed on the client**—Java Runtime Environment (JRE) version 1.4 or later must be installed on your system to run Java applications. Download the latest JRE version from the Java Software website <http://www.java.com/>. Installing JRE installs Java plug-ins, which once installed, load automatically and transparently to render Java applets.



NOTE: The CLI terminal is supported on JRE version 1.4 or later only.

CLI Overview

The Junos OS CLI uses industry-standard tools and utilities to provide a set of commands for monitoring and configuring a routing platform. You type commands on a line and press Enter to execute them. The CLI provides online 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 commands in the CLI are organized hierarchically, with commands that perform a similar function grouped together under the same level. For example, all commands that display information about the device system and system software are grouped under the **show** command, and all commands that display information about the routing table are grouped under the **show route** command. The hierarchical organization results in commands that have a regular syntax and provides the following features that simplify CLI use:

- Consistent command names—Commands that provide the same type of function have the same name, regardless of the portion of the software they are operating on. For example, all **show** commands display software information and statistics, and all **clear** commands erase various types of system information.
- Lists and short descriptions of available commands—Information about available commands is provided at each level of the CLI command hierarchy. If you type a question mark (?) at any level, you see a list of the available commands along with a short description of each command.
- Command completion—Command completion for command names (keywords) and command options is also available at each level of the hierarchy. In the CLI terminal, you can perform one of the following actions to complete a command:
 - Enter a partial command name followed immediately by a question mark (with no intervening space) to see a list of commands that match the partial name you typed.
 - Press the Spacebar to complete a command or option that you have partially typed. If the partially typed letters begin a string that uniquely identifies a command, the complete command name appears. Otherwise, a prompt indicates that you have entered an ambiguous command, and the possible completions are displayed.

The Tab key option is currently not available on the CLI terminal.

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.

For more information about the Junos OS CLI, see the [Junos OS CLI User Guide](#).

- See Also**
- [Troubleshooting Ping Host on page 550](#)
 - [Troubleshooting Ping MPLS on page 553](#)
 - [Troubleshooting Traceroute on page 557](#)
 - [Troubleshooting Packet Capture on page 574](#)

SKY ATP Enrollment

- [Sky ATP Enrollment on page 580](#)

Sky ATP Enrollment

Sky Advanced Threat Prevention (Sky ATP) is a cloud-based threat identification and prevention solution by Juniper Networks. It protects you from malware and sophisticated cyber threat by inspecting email and web traffic for advanced threats.

Sky ATP integrates with the SRX Series devices and simplifies deployment and enhance the anti-threat capabilities of the SRX firewall.

Use this page to enroll the SRX device to Sky ATP.

- Understand which type of Sky ATP license you have: free or premium. The license controls which Sky ATP features are available.
- To configure a Sky ATP realm, you must already have a Sky ATP account with an associated license.
- Decide which region will be covered by the realm you are creating. You must select a region when you configure a realm.

To enroll your device to Sky ATP from J-Web:

1. Select **Administration>Sky ATP Enrollment**.

The SKY ATP Enrollment page appears.

2. Click **Launch** to get enrollment command.

You will be redirected to the Select Geographic Region page in a new tab in the browser. Read the instructions in this page and decide which region will be covered by the realm you are creating. You must select a region when you configure a realm.

3. (Configure>Security>Proxy Profile) Created proxy profile can be selected from the drop down list and map to security-intelligence & advanced-anti-malware connections by clicking the **Apply** button.

4. Select the geographic location of your SKY ATP Cloud Service from the dropdown list.

The available options are: North America and European Union.

Click **Go**.

You will be redirected to the Sky ATP server login page associated with the location that you selected.

5. Enter your Sky ATP login credentials and log in.

A security realm is a group identifier for an organization used to restrict access to Web applications. You must create at least one security realm to login into Sky ATP. Once you create a realm, you can enroll SRX Series devices into the realm. You can also give more users (administrators) permission to access the realm. If you have multiple security realms, note that each SRX Series device can only be bound to one realm, and users cannot travel between realms.

The Sky ATP user interface application appears.

6. Click **Devices**.

The Enrolled Devices page appears.

7. Click **Enroll** in the Enrolled Devices page.

The Enroll popup window appears displaying a URL.

8. Copy the URL displayed in the Enroll popup window.

9. Go back to the browser tab where J-Web application is residing.

The SKY ATP Enrollment page in J-Web from where you had navigated to the Sky ATP application is displayed.

10. Paste the URL that you copied from the Sky ATP application in the Inside Enrollment text box in the SKY ATP Enrollment page of J-Web.

11. Click **Enroll**.

The **Enrollment Status: IN PROGRESS** is displayed. The enrollment process will take 6 to 7 minutes. After the enrollment is complete, the status changes to **SUCCESSFUL** or **FAILED**.

Starting in Junos OS Release 19.2R1, go to **Administration > Sky ATP Enrollment** and follow the steps to enroll your device to Juniper Sky ATP from J-Web:

STEP 1 Proxy Profile Configuration (Optional)

To configure proxy profile:



NOTE: If proxy profile is configured, then all communication between SRX device and Juniper Sky ATP happens through proxy server. If not, then the SRX device and Juniper Sky ATP communicates directly.

1. Select an option in the Proxy Profile.



NOTE: The list displays the proxy profile created in the Proxy Profile page (Configure > Security Services > Security Policy > Objects > Proxy Profiles).

Or

2. Click **Create Proxy** to create a proxy profile.

Create Proxy Profile page appears.

3. Enter the following details:

- a. Profile Name—Enter a name for the proxy profile.
- b. Connection Type—Select the type of connection used by the proxy profile: Server IP or Host Name.

- c. Port Number—Select a port number for the proxy profile from 0 to 65535.
4. Click **OK**.

STEP 2 Enroll SRX Device with SKY ATP

To enroll a SRX device to Juniper Sky ATP:

1. Log in to Juniper Sky ATP Web UI or click **Launch**.

Clicking **Launch** redirects you to the Select Geographic Region page in a new tab in the browser. Read the instructions in this page and decide which region is covered by the realm that you are creating.



NOTE: You must select a region when you configure a realm.

2. Click the **Enroll** button on the Devices page.
3. Copy the command to your clipboard and click **OK**.
4. Follow Step 3 on J-Web UI to initiate the enrollment.

STEP 3 Initiate Enrollment

Paste the command that was copied from Juniper Sky ATP Web UI and click **Enroll** to enroll the SRX device to Juniper Sky ATP.



NOTE: The command is valid for seven days. Running this command, commits the existing configuration changes (if any) and stops the previously generated enroll commands (if any).

If you want to remove any existing SRX device enrollment, paste the command in the J-Web UI and click **Disenroll**.

- See Also**
- *Diagnostic Tools Overview*
 - *J-Web Traceroute Results and Output Summary*
 - *Using the J-Web Ping MPLS Tool*
 - *Using the J-Web Ping Host Tool*
 - *Using the J-Web Packet Capture Tool*

