

J-Web User Guide for SRX Series Firewalls

Published
2024-03-25

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.

J-Web User Guide for SRX Series Firewalls

Copyright © 2024 Juniper Networks, Inc. All rights reserved.

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

About This Guide | xxviii

1

Juniper Web Device Manager

Getting Started | 2

Juniper Web Device Manager Overview | 2

What is J-Web? | 2

Benefits of J-Web | 3

Access the J-Web User Interface | 3

Prerequisites for Using J-Web | 3

Log in to J-Web | 4

The J-Web Setup Wizard | 8

Configure SRX Series Firewalls Using the J-Web Setup Wizard | 8

Example: J-Web Wizard for Standalone Mode | 10

J-Web Setup Wizard Parameters | 22

Explore J-Web | 39

J-Web: A First Look | 40

J-Web Launch Pad | 40

J-Web Top Pane | 42

J-Web Side Pane | 44

J-Web Main Pane | 47

J-Web Workflow Wizards | 49

Summary | 50

2

Add SRX Series Firewall to Security Director Cloud

Add an SRX Series Firewall to Juniper Security Director Cloud | 52

3

Dashboard

J-Web Dashboard | 55

Dashboard Overview | 55

What is J-Web Dashboard | 55

Work with Widgets | 56

4

Monitor**Network | 62**

Monitor Interfaces | 62

Monitor DHCP Server Bindings | 63

Monitor IPsec VPN | 65

Logs | 69

Monitor Session | 69

Monitor Threats | 75

Monitor Web Filtering | 81

Monitor ATP | 85

Monitor VPN | 90

Monitor All Events | 93

Monitor System | 101

Monitor Alarms | 103

Maps and Charts | 105

Monitor Traffic Map | 105

Monitor Threats Map | 108

Monitor Applications | 115

Monitor Users | 118

Statistics | 120

Monitor Threat Prevention | 120

Monitor VPN Phase I | 122

Monitor VPN Phase II | 123

Monitor DNS Security | 125

Monitor Encrypted Traffic Insights | 127

Reports | 129

About Reports Page | 129

- Overview | 130**
- Threat Assessment Report | 135**
- Application and User Usage | 135**
- Top Talkers | 136**
- IPS Threat Environment | 136**
- Viruses Blocked | 136**
- URL Report | 137**
- Virus: Top Blocked | 137**
- Top Firewall Events | 137**
- Top Firewall Deny Destinations | 137**
- Top Firewall Denies | 137**
- Top IPS Events | 137**
- Top Anti-spam Detected | 138**
- Top Screen Attackers | 138**
- Top Screen Victims | 138**
- Top Screen Hits | 138**
- Top Firewall Rules | 138**
- Top Firewall Deny Sources | 138**
- Top IPS Attack Sources | 138**
- Top IPS Attack Destinations | 138**
- Top IPS Rules | 138**
- Top Web Apps | 139**
- Top Applications Blocked | 139**
- Top URLs by User | 139**
- Top Source Zone by Volume | 139**
- Top Applications by User | 139**
- Top Botnet Threats By Source Address via IDP Logs | 139**
- Top Botnet Threats by Destination Address via IDP Logs | 139**
- Top Botnet Threats by Threat Severity via IDP Logs | 140**
- Top Malware Threats by Source Address via IDP Logs | 140**
- Top Malware Threats by Destination Address via IDP Logs | 140**
- Top Malware Threats by Threat Severity via IDP Logs | 140**
- Top Blocked Applications via Webfilter Logs | 140**
- Top Permitted Application Subcategories by Volume via Webfilter Logs | 141**
- Top Permitted Application Subcategories by Count via Webfilter Logs | 141**

Device Administration

Basic Settings | 144

Configure Basic Settings | 144

Cluster Management | 164

Configure Cluster (HA) Setup | 164

About the Cluster Configuration Page | 179

Edit Node Settings | 182

Add an HA Cluster Interface | 183

Edit an HA Cluster Interface | 185

Delete an HA Cluster Interface | 185

Add a Redundancy Group | 186

Edit a Redundancy Group | 188

Delete a Redundancy Group | 189

User & Roles | 190

About the Users Page | 190

Create a User | 192

Edit a User | 197

Delete a User | 198

About the Roles Page | 198

Create a Role | 202

Edit a Role | 204

Delete a User | 204

Multi Tenancy—Resource Profiles | 206

About the Resource Profiles Page | 206

Global Settings | 208

Add a Resource Profile | 209

Edit a Resource Profile | 213

Delete a Resource Profile | 213

Multi Tenancy—Interconnect Ports | 215

About the Interconnect Ports Page | 215

Add a LT Logical Interface | 217

Edit a LT Logical Interface | 224

Delete a Logical Interface | 224

Search for Text in an Interconnect Ports Table | 224

Multi Tenancy—Logical Systems | 226

About the Logical Systems Page | 226

Add a Logical System | 228

Edit a Logical System | 239

Delete a Logical System | 240

Search Text in Logical Systems Table | 240

Multi Tenancy—Tenants | 241

About the Tenants Page | 241

Add a Tenant | 243

Edit a Tenant | 251

Delete a Tenant | 251

Search Text in Tenants Table | 252

Certificates Management—Certificates | 253

About the Certificates page | 253

Create a Device Certificate | 255

 Create Device Certificate (Let's Encrypt) | 256

 Create Device Certificate (Local Self-Signed) | 257

 Create Device Certificate (SCEP) | 260

 Create Device Certificate (ACME) | 262

 Create Device Certificate (CMPv2) | 264

- Create Device Certificate (CSR) | 266
- Load Signed Device Certificate (Externally Generated) | 269

Add a Certificate Authority (CA) | 270

- Add CA Certificate | 270

Export a Device Certificate | 274

Edit a CA Certificate | 275

Delete a Certificate | 275

Search Text in the Certificates Table | 276

Re-Enroll a Device Certificate | 276

Load CA Certificate | 277

Reload CA Certificate | 279

Certificate Management—Certificate Authority Group | 281

About the Certificate Authority Group Page | 281

Import a Trusted CA Group | 282

Add a CA Group | 283

Edit a CA Group | 284

Delete a CA Group | 285

Search Text in the Certificate Authority Group Table | 285

License Management | 287

Manage Your Licenses | 287

- About License Management Page | 287
- Add License | 288
- Delete Installed Licenses | 289
- Update Installed Licenses | 289
- Update Trial Licenses | 289
- Display License Keys | 289
- Download License Keys | 290
- Software Feature Licenses | 290

Security Package Management | 291

About the Security Package Management Page | 291

Install or Upload IPS Signatures Package | 295

IPS Signatures Settings | 297

Install Application Signatures Package | 299

Application Signatures Settings | 299

Manage URL Categorization | 301

Check URL Recategorization Status | 302

Install URL Category Package | 302

URL Categories Settings | 303

ATP Management | 306

Enroll Your Device with Juniper ATP Cloud | 306

About the Diagnostics Page | 309

Operations | 312

Maintain Files | 312

 About Files Page | 312

 Clean Up Files | 312

 Download and Delete Files | 313

Maintain Reboot Schedule | 315

Maintain System Snapshots | 317

Software Management | 319

Upload Software Packages | 319

Install Software Packages | 320

Rollback Software Package Version | 321

Configuration Management | 323

Manage Upload Configuration Files | 323

Manage Configuration History | 324

Manage Rescue Configuration | 328

Alarm Management | 329

Monitor Chassis Alarm | 329

- About Chassis Alarm Page | 329
- Create Chassis Alarm Definition | 329
- Edit Chassis Alarm Definition | 334

Monitor System Alarm | 335

- About System Alarm Page | 335
- Create System Alarm Configuration | 335
- Edit System Alarm Configuration | 339

RPM | 340

Setup RPM | 340

View RPM | 349

Tools | 355

Troubleshoot Ping Host | 355

- About Ping Host Page | 355

Troubleshoot Ping MPLS | 359

- About Ping MPLS Page | 360

Troubleshoot Traceroute | 365

- About Traceroute Page | 365

Control Plane Packet Capture | 368

- About the Control Plane Packet Capture Page | 368

About the Data Plane Packet Capture Page | 375

Access CLI | 379

- About CLI Terminal Page | 379

View CLI Configuration | 381

- About CLI Viewer Page | 381

Edit CLI Configuration | 382

- About CLI Editor Page | 382

Point and Click CLI | 383

| About Point and Click CLI Page | 383

Reset Configuration | 390

Reset Configuration and Rerun Setup Wizard | 390

6

Network

Connectivity—Interfaces | 393

About the Interfaces Page | 393

Add a Logical Interface | 397

Edit an Interface | 404

Delete a Logical Interface | 405

Connectivity—VLAN | 406

About the VLAN Page | 406

Add a VLAN | 408

Edit a VLAN | 410

Delete a VLAN | 411

Assign an Interface to VLAN | 411

Connectivity—Link Aggregation | 413

About the Link Aggregation Page | 413

Link Aggregation Global Settings | 415

Add a Logical Interface to Link Aggregation | 416

Add a Link Aggregation | 417

Edit an Aggregated Interface | 419

Delete Link Aggregation | 420

Search for Text in the Link Aggregation Table | 420

Connectivity—Wireless LAN | 422

About the Settings Page | 422

Create an Access Point | 424

Edit an Access Point | 425

- Delete an Access Point | 426
- Create an Access Point Radio Setting | 426
- Edit an Access Point Radio Setting | 430
- Delete an Access Point Radio Settings | 430
- DHCP Client | 432**
- About the DHCP Client Page | 432
- Add DHCP Client Information | 433
- Delete DHCP Client Information | 435
- DHCP Server | 436**
- About the DHCP Server Page | 436
- Add a DHCP Pool | 438
- Edit a DHCP Pool | 442
- Delete a DHCP Pool | 443
- DHCP Groups Global Settings | 443
- Add a DHCP Group | 444
- Edit a DHCP Group | 444
- Delete a DHCP Group | 445
- Firewall Filters—IPv4 | 446**
- About the IPv4 Page | 446
- Add IPv4 Firewall Filters | 447
- Firewall Filters—IPv6 | 464**
- About the IPv6 Page | 464
- Add IPv6 Firewall Filters | 465
- Firewall Filters—Assign to Interfaces | 480**
- About the Assign to Interfaces Page | 480
- NAT Policies | 482**
- About the NAT Policies Page | 482

Create a Source NAT | 484

Edit a Source NAT | 490

Delete a Source NAT | 490

NAT Pools | 491

About the NAT Pools Page | 491

Global Options | 493

Create a Source NAT Pool | 494

Edit a Source NAT Pool | 498

Delete a Source NAT Pool | 499

Add a Destination NAT Pool | 499

Edit a Destination NAT Pool | 501

Delete a Destination NAT Pool | 501

Destination NAT | 502

About the Destination Page | 502

Add a Destination Rule Set | 504

Edit a Destination Rule Set | 507

Delete a Destination Rule Set | 507

Static NAT | 508

About the Static Page | 508

Add a Static Rule Set | 510

Edit a Static Rule Set | 514

Delete a Static Rule Set | 514

NAT Proxy ARP/ND | 516

About the Proxy ARP/ND Page | 516

Add a Proxy ARP | 517

Edit a Proxy ARP | 519

Delete a Proxy ARP | 519

Add a Proxy ND | 520

Edit a Proxy ND | 521

Delete a Proxy ND | 521

Static Routing | 523

About the Static Routing Page | 523

Add a Static Route | 524

Edit a Static Route | 526

Delete a Static Route | 526

RIP Routing | 527

About the RIP Page | 527

Add a RIP Instance | 529

Edit a RIP Instance | 531

Delete a RIP Instance | 531

Edit RIP Global Settings | 531

Delete RIP Global Settings | 535

OSPF Routing | 536

About the OSPF Page | 536

Add an OSPF | 538

Edit an OSPF | 547

Delete an OSPF | 547

BGP Routing | 549

About the BGP Page | 549

Add a BGP Group | 553

Edit a BGP Group | 558

Delete a BGP Group | 559

Edit Global Information | 559

Routing Instances | 565

About the Routing Instances Page | 565

Add a Routing Instance | 567

Edit a Routing Instance | 568

Delete a Routing Instance | 569

Routing—Policies | 570

About the Policies Page | 570

Global Options | 572

Add a Policy | 573

Clone a Policy | 585

Edit a Policy | 585

Delete a Policy | 585

Test a Policy | 586

Routing—Forwarding Mode | 587

About the Forwarding Mode Page | 587

CoS—Value Aliases | 589

About the Value Aliases Page | 589

Add a Code Point Alias | 590

Edit a Code Point Alias | 591

Delete a Code Point Alias | 592

CoS—Forwarding Classes | 593

About the Forwarding Classes Page | 593

Add a Forwarding Class | 594

Edit a Forwarding Class | 595

Delete a Forwarding Class | 595

CoS Classifiers | 597

About the Classifiers Page | 597

Add a Classifier | 599

Edit a Classifier | 600

Delete a Classifier | 601

CoS—Rewrite Rules | 602

About the Rewrite Rules Page | 602

Add a Rewrite Rule | 603

Edit a Rewrite Rule | 605

Delete a Rewrite Rule | 605

CoS—Schedulers | 607

About the Schedulers Page | 607

Add a Scheduler | 608

Edit a Scheduler | 610

Delete a Scheduler | 611

CoS—Scheduler Maps | 612

About the Scheduler Maps Page | 612

Add a Scheduler Map | 613

Edit a Scheduler Map | 614

Delete a Scheduler Map | 615

CoS—Drop Profile | 616

About the Drop Profile Page | 616

Add a Drop Profile | 617

Edit a Drop Profile | 619

Delete a Drop Profile | 619

CoS—Virtual Channel Groups | 620

About the Virtual Channel Groups Page | 620

Add a Virtual Channel | 621

Edit a Virtual Channel | 622

Delete a Virtual Channel | 623

CoS—Assign To Interface | 624

About the Assign To Interface Page | 624

Edit a Port | 626

Add a Logical Interface | 626

Edit a Logical Interface | 628

Delete a Logical Interface | 629

Application QoS | 630

About the Application QoS Page | 630

Add an Application QoS Profile | 633

Edit an Application QoS Profile | 635

Clone an Application QoS Profile | 635

Delete an Application QoS Profile | 636

Add a Rate Limiter Profile | 636

Edit a Rate Limiter Profile | 637

Clone a Rate Limiter Profile | 638

Delete a Rate Limiter Profile | 638

IPsec VPN | 640

About the IPsec VPN Page | 640

IPsec VPN Global Settings | 643

Create a Site-to-Site VPN | 647

Create a Remote Access VPN—Juniper Secure Connect | 664

Create a Remote Access VPN—NCP Exclusive Client | 687

Edit an IPsec VPN | 700

Delete an IPsec VPN | 701

Dynamic VPN | 702

About the Dynamic VPN Page | 702

Global Settings | 704

IPsec Template | 706

Add a Dynamic VPN | 707

Edit a Dynamic VPN | 708

Delete a Dynamic VPN | 709

Compliance | 710

About the Compliance Page | 710

Create Pre-Logon Compliance | 712

Edit Pre-Logon Compliance | 718

Delete Pre-Logon Compliance | 718

Security Policies and Objects

Security Policies | 721

About the Security Policies Page | 721

Global Options | 726

Add a Rule to a Security Policy | 729

Clone a Security Policy Rule | 746

Edit a Security Policy Rule | 747

Delete a Security Policy Rule | 747

Configure Captive Portal for Web Authentication and Firewall User Authentication | 748

Overview | 748

Workflow | 749

Step 1: Create a Logical Interface and Enable Web Authentication | 751

Step 2: Create an Access Profile | 757

Step 3: Configure Web Authentication Settings | 758

Step 4: Create Security Zones and Assign Interfaces to the Zones | 760

Step 5: Enable Web or Firewall User Authentication for Captive Portal in the Security Policy | 764

Step 6: Verify the Web Authentication and User Authentication Configuration | 771

Metadata Streaming Policy | 775

About the Metadata Streaming Policy Page | 775

Create a Metadata Streaming Policy | 777

Edit a Metadata Streaming Policy | 778

Delete a Metadata Streaming Policy | 779

Zones/Screens | 780

About the Zones/Screens Page | 780

Add a Zone | 782

Edit a Zone | 785

Delete a Zone | 785

Add a Screen | 785

Edit a Screen | 796

Delete a Screen | 797

Zone Addresses | 798

About the Zone Addresses Page | 798

Add Zone Addresses | 800

Clone Zone Addresses | 802

Edit Zone Addresses | 803

Delete Zone Addresses | 803

Search Text in a Zone Addresses Table | 803

Global Addresses | 805

About the Global Addresses Page | 805

Add an Address Book | 806

Edit an Address Book | 810

Delete an Address Book | 810

Services | 811

About the Services Page | 811

Add a Custom Application | 813

Edit a Custom Application | 816

Delete Custom Application | 816

Add an Application Group | 817

Edit an Application Group | 818

Delete an Application Group | 819

Dynamic Applications | 820

About the Dynamic Applications Page | 820

Global Settings | 823

Add Application Signatures | 826

Clone Application Signatures | 831

Add Application Signatures Group | 832

Edit Application Signatures | 833

Delete Application Signatures | 833

Search Text in an Application Signatures Table | 834

Application Tracking | 835

About the Application Tracking Page | 835

Schedules | 837

About the Schedules Page | 837

Add a Schedule | 839

Clone a Schedule | 841

Edit a Schedule | 841

Delete a Schedule | 842

Search Text in Schedules Table | 842

Proxy Profiles | 843

About the Proxy Profiles Page | 843

Add a Proxy Profile | 845

Edit a Proxy Profile | 846

Delete a Proxy Profile | 846

Security Services

Content Security Default Configuration | 849

About the Default Configuration Page | 849

Edit a Default Configuration | 851

Delete a Default Configuration | 851

Content Security Antivirus Profiles | 853

About the Antivirus Profiles Page | 853

Add an Antivirus Profile | 855

Clone an Antivirus Profile | 861

Edit an Antivirus Profile | 861

Delete an Antivirus Profile | 862

Prevent Virus Attacks by Using J-Web Content Security Antivirus | 862

Content Security Antivirus Overview | 863

Benefits of Content Security Antivirus | 864

Antivirus Workflow | 865

Step 1: Update Default Configuration for Antivirus | 867

Step 2: Configure Antivirus Custom Object | 869

Step 2a: Configure a URL Pattern List That You Want to Bypass | 869

Step 2b: Categorize the URLs That You Want to Allow | 871

Step 3: Create Antivirus Profile | 873

Step 4: Apply the Antivirus Profile to a Content Security Policy | 875

Step 5: Assign the Content Security Policy to a Security Firewall Policy | 876

Step 6: Verify That Content Security Antivirus Is Working | 879

What's Next? | 881

Sample Configuration Output | 881

Content Security Web Filtering Profiles | 884

About the Web Filtering Profiles Page | 884

Add a Web Filtering Profile | 887

Clone a Web Filtering Profile | 893

Edit a Web Filtering Profile | 894

Delete a Web Filtering Profile | 895

Allow or Block Websites by Using J-Web Integrated Content Security Web Filtering | 895

Content Security URL Filtering Overview | 896

Benefits of Content Security Web Filtering | 897

Web Filtering Workflow | 897

Step 1: List URLs That You Want to Allow or Block | 899

Step 2: Categorize the URLs That You Want to Allow or Block | 901

Step 3: Add a Web Filtering Profile | 903

Step 4: Reference a Web Filtering Profile in a Content Security Policy | 904

Step 5: Assign a Content Security Policy to a Security Policy | 907

Step 6: Verify That the URLs Are Allowed or Blocked from the Server | 910

What's Next | 911

Sample Configuration Output | 911

Content Security Antispam Profiles | 914

About the Antispam Profiles Page | 914

Add an Antispam Profile | 916

Clone an Antispam Profile | 917

Edit an Antispam Profile | 918

Delete an Antispam Profile | 919

Content Security Content Filtering Profiles | 920

About the Content Filtering Profiles Page | 920

Add a Content Filtering Profile | 922

Clone a Content Filtering Profile | 926

Edit a Content Filtering Profile | 927

Delete a Content Filtering Profile | 928

Content Security Custom Objects | 929

About the Custom Objects Page | 929

Add a MIME Pattern List | 932

Add a File Extension List | 934

Add a Protocol Command List | 934

Add a URL Pattern List | 935

Add a URL Category List | 936

Add a Custom Message List | 938

Clone Custom Objects | 939

Edit Custom Objects | 939

Delete Custom Objects | 940

Content Security Policies | 942

About the Content Security Policies Page | 942

Create a Content Security Policy | 944

Clone a Content Security Policy | 947

Edit a Content Security Policy | 948

Delete a Content Security Policy | 948

IPS Policies | 950

About the IPS Policies Page | 950

Import IPS Predefined Policies | 952

Add an IPS Policy | 953

Clone an IPS Policy | 953

Edit an IPS Policy | 954

Delete an IPS Policy | 955

Add Rules to an IPS Policy | 955

Edit an IPS Policy Rule | 965

Delete an IPS Policy Rule | 966

IPS Signatures | 967

About the IPS Signatures Page | 967

Import Snort Rules | 972

Create a Custom IPS Signature | 973

Create IPS Signature Static Groups | 989

Create IPS Signature Dynamic Group | 992

Clone an IPS Signature | 997

Edit an IPS Signature | 998

Delete an IPS Signature | 999

IPS Sensor | 1001

About the Sensor Page | 1001

ALG | 1009

About the ALG Page | 1009

Metadata Streaming Profile | 1020

About the Metadata Streaming Profile Page | 1020

Configure DNS Filter | 1022

Create a Metadata Streaming Profile | 1023

Edit a Metadata Streaming Profile | 1026

Delete a Metadata Streaming Profile | 1026

ATP Anti-malware | 1027

About the Anti-malware Page | 1027

Create an Anti-malware Profile | 1029

Edit an Anti-malware Profile | 1035

Delete an Anti-malware Profile | 1036

ATP SecIntel Profiles | 1037

About the SecIntel Profiles Page | 1037

Configure DNS Sinkhole | 1040

Create a Command and Control Profile | 1041

Edit a Command and Control Profile | 1044

Delete a Command and Control Profile | 1044

Create a DNS Profile | 1045

Edit a DNS Profile | 1046

Delete a DNS Profile | 1047

Create an Infected Hosts Profile | 1048

Edit an Infected Hosts Profile | 1050

Delete an Infected Hosts Profile | 1051

ATP SecIntel Profile Groups | 1052

About the SecIntel Profile Groups Page | 1052

Create a SecIntel Profile Group | 1054

Edit a SecIntel Profile Group | 1056

Delete a SecIntel Profile Group | 1056

SSL Initiation Profiles | 1057

About the SSL Initiation Profile Page | 1057

Add an SSL Initiation Profile | 1059

Edit an SSL Initiation Profile | 1062

Delete SSL Initiation Profile | 1063

SSL Proxy Profiles | 1064

About the SSL Proxy Page | 1064

Add an SSL Proxy Profile | 1067

Clone an SSL Proxy Profile | 1073

Edit an SSL Proxy Profile | 1074

Delete a SSL Proxy Profile | 1074

Firewall Authentication—Access Profile | 1076

About the Access Profile Page | 1076

Add an Access Profile | 1078

Edit an Access Profile | 1085

Delete an Access Profile | 1086

Firewall Authentication—Address Pools | 1087

About the Address Pools Page | 1087

Add an Address Pool | 1089

Edit an Address Pool | 1092

Delete Address Pool | 1093

Search for Text in an Address Pools Table | 1093

Firewall Authentication Settings | 1095

About the Authentication Settings Page | 1095

Firewall Authentication—UAC Settings | 1098

About the UAC Settings Page | 1098

Firewall Authentication—Active Directory | 1102

About the Active Directory Page | 1102

Firewall Authentication—Local Authentication | 1108

About the Local Authentication Page | 1108

Add a Local Authentication Entry | 1109

Delete a Local Authentication Entry | 1110

Firewall Authentication—Authentication Priority | 1111

About the Authentication Priority Page | 1111

Firewall Authentication—JIMS | 1113

About the Juniper Identity Management Service Page | 1113

Add a Juniper Identity Management Service Profile | **1114**

Edit a Juniper Identity Management Service Profile | **1118**

Delete a Juniper Identity Management Service Profile | **1119**

ICAP Redirect | 1120

About the ICAP Redirect Profile Page | **1120**

Add an ICAP Redirect Profile | **1122**

Edit an ICAP Redirect Profile | **1125**

Delete ICAP Redirect Profile | **1125**

About This Guide

Use this guide to understand the Junos Web Device Manager, its capabilities, and features.

1

PART

Juniper Web Device Manager

[Getting Started | 2](#)

Getting Started

IN THIS CHAPTER

- [Juniper Web Device Manager Overview | 2](#)
- [Access the J-Web User Interface | 3](#)
- [The J-Web Setup Wizard | 8](#)
- [Explore J-Web | 39](#)

Juniper Web Device Manager Overview

IN THIS SECTION

- [What is J-Web? | 2](#)
- [Benefits of J-Web | 3](#)

What is J-Web?

Juniper Networks SRX Series Firewalls are shipped with the Juniper Networks Junos operating system (Junos OS) preinstalled.

Junos OS has the following primary user interfaces:

- Juniper Web Device Manager (J-Web) GUI
- Junos OS CLI

The J-Web interface allows you to monitor, configure, troubleshoot, and manage your device by means of a Web browser enabled with HTTP over Secure Sockets Layer (HTTPS) by default.

Benefits of J-Web

- Provides a simple user interface that enables new users to quickly become proficient.
- Enables effective threat management while producing detailed data access and user activity reports. An action-oriented design enables the network administrator to detect threats across the network as they occur, quickly block the traffic going to or coming from a specific region, and apply immediate remedial action with a single click.
- Enables administrators to assess the effectiveness of each firewall rule and quickly identify the unused rules, which results in better management of the firewall environment.

RELATED DOCUMENTATION

[Access the J-Web User Interface | 3](#)

[Explore J-Web | 39](#)

Access the J-Web User Interface

IN THIS SECTION

- [Prerequisites for Using J-Web | 3](#)
- [Log in to J-Web | 4](#)

Prerequisites for Using J-Web

To access the J-Web interface for all SRX Series Firewalls, your management device requires the following software:

- Supported browsers—Mozilla Firefox and Google Chrome.

NOTE: By default, you establish a J-Web session through an HTTPS-enabled Web browser. Microsoft ended Internet Explorer support in June 2022. Therefore, starting with Junos OS Release 22.4R1 or later, J-Web UI is not supported in Internet Explorer.

- Language support— English-version browsers.

Log in to J-Web

NOTE: This document assumes that you are accessing the device to launch J-Web for the first time using a factory default configuration. If your SRX Series Firewall is already configured with a management IP address, you simply point your browser to the device's management address to access J-Web.

The factory default settings vary between SRX Series Firewalls. In addition, some SRX Series Firewalls have interface while others use a revenue (network interface) port for Ethernet based management. When running a factory default configuration SRX 300 and 500 Series devices typically provide DHCP services on specific network interface ports that are enabled for host management access.

On SRX Series Firewalls with a dedicated management interface, DHCP services may or may not be present in the factory default. Some devices provide DHCP server functions on the dedicated management interface (fxp0). When using a device that does not offer DHCP services, for example an SRX5400, you must ensure the management device has a compatible IP address. This address can be manually assigned or be allocated by an external DHCP server on the management network.

[Table 1 on page 4](#) provides the factory defaults relating to J-Web access for SRX Series Firewalls. If your SRX Series Firewall is not listed, refer to the corresponding hardware guide for details on the factory defaults.

Table 1: SRX Series Firewall Factory Defaults Relating to J-Web Access

| SRX Series Firewall | Management Interface | DHCP Server Ports | DHCP Subnet | J-Web Server IP |
|---------------------|---------------------------|----------------------------|----------------|-----------------|
| SRX300, SRX320 | ge-0/0/1 through ge-0/0/6 | ge-0/0/1 through ge-0/0/6 | 192.168.1.0/24 | 192.168.1.1 |
| SRX340, SRX345 | MGMT/fxp0 | fxp0 | 192.168.1.0/24 | 192.168.1.1 |
| | | ge-0/0/1 through ge-0/0/14 | 192.168.2.0/24 | 192.168.2.1 |
| SRX380 | MGMT/fxp0 | fxp0 | 192.168.1.0/24 | 192.168.1.1 |
| | | ge-0/0/1 through ge-0/0/18 | 192.168.2.0/24 | 192.168.2.1 |

Table 1: SRX Series Firewall Factory Defaults Relating to J-Web Access (Continued)

| SRX Series Firewall | Management Interface | DHCP Server Ports | DHCP Subnet | J-Web Server IP |
|---------------------------|---------------------------|---------------------------|--|---|
| SRX550 HM | ge-0/0/1 through ge-0/0/5 | ge-0/0/1 through ge-0/0/5 | 192.168.1.0/24 through 192.168.5.0/24 | 192.168.1.1 through 192.168.5.1 |
| SRX1500 | MGMT/fxp0 | ge-0/0/1 | 192.168.2.0/24 | 192.168.1.1 192.168.2.1, 192.168.3.1, or 192.168.4.1 |
| SRX1600 | MGMT/fxp0 | ge-0/0/1 | 192.168.2.0/24 | 192.168.1.1 or 192.168.2.1 |
| SRX2300 | MGMT/fxp0 | mge-0/0/1 | 192.168.2.0/24 | 192.168.1.1 or 192.168.2.1 |
| SRX4100, SRX4200 | MGMT/fxp0 | NA | NA | 192.168.1.1 |
| SRX4600 | MGMT/fxp0 | xe-1/1/1 | NA (no DHCP address pool in the default configuration) | 192.168.1.1 |
| SRX5400, SRX5600, SRX5800 | MGMT/fxp0 | NA | NA | 192.168.1.1 |
| vSRX Virtual Firewall | fxp0 | NA | NA | NA |

To log into the J-Web interface on a new device:

1. Connect the appropriate Ethernet network port on your device to the Ethernet port on the management device (laptop or PC), using an RJ-45 cable. See [Table 1 on page 4](#).
2. If you are using an SRX Series Firewall that provides DHCP services for the management device, confirm that the management device successfully acquires an IP address from the SRX Series Firewall. When using an SRX Series Firewall that does not provide DHCP services for the

management device, you must manually configure the management device with a compatible IP address. See [Table 1 on page 4](#) .

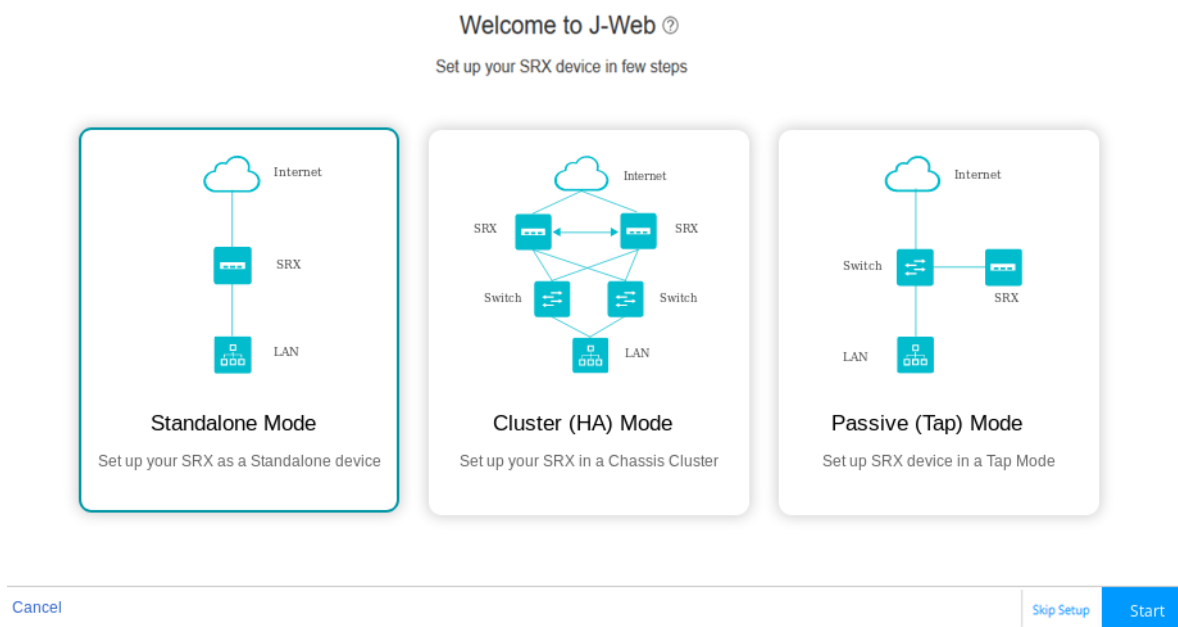
3. Open a browser and enter **https:// <IP address>** in the address bar.

Where, <IP address> is the IP address of the SRX Series Firewall.

NOTE: In a factory default configuration, a self-signed certificate is used to support the HTTPS connection. You can safely accept the security exception to perform initial configuration.

As the device is running a factory default configuration, the J-Web Setup Wizard screen opens. See [Figure 1 on page 6](#) .

Figure 1: J-Web Setup Wizard Page



Two examples are given to better illustrate the use of the information in [Table 1 on page 4](#) :

- a. You have an SRX380 device:
 - i. You connect your management PC, which is configured for DHCP address assignment, to the **fxp0** port, or to port **ge-0/0/1** through **ge-0/0/18**.
 - ii. If connected to the fxp0 port, you access J-Web at **https://192.168.1.1**.
 - iii. If connected to ge-0/0/1 through ge-0/0/18, you access J-Web at **https://192.168.2.1**.

- b. You have an SRX5400 device:
 - i. You connect your management PC, which is statically configured with an IP address from 192.168.1.0/24 subnet, to the **fxp0** port.

NOTE: The static IP address assignment cannot use 192.168.1.1 for fxp0 on the management subnet as the SRX Series Firewall uses this IP address.

- ii. You access J-Web at **https://192.168.1.1**.

After a successful user login, J-Web opens the **Basic settings** page.

4. Optional. If you do not want to perform the initial configuration, then:

- a. Click **Skip Setup**.

The J-Web Device Password screen appears. See [Figure 2 on page 7](#).

Figure 2: Device Password

Device Password

With super user permissions for your root account, you can change any of the system settings. Please set your root password before you commit any configuration changes.

Username root

Password* ? Show

Cancel OK

- b. Enter the root password.
 - c. Click **OK**.

The password is committed to the device and the J-Web login page appears.

- d. Enter the username and password again and click **Log In**.

The J-Web application window appears.

NOTE: You can choose **Device Administration > Reset Configuration** through the J-Web menu to reset and reconfigure the SRX Series Firewall.

Congratulations! Now that you have access to the J-Web interface, you are ready to use J-Web to configure, manage, and monitor your SRX device.

- Get a quick overview of the J-Web user interface: ["Explore J-Web" on page 39](#)
- Use the setup wizard for initial configuration: ["The J-Web Setup Wizard" on page 8](#)
- Access the device dashboard: ["Dashboard Overview" on page 55](#)
- Monitor device traffic: ["Monitor Traffic Map" on page 105](#)
- Configure your device: ["Configure Basic Settings" on page 144](#)
- Watch a Learning Bytes video showing J-Web usage on a vSRX Virtual Firewall: [SRX J-Web Access](#)

The J-Web Setup Wizard

IN THIS SECTION

- [Configure SRX Series Firewalls Using the J-Web Setup Wizard | 8](#)
- [Example: J-Web Wizard for Standalone Mode | 10](#)
- [J-Web Setup Wizard Parameters | 22](#)

Configure SRX Series Firewalls Using the J-Web Setup Wizard

Using the Setup wizard, you can perform step-by-step configuration of a services gateway that can securely pass traffic.

For information on how to start and access the J-Web user interface, see ["Access the J-Web User Interface" on page 3](#).

You can choose one of the following setup modes to configure the services gateway:

- Standalone mode—Configure your SRX Series Firewall to operate in a standalone mode. In this mode, you can configure basic settings such as device credentials, time, management interface, zones and interfaces, and DNS servers and default gateways.
- Cluster (HA) mode—Configure your SRX Series Firewall to operate in a cluster (HA) mode. In the cluster mode, a pair of devices are connected together and configured to operate like a single node, providing device, interface, and service level redundancy.

NOTE: You cannot configure Standalone or Passive mode when your device is in the HA mode.

- Passive (Tap) mode—Configure your SRX Series Firewall to operate in a TAP mode. TAP mode allows you to passively monitor traffic flows across a network. If IPS is enabled, then the TAP mode inspects the incoming and outgoing traffic to detect the number of threats.

NOTE:

- SRX5000 line of devices, SRX4600, and vSRX Virtual Firewall devices do not support the passive mode configuration.
- Starting in Junos OS Release 23.4R1, J-Web supports SRX1600 and SRX2300 Firewalls.

To help guide you through the process, the wizard:

- Determines which configuration tasks to present to you based on your selections.
- Flags any missing required configuration when you attempt to leave a page.

To configure SRX Series Firewalls using the J-Web Setup wizard:

1. Select the configuration mode that you want to setup and click **Start**.

The Setup Wizard page appears.

2. For standalone and passive (Tap) modes, complete the configuration according to the guidelines provided in [Table 3 on page 22](#).

If you select Cluster (HA) Mode, for the configuration information see "[Configure Cluster \(HA\) Setup](#)" on page 164.

NOTE: The root password is mandatory in the setup wizard. All other options are optional. In the passive mode, configuration of the management interface, Tap interface, and services are mandatory.

3. Review the configuration details. If you want to change the configuration, click **Edit Configuration**, else click **Finish**.

Wait till the configuration is committed. A successful message is displayed once the entire configuration is committed to the device.

NOTE:

- If the commit fails, J-Web displays you the error message received from CLI and you remain on the wizard's last page. Check over your configuration and make changes as necessary so that the commit succeeds.
- For SRX300 line of devices and SRX550M devices in passive mode, an additional message is displayed about the device reboot if you have enabled Juniper ATP Cloud or Security Intelligence services. For other SRX Series Firewalls, the device will not reboot.

4. Read if any instructions are available and then click **Open J-Web Login Page**.

The J-Web Login page appears.

5. Enter the root username and password and click **Log In**.

Launch Pad screen appears until the J-Web UI is loaded. See ["J-Web: A First Look" on page 40](#) .

Example: J-Web Wizard for Standalone Mode

In this section, we'll show you a typical J-Web setup wizard workflow for standalone mode operation. The J-Web interface is updated and modified over time. The below example is representative of the typical workflow. This specific example is based on the Junos 21.3R1 release.

[Table 2 on page 10](#) provide details on the configuration parameters used for initial setup.

Table 2: Standalone Setup Wizard Parameters

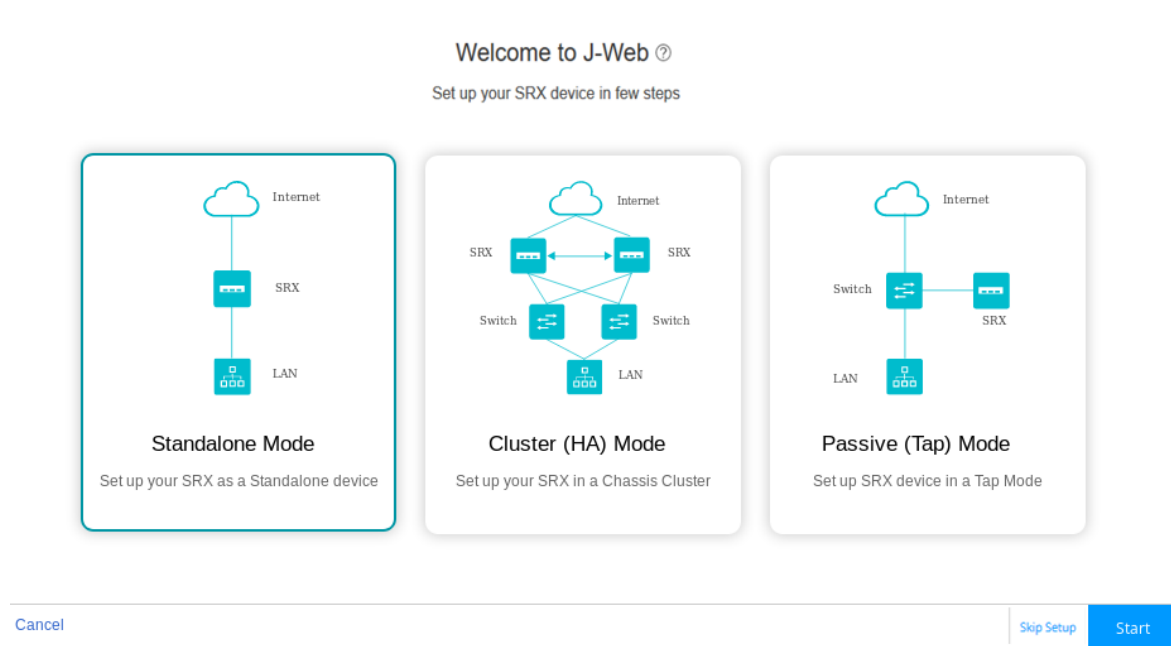
| Configuration Parameter | Example Value |
|-------------------------|-------------------------------------|
| Root Password | <i>"Sample_psswd_for_doc-only!"</i> |

Table 2: Standalone Setup Wizard Parameters (Continued)

| Configuration Parameter | Example Value |
|--|---|
| Hostname | SRX-300 |
| Management interface | ge-0/0/1 |
| Management IP and CIDR | 10.102.70.79/24 |
| Access Protocols | HTTPS, SSH, Ping |
| Static route for management | 10.0.0.0/8, next hop 10.102.70.254 |
| NTP and DNS | <ul style="list-style-type: none"> • NTP: north-america.pool.ntp.org • DNS: 8.8.8.8 and 8.8.4.4 • Time zone: PST/Los Angeles |
| Remote access | SSH with root login allowed |
| Non root user (Admin/super user account) | user "lab", password " <i>Sample_psswd_for_doc-only!</i> " |
| Security Policy | Default |

Refer to ["Access the J-Web User Interface"](#) on page 3 for information on how to access the J-Web interface. This example is based on an SRX300. Based on the information in [Table 1 on page 4](#), the management device is set for DHCP is and is attached to the ge-0/0/1 interface. When running a factory default configuration, the ge-0/0/1 interface is configured as a DHCP server and assigns an address to the PC from the 192.168.1.0/24 subnet. To access J-Web in this scenario, you point the browser to https://192.168.1.1.

1. We begin at the J-Web setup wizard screen. You click on the option for **Standalone Mode** and then on the **Start button**.

Figure 3: J-Web Setup Wizard Modes

2. Configure the device name, root user, and non-root (administrator) user login information on the Device Credentials page.

NOTE: Enable SSH for root user.

Figure 4: J-Web Setup Wizard Device Credentials

Setup Wizard

Device Credentials Time Management Interface Zones & Interfaces DNS Servers & Default Gateways

System Identity

Device name (?)

Root Account

It is recommended to use the Admin account to manage SRX devices.

Username

Password* (?) [Show](#)

SSH for root user (?)

Admin Account

Username

Password (?) [Show](#)

[Cancel](#) [Next](#)

3. Click **Next**.

The **Time** page opens.

4. Configure the timezone, time source, and in the case of NTP, the desired server(s).

Figure 5: J-Web Setup Wizard Time Servers

Setup Wizard

Device Credentials **Time** Management Interface Zones & Interfaces DNS Servers & Default Gateways

Time

Time zone: America/Los_Angeles

Time source (?): **NTP Server** Computer Time Manual

NTP servers* (?):

| 6 Available | 1 Selected |
|--|--|
| <input type="checkbox"/> NTP Servers | <input type="checkbox"/> NTP Servers |
| <input type="checkbox"/> africa.pool.ntp.org | <input checked="" type="checkbox"/> north-america.pool.ntp.org |
| <input type="checkbox"/> antarctica.pool.ntp.org | |
| <input type="checkbox"/> asia.pool.ntp.org | |
| <input type="checkbox"/> europe.pool.ntp.org | |
| <input type="checkbox"/> oceania.pool.ntp.org | |

Cancel Back Next

5. Click **Next**.

The **Management Interface** page opens.

6. Again, this setup example is based on a SRX 300 series device. This SRX Series Firewall does not have a dedicated management interface. In many cases, their role in branch offices results in their being managed remotely through the WAN interface (ge-0/0/0). On larger SRX Series Firewalls, a dedicated management interface (fxp0) is provided for attachment to an out-of-band (OOB) management network. In this example, you configure the ge-0/0/1 interface as a dedicated OOB management interface.

Figure 6: J-Web Setup Wizard Management Interface

Setup Wizard

Device Credentials Time **Management Interface** Zones & Interfaces DNS Servers & Default Gateways

Management Interface

Management interface (?)

IPv4 IPv6 Access Protocols

Management address (?) /
The updated address is required to access j-Web after the setup is complete.
Note this address or [email to self](#)

Management subnet mask (?)

Static route (?) /

Static route subnet mask (?)

Next-hop gateway (?)

[Cancel](#) [Back](#) [Next](#)

Before continuing, you click on the **Access Protocols** tab to confirm that HTTPS, SSH, and Ping (ICMP echo) are permitted on the management interface.

Figure 7: J-Web Setup Wizard Access Protocols

Setup Wizard

Device Credentials Time **Management Interface** Zones & Interfaces DNS Servers & Default Gateways

Management Interface

Management interface [?](#) [v](#)

IPv4 IPv6 **Access Protocols**

| | |
|---------------------------|-------------------------------------|
| HTTPS ? | <input checked="" type="checkbox"/> |
| SSH ? | <input checked="" type="checkbox"/> |
| Ping ? | <input checked="" type="checkbox"/> |
| DHCP ? | <input type="checkbox"/> |
| NETCONF ? | <input type="checkbox"/> |

[Cancel](#) [Back](#) [Next](#)

7. Click **Next**.

The **Zones & Interfaces** page opens.

8. In this example you maintain the factory default security policy. Recall, you can always use J-Web to later modify all aspects of the configuration, to include security, after you complete the initial setup.

Figure 8: J-Web Setup Wizard Security Zones

Setup Wizard

Device Credentials Time Management Interface **Zones & Interfaces** DNS Servers & Default Gateways

Trust Zone Interfaces

[Zone Level Settings](#) | + | ✎ | 🗑️ | 🔍

| <input type="checkbox"/> | Interfaces | Description | IP Address | VLAN | System Services | Protocols |
|--------------------------|------------|-------------|----------------|------------|-----------------|-----------|
| <input type="checkbox"/> | irb.0 | — | 192.168.1.1/24 | vlan-trust | — | — |

1 items

Untrust Zone Interfaces

[Zone Level Settings](#) | + | ✎ | 🗑️ | 🔍

| <input type="checkbox"/> | Interfaces | Description | IP Address | Address Mode | System Services | Protocols |
|----------------------------|------------|-------------|------------|--------------|---|-----------|
| <input type="checkbox"/> ▶ | ge-0/0/0.0 | — | — | DHCP client | dhcp + 2 | — |
| <input type="checkbox"/> ▶ | ge-0/0/7.0 | — | — | DHCP client | dhcp + 1 | — |

2 items

[Cancel](#)

[Back](#)
[Next](#)

9. Click **Next**.

The **DNS Servers & Default Gateways** page opens.

10. Configure a public DNS server IP and leave the default gateway fields blank. If desired, you can add default routes to access other networks that should be reachable over the management interface.

Figure 9: J-Web Setup Wizard DNS and Default Gateways

Setup Wizard

Device Credentials Time Management Interface Zones & Interfaces **DNS Servers & Default Gateways**

DNS Servers

DNS server 1 ⓘ

DNS server 2 ⓘ

Default Gateway

Default gateway (IPv4) ⓘ

Default gateway (IPv6) ⓘ

[Cancel](#) [Back](#) [Next](#)

11. Click Next.

The **Setup Wizard** opens. This page summarizes your configuration. If desired, you use the **Edit Configuration** option to make changes.

Figure 10: J-Web Setup Wizard Summary

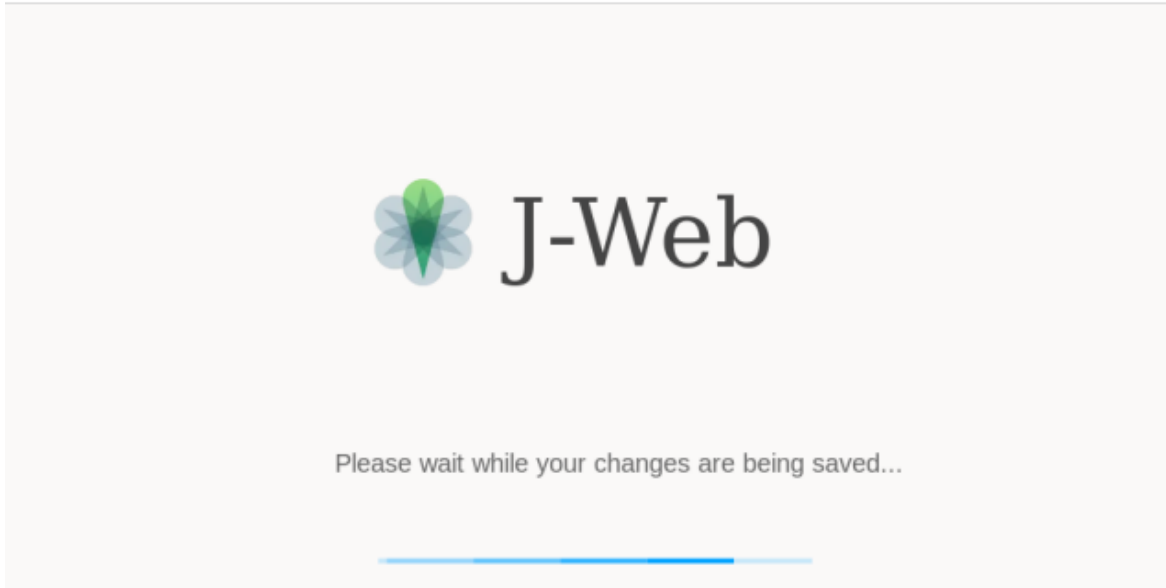
Setup Wizard

| | | |
|---|----------------------------|---|
| Device Credentials | | Edit Configuration |
| Device name | SRX-300 | |
| SSH for root user | Enabled | |
| Time | | Edit Configuration |
| NTP servers | north-america.pool.ntp.org | |
| Management Interface | | Edit Configuration |
| Management interface | ge-0/0/1 | |
| Management address | 10.102.70.79/24 | |
| Access protocols | HTTPS, SSH, Ping | |
| Zones & Interfaces | | Edit Configuration |
| Trust | irb.0 | |
| Untrust | ge-0/0/0.0, ge-0/0/7.0 | |
| DNS Servers & Default Gateways | | Edit Configuration |
| DNS servers | 8.8.8.8, 8.8.4.4 | |
| Cancel | | Back Finish |

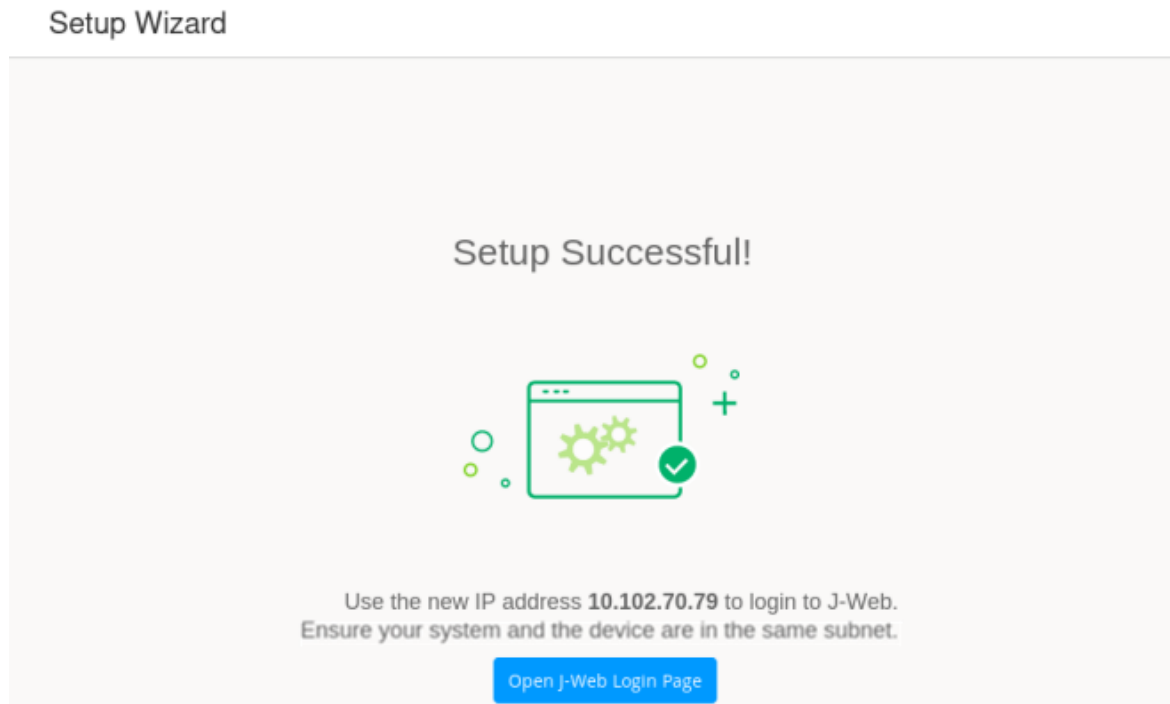
- When satisfied with the configuration, click on **Finish**. The Setup Wizard displays a status page to indicate the initial configuration is being pushed to the SRX Series Firewalls.

Figure 11: J-Web Setup Wizard Configuration Push

Setup Wizard



In a few moments, the **Setup Successful** page is displayed. Congratulations! Your SRX Series Firewall is remotely accessible and is ready for ongoing management using the J-Web interface.

Figure 12: J-Web Setup Wizard Successful

NOTE: Recall that in this SRX-300 based example the management device is directly connected to the SRX on the ge-0/0/1 port. You performed initial configuration using a 192.168.1.0/24 address that was assigned by the SRX Series Firewall using DHCP. Using the setup wizard, you configured the ge-0/0/1 interface as a dedicated management interface and assigned a static IP address of 10.102.70.89/24. As a result, the ge-0/0/1 interface no longer functions as a DHCP server.

Once the new configuration is activated, you must ensure the management device is configured with a compatible IP address if it remains directly connected to the ge-0/0/1 interface. You log in back into J-Web using <https://10.102.70.89>.

Congratulations! You have completed initial setup using J-Web. Keep going by visiting the below links:

- Get a quick overview of the J-Web user interface: ["Explore J-Web" on page 39](#)
- Access the device dashboard: ["Dashboard Overview" on page 55](#)
- Monitor device traffic: ["Monitor Traffic Map" on page 105](#)
- Configure your device: ["Configure Basic Settings" on page 144](#)
- Use the Getting Started panel: [Security J-Web Getting Started](#)

J-Web Setup Wizard Parameters

This section serves as a reference for the mode specific parameters that you can configure using the J-Web Setup Wizard. [Table 3 on page 22](#) provide details of the parameters that can be configured in the standalone and passive (Tap) modes. For details on parameters supported in cluster (HA) mode, see "[Configure Cluster \(HA\) Setup](#)" on page 164 .

Table 3: Setup Wizard Configuration

| Field | Action |
|---------------------------|--|
| Device Credentials | |
| System Identity | |
| Device name | <p>Enter a hostname.</p> <p>You can use alphanumeric characters, special characters such as the underscore (_), the hyphen (-), or the period (.); the maximum length is 255 characters.</p> |
| Root Account | |
| Username | <p>Displays the root user.</p> <p>NOTE: We recommend that you do not use root user account as a best practice to manage your devices.</p> |
| Password | <p>Enter a password.</p> <p>You can use alphanumeric characters and special characters; the minimum length is six characters.</p> |
| SSH for root user | <p>Enable this option to allow the root login (to the device) using SSH.</p> |
| Admin Account | |
| Username | <p>Enter the admin username to manage the device.</p> |
| Password | <p>Enter the admin password.</p> |

Table 3: Setup Wizard Configuration (Continued)

| Field | Action |
|--|---|
| Time Configuration | |
| Time | |
| Time zone | Select a time zone from the list. |
| Time source | <p>Select either NTP server, computer time, or Manual to configure the system time:</p> <ul style="list-style-type: none"> • NTP Server > NTP servers—Select the NTP server in the Available column and move to the selected column using the right arrow. Once the system is connected to the network, the system time is synced with the NTP server time. <p>In addition, to add a new NTP server, click + and enter a hostname or IP address of the NTP server and click OK.</p> <p>NOTE: If you want to add more NTP servers, go to Device Administration > Basic Settings > Date & Time Details through the J-Web menu.</p> <ul style="list-style-type: none"> • Computer Time > Computer time—Device automatically synchronizes with your computer time only during the setup. • Manual > Date and time—Select the date and time (in MM-DD-YYYY and HH:MM:SS 24-hour format) to configure the system time manually. |
| Management Interface Configuration | |
| <p>Management Interface</p> <p>NOTE: If you change the management IP address and click Next, a warning message appears on the Management Interface page that you need to use the new management IP address to log in to J-Web because you may lose the connectivity to J-Web.</p> | |

Table 3: Setup Wizard Configuration (Continued)

| Field | Action |
|---|---|
| Management interface | <p>Select an interface from the list.</p> <p>If fxp0 port is your device's management port, then the fxp0 port is displayed. You can change it as required or you can select None and proceed to the next page.</p> <p>NOTE:</p> <ul style="list-style-type: none"> You can choose the revenue port as management port if your device does not support the fxp0 port. Revenue ports are all ports except fxp0 and em0. If you are in the Standalone mode, you can choose None for the management interface and click Next to proceed to the next screen. If you are in the Passive (Tap) mode, it is mandatory to configure a management port. J-Web needs a management port for viewing generated report. |
| <p>IPv4</p> <p>NOTE: Click email to self to get the newly configured IPv4 or IPv6 address to your inbox. This is useful if you lose connectivity when you change the management IP address to another network.</p> | |
| Management address | <p>Enter a valid IPv4 address for the management interface.</p> <p>NOTE: If fxp0 port is your device's management port, then the fxp0 port's default IP address is displayed. You can change it if required.</p> |
| Management subnet mask | <p>Enter a subnet mask for the IPv4 address.</p> <p>If you have changed the management address, use the new IP address to access J-Web.</p> |
| Static route | <p>Enter an IPv4 address for the static route to route to the other network devices.</p> |
| Static route subnet mask | <p>Enter a subnet mask for the static route IPv4 address.</p> |

Table 3: Setup Wizard Configuration (Continued)

| Field | Action |
|--|--|
| Next hop gateway | Enter a valid IPv4 address for the next hop. |
| IPv6 | |
| Management access | Enter a valid IPv6 address for the management interface. |
| Management subnet prefix | Enter a subnet prefix length for the IPv6 address. |
| Static route | Enter an IPv6 address for the static route if required to reach the device through the management interface. |
| Static route subnet prefix | Enter a subnet prefix length for the static route IPv6 address. |
| Next hop gateway | Enter a valid IPv6 address for the next hop. |
| Access Protocols | |
| NOTE: This option is available for all the ports except fxp0. | |
| HTTPS | This option is enabled by default. |
| SSH | This option is enabled by default. |
| Ping | Enable this option for ping service. |
| DHCP | Enable this option for DHCP service. |
| NETCONF | Enable this option for NETCONF service. |
| Zones & Interfaces | |

Table 3: Setup Wizard Configuration (Continued)

| Field | Action |
|-------|--------|
|-------|--------|

Security Policy

NOTE: This option is available only for the Standalone mode. For the Passive (Tap) mode, this option is available under Tap Settings.

| | |
|-------------|--|
| From Zone | Name of the source zone. In the standalone mode, permits all traffic from the trust zone. |
| To Zone | Name of the destination zone. In standalone mode, permits all traffic from the trust zone to the untrust zone. |
| Source | Name of the source address (not the IP address) of a policy. |
| Destination | Name of the destination address. |
| Application | Name of a preconfigured or custom application of the policy match. |
| Action | Action taken when a match occurs as specified in the policy. |

Zones

–Displays the available trust and untrust zones configuration.

Trust Zone Interfaces

NOTE: This option is available only for the Standalone mode.

| | |
|---------------------------|---|
| Add Trust Zone Interface | Click + to add trust zone interface. For more information on the fields, see Table 4 on page 32 . |
| Edit Trust Zone Interface | Select an interface and click the pencil icon at the right corner of the table to modify the configuration. |

Table 3: Setup Wizard Configuration (Continued)

| Field | Action |
|--|--|
| Delete Trust Zone Interface | <p>Select an interface and click the delete icon at the upper-right corner of the table.</p> <p>A confirmation window appears. Click Yes to delete the selected interface or click No to discard.</p> |
| Search Trust Zone Interface | Click the search icon at the right corner of the table to quickly locate a zone or an interface. |
| Detailed View Trust Zone Interface | Hover over the interface name and click the Detailed View icon to view the zone and interface details. |
| Trust Zone Interfaces—Zone Level Settings | |
| Zone name | <p>View the trust zone name populated from your device factory default settings.</p> <p>NOTE: For standalone mode, trust and untrust zones are created by default even if these zones are not available in the factory default settings.</p> |
| Description | Enter the description for trust zone. |
| System services | <p>Enable this option for the types of traffic that can reach the device on a particular interface.</p> <p>By default, this option is enabled. You can disable if required.</p> |
| Protocols | <p>Enable this option to configure the device to perform stateful network traffic filtering on network packets using network traffic protocols (for example, TCP and UDP).</p> <p>By default, this option is enabled. You can disable if required.</p> |
| Application tracking | Enable this option to collect byte, packet, and duration statistics for application flows in the specified zone. |

Table 3: Setup Wizard Configuration (Continued)

| Field | Action |
|--|--|
| Source identity log | Enable this option for the device to log the user identity information based on the source zone configured in the security policy. |
| Untrust Zone Interfaces | |
| Add Untrust Zone Interface | Click + to add untrust zone interface. For more information on the fields, see Table 5 on page 38 . |
| Edit Untrust Zone Interface | Select an interface and click the pencil icon at the right corner of the table to modify the configuration. |
| Delete Untrust Zone Interface | Select an interface and click the delete icon at the upper-right corner of the table. A confirmation window appears. Click Yes to delete the selected interface or click No to discard. |
| Search Untrust Zone Interface | Click the search icon at the upper-right corner of the table to quickly locate a zone or an interface. |
| Detailed View Untrust Zone Interface | Hover over the interface name and click the Detailed View icon to view the zone and interface details. |
| Untrust Zone Interfaces—Zone Level Settings | |
| Zone name | View the untrust zone name populated from your device factory default settings. NOTE: For standalone mode, trust and untrust zones are created by default even if these zones are not available in the factory default settings. |
| Description | Enter the description for untrust zone. |

Table 3: Setup Wizard Configuration (Continued)

| Field | Action |
|--|--|
| Application tracking | Enable this option to collect byte, packet, and duration statistics for application flows in the specified zone. |
| Source identity log | Enable this option for the device to log the user identity information based on the source zone configured in the security policy. |
| DNS Servers & Default Gateways | |
| DNS Servers | |
| DNS server 1 | Enter the IPv4 or IPv6 address of the primary DNS. |
| DNS server 2 | Enter the IPv4 or IPv6 address of the secondary DNS. |
| Default Gateway | |
| Default gateway (IPv4) | Enter the IPv4 address of the next possible destination for any network. |
| Default gateway (IPv6) | Enter the IPv6 address of the next possible destination for any network. |
| Tap Settings | |
| NOTE: This option is available only for the Passive (Tap) mode. | |
| Tap Settings | |
| Tap interface | Select the interface from the list. |
| IP-IP tunnel inspection | Enable this option for the SRX Series Firewall to inspect pass through traffic over an IP-IP tunnel. |

Table 3: Setup Wizard Configuration (Continued)

| Field | Action |
|---|---|
| GRE tunnel inspection | Enable this option for the SRX Series Firewall to inspect pass through traffic over a GRE tunnel. |
| Security Policy & Advanced Services | |
| NOTE: Your device must have internet connectivity to use IPS, Web filtering, Juniper ATP Cloud, and Security threat intelligence services. | |
| From Zone | Name of the source zone. In the Tap mode, permits all traffic from the tap zone. |
| To Zone | Name of the destination zone. In the Tap mode, permits all traffic from the TAP zone to the TAP zone. |
| Source | Name of the source address (not the IP address) of a policy. |
| Destination | Name of the destination address. |
| Application | Name of a preconfigured or custom application of the policy match. |
| Action | Action taken when a match occurs as specified in the policy. |
| Content Security | |
| Content Security | Enable this option for configuring Content Security services. |
| License | <p>Enter Content Security license key and click Install License to add a new license.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • Use a blank line to separate multiple license keys. • To use Content Security services, your device must have internet connectivity from a revenue interface. |

Table 3: Setup Wizard Configuration (Continued)

| Field | Action |
|-----------------------|--|
| Content Security type | <p>Select an option to configure Content Security features:</p> <ul style="list-style-type: none"> • Web Filtering • Antivirus • Antispam |
| Web filtering type | <p>Select an option:</p> <ul style="list-style-type: none"> • 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). • Local—Specifies the local profile type. |
| IPS | |
| IPS | Enable this option to install the IPS signatures. |
| License | <p>Enter the license key and click Install License to add a new license.</p> <p>NOTE: The installation process may take few minutes.</p> |
| IPS signature | <p>Click Browse to navigate to the IPS signature package folder and select it. Click Install to install the selected IPS signature package.</p> <p>NOTE: You can download the IPS signature offline package at https://support.juniper.net/support/downloads/.</p> |
| ATP Cloud | |

Table 3: Setup Wizard Configuration (Continued)

| Field | Action |
|------------------------------|---|
| ATP Cloud | <p>Enable this option to use Juniper ATP Cloud services.</p> <p>NOTE: After the Juniper ATP Cloud configuration is pushed, only the SRX300 line of devices and SRX550M devices are rebooted. Your device must have internet connectivity to enable Juniper ATP Cloud enrollment process through J-Web.</p> |
| Security Intelligence | |
| Security intelligence | <p>Enable this option to use Security intelligence services.</p> <p>NOTE: After the Security Intelligence configuration is pushed, only the SRX300 line of devices and SRX550M devices are rebooted. Your device must have internet connectivity to enable Juniper ATP Cloud enrollment process through J-Web.</p> |
| User Firewall | |
| User Firewall | Enable this option to use user firewall services. |
| Domain name | Enter a domain name for Active Directory. |
| Domain controller | Enter domain controller IP address. |
| Username | Enter a username for administrator privilege. |
| Password | Enter a password for administrator privilege. |

Table 4: Add Trust Zone

| Field | Action |
|----------------|--------|
| General | |

Table 4: Add Trust Zone (Continued)

| Field | Action |
|---|--|
| Type (family) | <ul style="list-style-type: none"> • Select Switching. Fields for switching interface are: NOTE: This option will be available for only SRX300 Series Firewalls, SRX550M, and SRX1500, and SRX1600 Firewalls. For SRX2300, SRX4100, SRX4200, SRX4600, SRX5000 Series Firewalls, and vSRX Virtual Firewalls, the Type (family) field is not available. • IRB interface Unit—Enter the IRB unit. • Description—Enter the description for the interface. • Select Routing. Fields for routing interface are: For SRX5000 Series Firewalls, SRX4100, SRX4200, SRX4600, and vSRX Virtual Firewalls, the Type (family) field is not available. • Interface—Select an option from list. • Interface unit—Enter the Inet unit. NOTE: VLAN tagging is enabled automatically if the interface unit is higher than zero. • Description—Enter the description for the interface. • VLAN ID—Enter the VLAN ID. NOTE: VLAN ID is mandatory if the interface unit is higher than zero. |
| Interfaces | <p>Select an interface from the Available column and move it to the Selected column.</p> <p>NOTE: This option is available only for the Switching family type.</p> |
| <p>VLAN</p> <p>NOTE: This option is available only for the Switching family type.</p> | |
| Name | Enter a unique name for the VLAN. |
| VLAN ID | Enter the VLAN ID. |

Table 4: Add Trust Zone (Continued)

| Field | Action |
|---------------------------------|---|
| IPv4 | |
| IPv4 address | Enter a valid IPv4 address for the switching or the routing interface. |
| Subnet mask | Enter a subnet mask for the IPv4 address. |
| IPv6 | |
| IPv6 address | Enter a valid IPv6 address for the switching or the routing interface. |
| Subnet prefix | Enter a subnet prefix for the IPv6 address. |
| DHCP Local Server | |
| DHCP local server | Enable this option to configure the switch to function as an extended DHCP local server. |
| Pool name | Enter the DHCP pool name. |
| Pool start address | Enter the starting IPv4 address of the DHCP server pool address range. This address must be within the IPv4 network. |
| Pool end address | Enter the ending IPv4 address of the DHCP server pool address range. This address must be within the IPv4 network. NOTE: This address must be greater than the address specified in Pool start address. |
| Propagate settings from | Select an option from the list. Propagation of TCP/IP settings (such as, DNS and gateway address) received on the device interface acting as DHCP client. |
| Services & Protocols | |

Table 4: Add Trust Zone (Continued)

| Field | Action |
|-----------------|---|
| System Services | <p>Select system services from the list in the Available column and then click the right arrow to move it to the Selected column.</p> <p>The available options are:</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. • ping—Specify the internet control message protocol. • r2cp—Enable Radio-Router Control Protocol. • reverse-ssh—Specify the reverse SSH Service. |

Table 4: Add Trust Zone (Continued)

| Field | Action |
|-------|--|
| | <ul style="list-style-type: none"> • 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. • 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. • 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. |

Table 4: Add Trust Zone (Continued)

| Field | Action |
|-----------|--|
| Protocols | <p>Select protocols from the list in the Available column and then click the right arrow to move it to the Selected column.</p> <p>The available options are:</p> <ul style="list-style-type: none"> • all—Specifies all protocol. • bfd—Bidirectional Forwarding Detection. • bgp—Border 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. |

Table 5: Add Untrust Zone

| Field | Action |
|--|---|
| General | |
| Interface | Select an interface from the list. |
| Interface unit | Enter the interface unit value. |
| VLAN ID | Enter the VLAN ID. NOTE: VLAN ID is mandatory if the interface unit is higher than zero. |
| Description | Enter the description for the interface. |
| Address Mode | Select an address mode for the interface. The available options are DHCP Client, PPPoE (PAP), PPPoE (CHAP) and Static IP. NOTE: PPPoE (PAP) and PPPoE (CHAP) are not supported for SRX5000 Series Firwalls and if any of the devices are in passive mode. |
| Username | Enter a username for PPPoE (PAP) or PPPoE (CHAP) authentication. |
| Password | Enter a password for PPPoE (PAP) or PPPoE (CHAP) authentication. |
| IPv4 | |
| NOTE: This option is available only for the Static IP address mode. | |
| IPv4 Address | Enter a valid IPv4 address for the interface. |
| Subnet Mask | Enter a subnet mask for the IPv4 address. |

Table 5: Add Untrust Zone *(Continued)*

| Field | Action |
|--|--|
| IPv6 | |
| NOTE: This option is available only for the Static IP address mode. | |
| IPv6 Address | Enter a valid IPv6 address for the interface. |
| Subnet Prefix | Enter a subnet prefix for the IPv6 address. |
| Services & Protocols | |
| System Services | Select system services from the list in the Available column and then click the right arrow to move it to the Selected column. |
| Protocols | Select protocols from the list in the Available column and then click the right arrow to move it to the Selected column. |

SEE ALSO

| [Explore J-Web](#) | 39

Explore J-Web

IN THIS SECTION

- [J-Web: A First Look](#) | 40
- [J-Web Launch Pad](#) | 40
- [J-Web Top Pane](#) | 42
- [J-Web Side Pane](#) | 44

- J-Web Main Pane | 47
- J-Web Workflow Wizards | 49
- Summary | 50

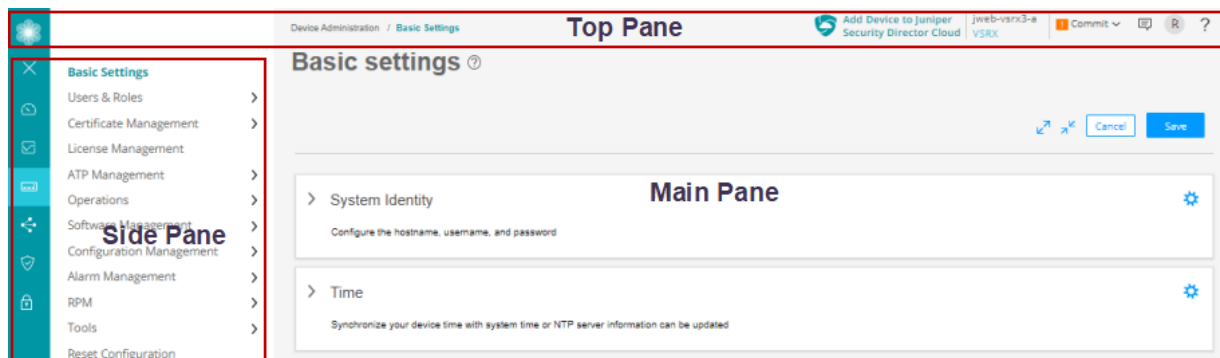
J-Web: A First Look

Each page of the J-Web interface is divided into the following panes (see [Figure 13 on page 40](#)):

- Launch pad—Displays high level details of the system identification, active users, and interface status. See [Figure 14 on page 41](#).
- Top pane—Displays identifying information and links.
- Side pane—Displays subtasks of the Dashboard, Monitor, Device Administration, Network, Security Policies and Objects, and Security Services tasks currently displayed in the main pane. Click an item to access it in the main pane.
- Main pane—Location where you monitor, configure, view or generate reports, and administrate the Juniper Networks device by entering information in text boxes, making selections, and clicking buttons.

NOTE: Starting in Junos OS Release 23.4R1, J-Web supports SRX1600 and SRX2300 Firewalls.

Figure 13: J-Web First Look



J-Web Launch Pad

After you successfully login to J-Web GUI, J-Web launch pad appears.

The launch pad provides a quick view of:

- Device information such as model number, serial number, hostname, software version, system time, and system up time.
- Number of active users using the device.
- State of the device physical interfaces: Up or Down.

The launch pad closes automatically once the application is loaded in the background. You do not have the option to manually close or refresh the launch pad.

NOTE:

- Launch pad is not displayed in the factory default settings.
- Launch pad is displayed for all users.

Figure 14 on page 41 shows the launch pad screen and its elements.

Figure 14: J-Web launch Pad Screen



J-Web Top Pane

For a more personal, helpful, and user experience, Juniper Networks has provided some aids within the J-Web GUI. [Table 6 on page 42](#) provides the details of the J-Web top pane elements.

Table 6: J-Web Top Pane Elements

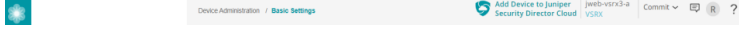



| Element | Description |
|---|---|
| <p>Banner</p>  | <p>Location—The gray bar at the top of the screen.</p> <p>You can access device details, feedback button, commit options, a profile management access menu, and a help button.</p> |
| <p>Add Device to Juniper Security Cloud</p>  | <p>Location—To the upper-right corner of the banner.</p> |
| <p>Device details</p>  | <p>Location—To the right of the Add Device to Juniper Security Director Cloud icon.</p> <p>Provides details of the device you have accessed.</p> |
| <p>Commit Configuration Menu</p>  | <p>Location—To the right of the device details icon.</p> <p>Provides options to:</p> <ul style="list-style-type: none"> • Commit your configurations • View configuration changes • Commit the changes with autorollback • Discard your configuration • Commit the changes in your preferred way |

Table 6: J-Web Top Pane Elements (Continued)




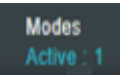
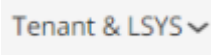
| Element | Description |
|--|--|
| <p>Feedback Button</p>  | <p>Location—To the right of the Commit menu.</p> <p>You can provide feedback (mailto:jweb-feedback@juniper.net) if you are having an issue with the product.</p> |
| <p>User Functions Menu</p>  | <p>Location—To the right of the Feedback icon.</p> <p>A head-and-shoulders icon and a field showing the logged in user type. Clicking your username or the down arrow button, logs you out of J-Web interface.</p> |
| <p>Help Button</p>  | <p>Location—To the right of the User Functions menu.</p> <p>Access to the online Help center and the Getting Started Guide are available by clicking the right-most icon on the banner, shaped like a question mark. The help center includes access to a list of supported web browsers, user interface assistance, as well as links to technical support and full J-Web documentation.</p> |
| <p>Mode</p>  | <p>Location—To the right of the device details.</p> <p>Provides the setup mode details whether your device is in the standard, chassis cluster (HA), or passive mode.</p> |

Table 6: J-Web Top Pane Elements (Continued)

| Element | Description |
|--|---|
| <p data-bbox="232 365 386 390">Tenant & LSYS</p>  | <p data-bbox="987 365 1398 426">Location—To the right of the Feedback icon.</p> <p data-bbox="987 459 1409 558">NOTE: This menu is only available for root-logical-system context and devices that support tenant and logical system.</p> <p data-bbox="987 592 1398 724">Starting in Junos OS 23.1R1 Release, you can view the name and number of available tenant or logical system. For example, Tenant (5).</p> <p data-bbox="987 758 1403 926">Select the name from the list to enter a root-logical-system user as a tenant or logical system. Use the search box to enter as a specific tenant or logical system,</p> <p data-bbox="987 959 1386 1127">To go back to the root-logical-system user context, click the down arrow on the selected tenant or logical system menu and choose Exit Tenant or Exit Logical System respectively.</p> <p data-bbox="987 1161 1382 1260">NOTE: Once the configuration cache synchronizes, the updated tenant or logical system data will be shown.</p> <p data-bbox="987 1293 1406 1461">If no tenant or logical system data is available, go to Device Administration > Multi Tenancy and create a new tenant or logical system from the respective menus.</p> |

J-Web Side Pane

J-Web presents you a security-focused administrator with a tabbed interface.

The following tabs across the side pane of the J-Web GUI provide workspaces in which an administrator can perform specific tasks:

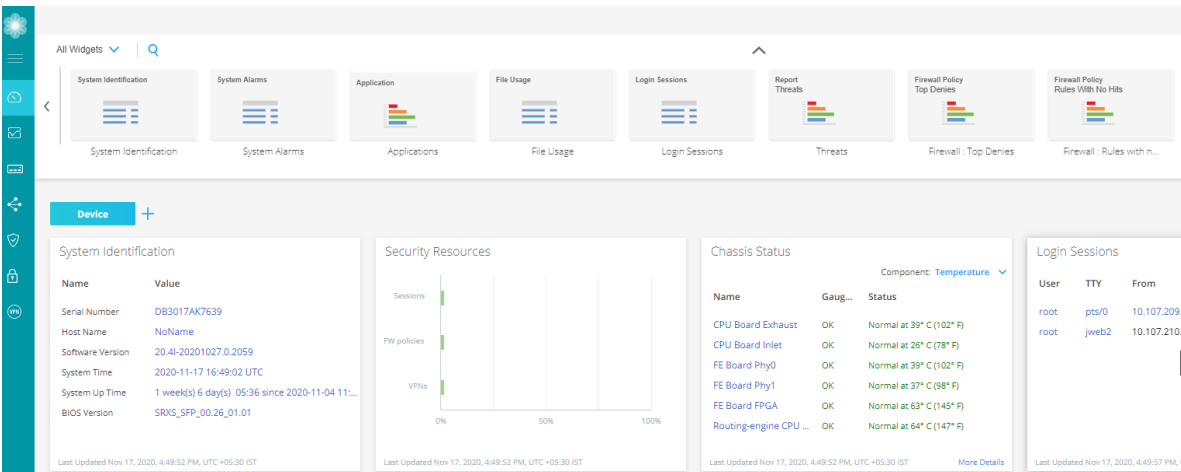
- **Dashboard**—The Dashboard is the main page for J-Web. You can customize the workspace in your Dashboard by adding widgets from the carousel. The placement of, and settings within, widgets are

saved so that anything from device information to firewall event information or from top blocked viruses to live threat maps can be unique for each user. Once you decide on the widgets that you want to see, you can minimize the carousel to regain some screen space.

NOTE: By default, the selected widgets are displayed every time you login to J-Web.

Figure 15 on page 45 shows an example of the J-Web Dashboard tab.

Figure 15: J-Web Dashboard Tab



- Monitor—The Monitor tab provides a workspace in which graphical representations of network traffic, firewall events, live threats, and network user data are available. There is also detailed data for alerts and alarms information. In this workspace, you can review the detailed information needed to understand what is happening to the managed security devices and traffic in your network.

Figure 16 on page 46 shows an example of the J-Web Monitor tab.

Figure 16: J-Web Monitor Tab

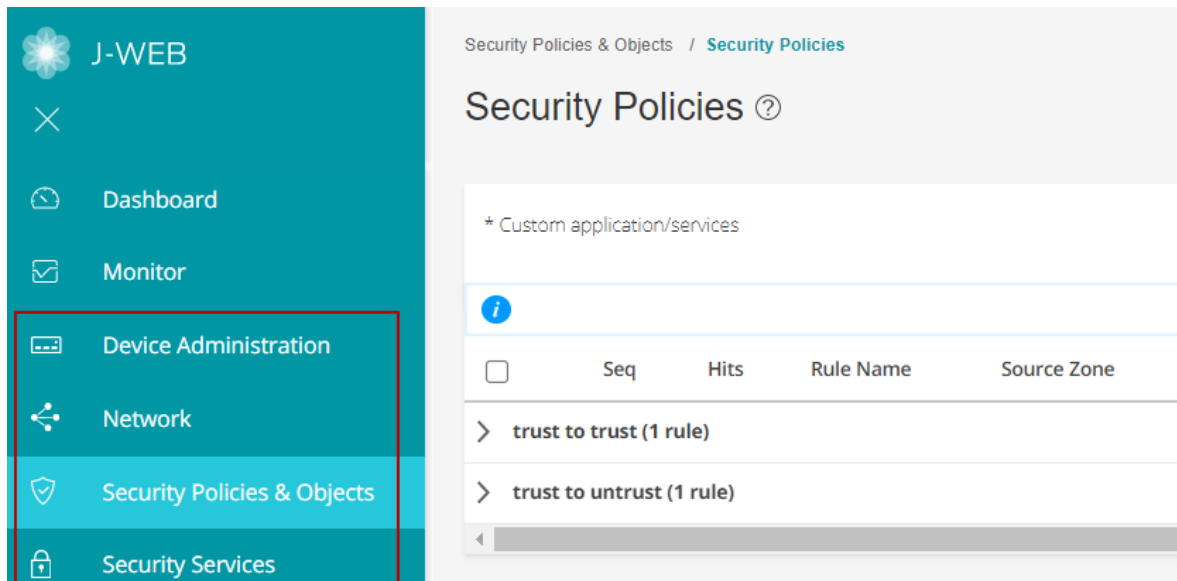
The screenshot shows the 'Interfaces' tab in the J-Web Monitor. The left sidebar contains navigation options: Interfaces (selected), Logs, Maps & Charts, Statistics, and Reports. The main content area displays a table of interfaces for Slot 0. The table has columns for Interface, Admin Status, Link Status, Address, Zone, and Services. The interface 'ge-0/0/3' is highlighted in blue.

| Interface | Admin Status | Link Status | Address | Zone | Services |
|------------|--------------|-------------|----------------|---------|------------------|
| ge-0/0/0 | Up | Down | | | |
| ge-0/0/0.0 | Up | Down | | untrust | dhcp, ftp, https |
| ge-0/0/1 | Up | Down | | | |
| ge-0/0/1.0 | Up | Down | 192.168.2.1/24 | trust | |
| ge-0/0/2 | Up | Up | | | |
| ge-0/0/2.0 | Up | Up | 192.168.3.1/24 | trust | |
| ge-0/0/3 | Up | Up | | | |
| ge-0/0/3.0 | Up | Up | 192.168.4.1/24 | trust | |
| ge-0/0/4 | Up | Down | | | |

- Configure—The highlighted workspace in [Figure 17 on page 47](#) is where all of the SRX Series Firewall configuration happens. You can configure the following features for managing your network security:
 - Device Administration—Such as basic settings, user management, certificate management, license management, security package management, ATP management, operations, software management, configuration management, alarm management, RPM, tools, and reset configuration.
 - Network—Such as connectivity, DHCP, firewall filters, NAT, routing, Class of Services (CoS), Application QoS, IPsec VPN, and dynamic VPN.
 - Security policies and objects—Such as security policies, zones/screens, zone and global addresses, services, dynamic applications, application tracking, schedules, and proxy profiles.
 - Security services—Such as Content Security, IPS, ALG, ATP, SSL profiles, firewall authentication, and ICAP redirect.

[Figure 17 on page 47](#) shows an example of the J-Web configuration menus.

Figure 17: J-Web Configure Menus



J-Web Main Pane

The main workspace of J-Web takes up the remainder of the browser window just below the Banner and next to the side pane. [Table 7 on page 47](#) shows a sample of navigation, customization, and help icons in the main pane of the J-Web GUI.

Table 7: J-Web Main Pane Elements



| Element | Description |
|--|--|
| Breadcrumbs  | Location—Upper left part of main screen. Not visible on the Dashboard. Trace your location in the GUI. The breadcrumbs provide a path back to one of the five tabs: Dashboard, Monitor, Configure, Reports, and Administration. |
| Info Tips  | Location—Various places around the GUI. Hover your mouse over any available question mark icon for quick pop-up guidance. |

Table 7: J-Web Main Pane Elements (Continued)



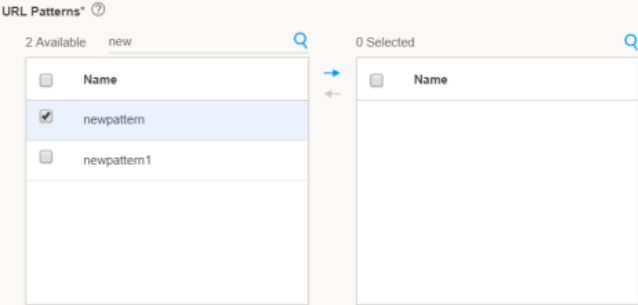
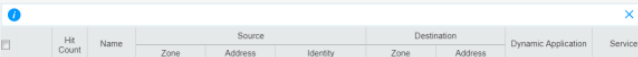





| Element | Description |
|--|---|
| <p>Show/Hide Columns</p>  | <p>Location—Upper right corner of some tabular display windows such as the Address Pools tab, Rules tab, and so on.</p> <p>In tabular displays, you can choose which columns are visible by clicking the icon and then selecting the check boxes on the menu.</p> |
| <p>Table Search</p>  | <p>Location—Upper right corner of tabular views.</p> <p>You can click the magnifying glass icon, within large tabular views, to search for specific text within any of the visible fields in the display.</p> |
| <p>Item Selector Search</p>  | <p>Location—Within the fields.</p> <p>You can use a search text box to select items for inclusion in a rule or policy.</p> |
| <p>Advanced Search</p>  | <p>Location—Above the table grid.</p> <p>The search includes the logical operators as part of the filter string. In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.</p> <p>NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.</p> |

Table 7: J-Web Main Pane Elements (Continued)

| Element | Description |
|--|---|
| Filter  | Location—Upper right corner of tabular views. You can click the filter icon to select any value from a list for category and subcategory columns. The grid is reloaded with the filtered category and subcategory. |
| Success message  | Location—At the top of the main pane. A message is displayed with this icon to state that your task is successful. |
| Information message  | Location—At the top of the main pane. A message is displayed with this icon to state you have some pending actions, but you can continue with the task. |
| Alert message  | Location—At the top of the main pane. A message is displayed with this icon to state you have some pending actions which you must complete to proceed with the required task. |
| Warning message  | Location—At the top of the main pane. A message is displayed with this icon to state you have some pending actions which you must complete else you cannot proceed with the required task. |

J-Web Workflow Wizards

J-Web contains assisting workflow wizards that guide you through some of its security functions. These include Setup wizard, Chassis Cluster wizard, PPPoE wizard, and NAT wizard. These wizards help you with a guided setup and helps you in performing step-by-step configuration of a services gateway that can securely pass traffic.

NOTE: PPPoE and NAT Wizards are available only in the SRX300 line of devices and SRX550M devices.

Summary

J-Web is a GUI approach that aims to provide a graphical framework to help you visualize and manage your SRX Series Firewalls more easily.

SEE ALSO

| [Add an SRX Series Firewall to Juniper Security Director Cloud](#) | 52

2

PART

Add SRX Series Firewall to Security Director Cloud

[Add an SRX Series Firewall to Juniper Security Director Cloud](#) | 52

Add an SRX Series Firewall to Juniper Security Director Cloud

You can add your SRX Series Firewall to Juniper Security Director Cloud from J-Web. After you add the SRX Series Firewall to the Juniper Security Director Cloud, you can manage your network security using these devices.

NOTE: Starting in Junos OS Release 23.4R1, J-Web supports SRX1600 and SRX2300 Firewalls.

In order for your device to be managed by Juniper Security Director Cloud, ensure the following:

- Your device must have Internet connectivity and access to the Juniper Security Director Cloud portal.
- Before adding, you must open the following ports of your device so that it communicates with Juniper Security Director Cloud:
 - TCP/443 (HTTPS) for [Juniper Security Director Cloud portal](#) and [Redirect server](#)
 - TCP/7804 (NETCONF) for SRX Series Firewall outbound access to Juniper Security Director Cloud portal
 - TCP/6514 (TLS syslog)
 - TCP/53 (DNS) - (IP: 8.8.8.8)
 - UDP/53 (DNS) - (IP: 8.8.4.4)

Here's how you can add your device to Juniper Security Director Cloud from J-Web:

1. Login to J-Web.
2. Click **Add Device to Juniper Security Director Cloud** located on the upper-right corner of the J-Web GUI to open the Add Device to Juniper Security Director Cloud page.
3. Select your location from the list and then enter your Juniper Security Director Cloud account email and password. Then, click **Next**.
4. Select your organization account name (with administrator permissions) and click **Proceed**.
The status progress bar is shown until your device is successfully added. During this process, your device gets added to the Juniper Security Director Cloud and commits the received configuration from the Cloud API.

A success message is displayed and your device is added to Juniper Security Director Cloud. The label next to the icon changes from **Add Device to Juniper Security Director Cloud** to **Managed by Juniper Security Director Cloud** and the changed label is grayed out.

NOTE:

- When you have logged into the J-Web and remove your device from Juniper Security Director Cloud, J-Web still displays the status as **Manged by Juniper Security Director Cloud**. Log in to J-Web again to see the label changed to **Add Device to Juniper Security Director Cloud**.
- If there are any network issues between the SRX Series Firewall and Juniper Security Director Cloud, J-Web still displays the status as **Manged by Juniper Security Director Cloud**.

Once added, you can see your device on the **Device Management > Devices** page when you log into the Juniper Security Director Cloud portal. You can only delete your device from Juniper Security Director Cloud and not from the J-Web GUI. To remove the device, select your device on the Devices page and click the delete icon.

RELATED DOCUMENTATION

| [Dashboard Overview](#) | 55

3

PART

Dashboard

J-Web Dashboard | 55

J-Web Dashboard

IN THIS CHAPTER

- [Dashboard Overview | 55](#)

Dashboard Overview

IN THIS SECTION

- [What is J-Web Dashboard | 55](#)
- [Work with Widgets | 56](#)

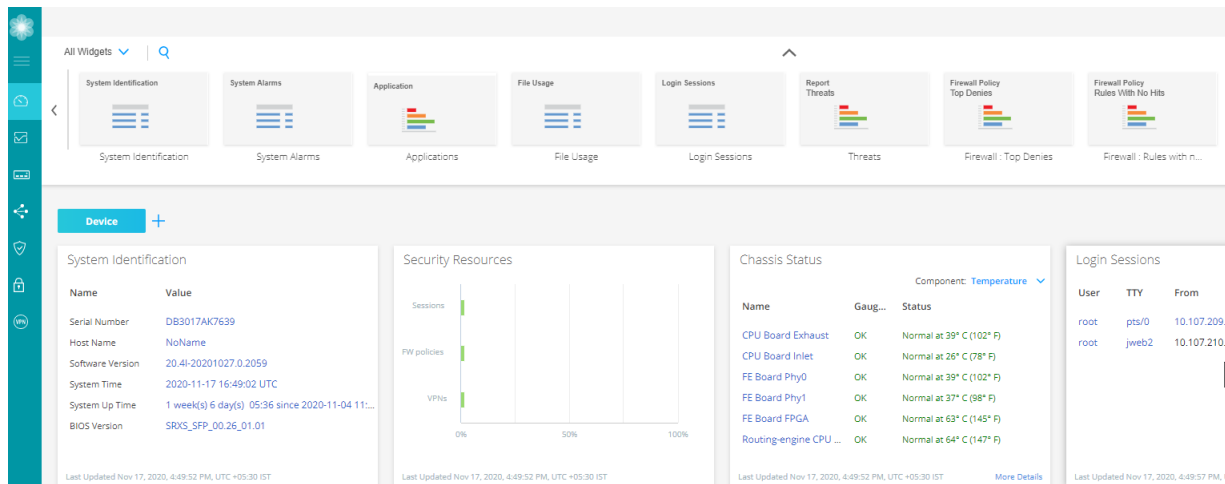
What is J-Web Dashboard

The J-Web dashboard provides a unified overview of the system and network status retrieved from SRX Series Firewalls.

To use the dashboard at the top-level menu, select **Dashboard**. By default, the Dashboard page displays all the widget thumbnails.

[Figure 18 on page 56](#) shows an example of the Dashboard page of SRX345 Firewall.

Figure 18: SRX345 Dashboard



Work with Widgets

Each widget pane acts as a separate frame. You can click + icon to add separate dashboard and name it as per your ease. You can refresh the display of the Dashboard page by clicking the refresh icon at the upper-right corner above the widget pane.

You can choose any one of the categories to view widgets on your device:

- All Widgets—Displays all the supported widgets
- Applications—Displays only the supported application related widgets
- Devices—Displays only the supported device related widgets
- Security—Displays only the supported security related widgets

NOTE:

- Starting in Junos OS Release 21.4R1, on-box reports related widgets are removed to speed up the J-Web UI loading process.
- The Threat Activity pane is not available on SRX5400, SRX5600, and SRX5800 devices.
- For SRX Series Firewalls 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.

- If the rescue configuration is not set, the set rescue configuration link directs you to the Device Administration > Configuration Management > Rescue page to set the rescue configuration.
- Starting in Junos OS Release 23.4R1, J-Web supports SRX1600 and SRX2300 Firewalls. For the other SRX Series Firewalls, you can create only one domain.

To use a widget on the Dashboard:

1. Drag the widgets from the palette or thumbnail container to your dashboard.

When you add more widgets on the J-Web Dashboard, you can observe high CPU usage on the Routing Engine for a short span of time on every refresh. We recommend that you use four widgets for lower CPU consumption.

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

NOTE: The dashlet data is refreshed every minute by default. You cannot manually configure the refresh interval of the dashlet. If the data is not aged in the cache, data loads from the cache during the dashlet refresh. If the data is aged, it is retrieved from the device during the next refresh interval cycle.

[Table 8 on page 57](#) provides the dashboard widgets options based on the selected device.

Table 8: Dashboard Widgets Options

| Field | Description |
|-----------------------|--|
| System Alarms | Provides the received time, severity, description of the alarms and the action to be taken. |
| System Identification | Provides system details such as serial number of the software, hostname, software version, BIOS version, system uptime, and system time. |
| Login Sessions | Provides the user credentials, login time, idle time, and host. |

Table 8: Dashboard Widgets Options (Continued)

| Field | Description |
|-----------------------------------|---|
| File Usage | <p>Provides current space requirements for log, temporary, crash, and database files. Click Maintain to download or delete some or all of these files.</p> <p>NOTE: File Usage widget supports RE3 line cards for SRX5000 line of devices.</p> |
| Resource Utilization | <p>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.</p> <p>NOTE: Resource Utilization widget supports RE3 line cards for SRX5000 line of devices.</p> |
| Signal Strength | Displays the signal strength of the device. |
| Interface: Most Dropped Packets | Displays top 5 interfaces based on the CLI response; top-count will increase to 10. |
| Security Resources | Provides the maximum, configured, and activated number of sessions, firewall/VPN policies, and IPsec VPNs. |
| Storage Usage | Displays used and available storage and usage information about other system components. |
| 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. |
| NAT - Top Source Translation Hits | <p>Displays the top 10 source translation hits.</p> <p>Click More Details to view source NAT logs at Monitor > Logs > All Events.</p> |

Table 8: Dashboard Widgets Options (Continued)

| Field | Description |
|--|---|
| NAT - Top Destination Translation Hits | <p>Displays the top 10 destination translation hits.</p> <p>Click More Details to view destination NAT logs at Monitor > Logs > All Events.</p> |
| IPsec VPNs (IKE Peers) | <p>Displays status count of IPsec VPN topologies, such as ADVPN Hub and Spoke, Remote Access, and Site-to-Site/Hub & Spoke.</p> <p>Click More Details to redirect to the Monitor > Network > IPsec VPN page.</p> |
| VPN Monitoring | <p>Displays the total number of IPsec VPNs (Total VPNs for All VPNs and total remote users for Remote Access). All VPNs option includes Site to Site, Hub & Spoke, ADVPN Hub, and ADVPN spoke. Remote Access includes Juniper Secure Connect and NCP Exclusive Entry Client.</p> <p>Widget pane also displays the VPNs status with a color code:</p> <ul style="list-style-type: none"> • Up (Green)—IKE and IPsec SA are up. • Down (Red)—IKE and IPsec are not operationally up. • Partially Up (Amber)—Either IKE or IPsec SA is up or one or few traffic selectors are up. <p>Click More Details available on the widget pane to redirect to the Monitor > Network > IPsec VPN page.</p> <p>On the widget pane, for the All VPNs option, each configured IPsec VPN is represented as an individual tunnel icon or box.</p> <p>On the widget pane, for the Remote Access option, each IKE SAs corresponding to the configured IPsec VPN is represented as an individual tunnel icon or box. If there are no IKE SAs for the VPN, then a single box is shown as down.</p> <p>When you hover over the box, widget displays VPN tunnel details such as Remote gateway, VPN name, IKE status, IPsec status, local IP, and remote IP. Click More Details to redirect to the Monitor > Network > IPsec VPN page with the VPN name filtered.</p> |
| Zones: Most Bandwidth By Bytes | <p>Displays zones with maximum throughput rate in bytes, sorted by incoming and outgoing bytes.</p> |

Table 8: Dashboard Widgets Options (Continued)

| Field | Description |
|-----------------------------|--|
| Zones: Most Dropped Packets | Displays firewall zones with maximum number of packet drops, sorted by count. |
| Top Scanned File Categories | Displays top scanned files for malware. These files can be executable files, archived files, or libraries. |

4

PART

Monitor

[Network](#) | 62

[Logs](#) | 69

[Maps and Charts](#) | 105

[Statistics](#) | 120

[Reports](#) | 129

Network

IN THIS CHAPTER

- Monitor Interfaces | 62
- Monitor DHCP Server Bindings | 63
- Monitor IPsec VPN | 65

Monitor Interfaces

You are here: **Monitor** > **Network** > **Interfaces**.

Use this page to view general information about all physical and logical interfaces for a device.

NOTE: Starting in Junos OS Release 23.4R1, J-Web supports SRX1600 and SRX2300 Firewalls.

[Table 9 on page 62](#) describes the fields on the Interfaces page.

Table 9: Fields on the Interfaces Page

| Field | Description |
|------------------|---|
| Show Interfaces | Select All or any particular slot to show the interface details. |
| View 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. |
| Clear Statistics | Clears the statistics for the selected interface. |

Table 9: Fields on the Interfaces Page (Continued)

| Field | Description |
|------------------------|--|
| Auto Refresh Frequency | Indicates the duration of time after which you want the data on the page to be refreshed automatically. |
| Interface | Displays the interface name. |
| Link Status | Displays whether the interface is linked (Up) or not linked (Down). |
| Address | Displays the IP address of the interface. |
| Zone | Displays whether the zone is an untrust zone or a trust zone. |
| Host Inbound Traffic | Displays the following: <ul style="list-style-type: none"> • Services that are enabled on the device, such as HTTPS and SSH. • Protocols that are enabled on the device, such as BGP and IGMP. |

RELATED DOCUMENTATION

| [Monitor Session | 69](#)

Monitor DHCP Server Bindings

You are here: **Monitor > Network > DHCP Server Bindings.**

Use this page to view information about dynamic and static DHCP leases, conflicts, pools, and statistics.

[Table 10 on page 64](#) describes the fields on the DHCP Server Bindings page.

Table 10: Fields on the DHCP Server Bindings Page

| Field | Description |
|------------------------|---|
| Routing Instance | Select the routing instance name. |
| DHCP Interface Details | Displays the interface on which the DHCP server is configured. |
| Clear | Clears all or selected binding information. |
| Client IP Address | Displays the IP address of the DHCP client. |
| MAC Address | Displays the MAC address of the DHCP server. |
| State | <p>State of the address binding table on the extended DHCP local server:</p> <ul style="list-style-type: none"> • BOUND—Client has an active IP address lease. • FORCE RENEW—Client has received the FORCE RENEW 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. |
| Lease Time Remaining | Displays the time (in hours and minutes) at which the lease expires. |
| DHCP Interface | Displays the interface on which the request was received. |
| Session ID | Displays the Session ID of the subscriber session. |

RELATED DOCUMENTATION

| [About Reports Page](#) | 129

Monitor IPsec VPN

You are here: **Monitor** > **Network** > **IPsec VPN**.

Use the monitoring functionality to view information of IKE, IPsec configuration, Security Associations (SA), and Statistics in a tabular format that includes sortable columns. A VPN provides a means by which remote computers communicate securely across a public WAN such as the Internet. IPsec VPN is a protocol that consist set of standards used to establish a VPN connection.

[Table 11 on page 65](#) describes the fields on the IPsec VPN page.

Table 11: Fields on the IPsec VPN Page

| Field | Description |
|----------------------------|---|
| IPsec Statistics list menu | Displays summary of the global IPsec VPN or selected IPsec VPN statistics. |
| Clear SA list menu | <p>Displays the options Clear All SAs or Clear Selected SA to clear SAs.</p> <p>If you choose Clear All SAs, then you can select Clear All IKE SAs, Clear All IPsec SAs, or Clear All IKE & IPsec SAs.</p> <p>If you choose Clear Selected SAs, then you can select Clear Selected IKE SA, Clear Selected IPsec SA, or Clear Selected IKE & IPsec SA.</p> |
| Refresh icon | <p>Click refresh icon to get latest operational data.</p> <p>NOTE: The configuration data is fetched from cache. Any changes to the CLI will be fetched only after you commit it and click Monitor > Network > IPsec VPN to refresh the page and get the latest configuration data.</p> |
| Search | You can search and filter either the remote gateway or the VPN name. |
| Remote Gateway | Displays gateway name of the remote system. |
| IKE Status | Displays if IKE is up or down. |

Table 11: Fields on the IPsec VPN Page (Continued)

| Field | Description |
|--------------------|--|
| Local IP | Displays the external interface, IP address, and port of the local peer so that its remote peer can communicate with it. |
| Remote IP | Displays the IP address and port of the remote peer. NOTE: The remote IP displays only when the IKE is up. |
| VPN Name | Displays IPsec VPN name. |
| TS/Proxy ID Status | Displays information and status (up or down) of the traffic selector or the proxy ID that are negotiated between the peers. |
| Connection Profile | Displays the connection profile in the FQDN or FQDN/realm format if configured. If not configured, the field displays as external-IP/VPN-Name. |
| IPsec Soft Life | Displays the soft lifetime (in seconds) which indicates that the IPsec key management system that the SA is about to expire. |
| IKE Index | Displays index number for a particular IKE SA. |
| IPsec Index | Displays index number for a particular IPsec SA. |
| Topology | Displays the topology deployment for an IPsec VPN. For example: Site to Site/Hub & Spoke or Remote Access VPN. |
| IKE Proposal | Lists algorithms negotiated with the remote peer. |
| IPsec Proposal | Lists protocols and algorithms negotiated with the remote peer. |

Table 11: Fields on the IPsec VPN Page (Continued)

| Field | Description |
|----------------------|---|
| Authentication Type | Display if the preshared key or certificate based is used by the Virtual Private network (VPN). |
| DPD | Displays dead peer detection (DPD) method used by devices to verify the current existence and availability of IPsec peers. |
| Role | Displays whether the device is an initiator or a responder. |
| IKE Initiator Cookie | Random number, called a cookie, which is sent to the remote node when the IKE negotiation is triggered. |
| IKE Responder Cookie | Random number generated by the remote node and sent back to the initiator as a verification that the packets are received. |
| IKE Life | Lifetime (in seconds) of an IKE SA. Range: 180 through 86,400. Default is 3600. |
| 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 each message contains. 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. Displays the authentication method used: 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. |

Table 11: Fields on the IPsec VPN Page (Continued)

| Field | Description |
|-----------------|---|
| Peer IKE-ID | Displays the IKE IDs for the local or remote devices. |
| Remote Access | Displays the remote access URL. NOTE: This option is applicable only for the remote access VPN with Juniper Secure Connect (JSC). |
| Remote User | Displays the remote IKE identity to exchange with the destination peer to establish communication. |
| DNS | Displays the IP addresses for a primary and a secondary DNS servers. |
| WINS | Displays the IP addresses for a primary and a secondary WINS servers. |
| Inbound SPI | Displays security parameter index (SPI) value to authenticate incoming traffic coming from the peer. |
| Outbound SPI | Displays algorithms, keys, or SPI values to decrypt and to authenticate outbound traffic to the peer. |
| IPsec Hard Life | Displays number of seconds until the SA expires. |
| IPsec Lifesize | Displays the lifesize remaining specifies the usage limits in kilobytes. If no lifesize is specified, it shows unlimited. |

RELATED DOCUMENTATION

| [Monitor Session](#) | 69

Logs

IN THIS CHAPTER

- Monitor Session | 69
- Monitor Threats | 75
- Monitor Web Filtering | 81
- Monitor ATP | 85
- Monitor VPN | 90
- Monitor All Events | 93
- Monitor System | 101
- Monitor Alarms | 103

Monitor Session

You are here: **Monitor** > **Logs** > **Session**.

Use the monitoring functionality to view the firewall events or sessions that occurred during the time period specified.

NOTE: Session page is available on all the SRX Series Firewalls except the SRX5000 line of devices.

[Table 12 on page 70](#) describes the fields on the Session page.

Table 12: Fields on the Session Page

| Field | Description |
|-------------------|---|
| Last | <p>Select the time from the list to view the activity that you are most interested in. Once you select the time, all the data presented in your view refreshes automatically.</p> <p>You can also use Customize to set a custom date and click Apply to view the specified session logs.</p> |
| More | <ul style="list-style-type: none"> • View PCAP Counters—View packet capture (PCAP) counter statistics for unknown application traffic. Click Clear Counters to reset all the packet capture counters value of the unknown application traffic to zero. • Delete PCAP Files—Select this option to permanently delete all the available PCAP files on your device. |
| Refresh | Click the refresh icon to get the latest session information. |
| Show Hide Columns | <p>The three vertical dots represents this icon.</p> <p>Enables you to show or hide a column in the grid.</p> |
| Export to CSV | <p>You can export the session data to a comma-separated value (.csv) file.</p> <p>Select the three vertical dots on the right-side of the page and then click Export to CSV. The CSV file is downloaded to your local machine. You can download only maximum of 100 sessions data.</p> |

Table 12: Fields on the Session Page (*Continued*)

| Field | Description |
|-----------------|--|
| Filter Criteria | <p>Use the filter text box present above the table grid. The search includes the logical operators as part of the filter string.</p> <p>NOTE: Starting in Junos OS 23.1R1 Release, J-Web supports the following operators:</p> <ul style="list-style-type: none"> • = (equal to) • AND • != (not equal to) • >= (greater than or equal to) • <= (less than or equal to) • Nested and/or <p>J-Web also supports Netmask when searching for IP addresses.</p> <p>In the filter text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.</p> <p>The following filters are available:</p> <ul style="list-style-type: none"> • Source IP • Destination IP • Session ID • Log type • User • Application • Source Zone • Destination Zone • Source Country • Destination Country |

Table 12: Fields on the Session Page (Continued)

| Field | Description |
|--------------|---|
| | <ul style="list-style-type: none"> • Source Port • Destination Port • Protocol |
| X | Click X to clear your search filter. |
| Save Filter | <p>Click Save Filter to save filters after you specify the filtering criteria.</p> <p>To save a filter:</p> <ol style="list-style-type: none"> 1. Enter the filter criteria you are looking for in the advanced search box. 2. Click Save Filter. 3. Enter a name for the filter and click the tick icon to save it. |
| Load Filter | <p>Displays the saved filters list.</p> <p>Hover over the saved filter name to view the query expression. You can delete the saved filter using the delete icon.</p> |
| View Details | <p>When you hover over the PCAP file, a Detailed View icon appears before the PCAP file. Click the icon to view the log details on the Detailed Log View page.</p> <p>Click on the download icon in the Detailed Log View page to download the packet capture file of an unknown application traffic. The session ID available in the file name identifies the PCAP file.</p> <p>NOTE: If the files are not available, the download fails and you will receive an error message.</p> |
| PCAP | <p>Click on the download icon to download the packet capture (PCAP) file of an unknown application traffic. The download icon appears only if a packet captured for the session log type close.</p> <p>The session ID available in the file name identifies the PCAP file.</p> <p>NOTE: If the files are not available, the download fails and you will receive an error message.</p> |

Table 12: Fields on the Session Page (Continued)

| Field | Description |
|--------------------|---|
| Time | Displays the time when the log was received. |
| Log Type | Displays the log type. |
| Source Zone | Displays the source zone of the session. |
| Source IP | Displays the source IP address from where the session occurred. |
| User | Displays the username from whom the session log is generated. |
| Destination Zone | Displays the destination zone of the session. |
| Destination IP | Displays the destination IP of the session occurred. |
| Destination Port | Displays the destination port of the session. |
| Application | Displays the application name from which the session logs are generated. |
| Action | Displays the action taken for the event: warning, allow, and block. |
| Policy | Displays the destination country of the log. |
| Bandwidth | Displays the bandwidth utilization for the session. |
| NAT Source IP | Displays the translated (or natted) source IP address. It can contain an IPv4 or an IPv6 addresses. |
| NAT Source Port | Displays the translated source port. |
| NAT Destination IP | Displays the translated (also called natted) destination IP address. |

Table 12: Fields on the Session Page (Continued)

| Field | Description |
|----------------------|--|
| NAT Destination Port | Displays the translated destination port. |
| Protocol ID | Displays the protocol ID in the log. |
| Session ID | Displays the traffic session ID of the log. |
| Interface | Displays the interface of the session. |
| Closure Reason | Displays the reason for the log generation. For example, a connection tear down may have an associated reason such as authentication failed. |
| Packets From Client | Displays the number of packets received from the client. |
| Bytes From Client | Displays the number of bytes received from the client. |
| Packets From Server | Displays the number of packets received from the server. |
| Bytes From Server | Displays the number of bytes received from the server. |
| Elapsed Time | Displays the time elapsed since the last time interval began. |
| Source Port | Displays the port number of the source. |

RELATED DOCUMENTATION

| [Monitor Threats](#) | 75

Monitor Threats

You are here: **Monitor** > **Logs** > **Threats**.

Use the monitoring functionality to view the security threats. Threats are defined as any IPS, screen, security intelligence, antivirus, content filtering, or antispam.

NOTE: Threat page is available on all the SRX Series Firewalls except the SRX5000 line of devices.

Table 13 on page 75 describes the fields on the Threats page.

Table 13: Fields on the Threats Page

| Field | Description |
|-------------------|---|
| Last | Select the time from the list to view the activity that you are most interested in. Once the time is selected, all of the data presented in your view is refreshed automatically. You can also use Customize to set a custom date and click Apply to view the specified threats. |
| Refresh | Click the refresh icon to get the latest threat information. |
| Show Hide Columns | This icon is represented by three vertical dots. Enables you to show or hide a column in the grid. |
| Export to CSV | You can export the threats data to a comma-separated value (.csv) file. Select the three vertical dots on the right-side of the page and click Export to CSV . The CSV file is downloaded to your local machine. You can download only maximum of 100 sessions data. |

Table 13: Fields on the Threats Page (*Continued*)

| Field | Description |
|-----------------|--|
| Filter Criteria | <p>Use the filter text box present above the table grid. The search includes the logical operators as part of the filter string.</p> <p>NOTE: Starting in Junos OS 23.1R1 Release, J-Web supports the following operators:</p> <ul style="list-style-type: none"> • = (equal to) • AND • != (not equal to) • >= (greater than or equal to) • <= (less than or equal to) • Nested and/or <p>J-web also supports Netmask when searching for IP addresses.</p> <p>In the filter text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.</p> <p>The following filters are available:</p> <ul style="list-style-type: none"> • Source IP • Destination IP • Session ID • Log type • User • Application • Source Zone • Destination Zone • Source Country • Destination Country |

Table 13: Fields on the Threats Page (Continued)

| Field | Description |
|-------------|---|
| | <ul style="list-style-type: none"> • Source Port • Destination Port • Protocol |
| X | Click X to clear your search filter. |
| Save Filter | <p>Click Save Filter to save filters after you specify the filtering criteria.</p> <p>To save a filter:</p> <ol style="list-style-type: none"> 1. Enter the filter criteria you are looking for in the advanced search box. 2. Click Save Filter. 3. Enter a name for the filter and click the tick icon to save it. |
| Load Filter | <p>Displays the saved filters list.</p> <p>Hover over the saved filter name to view the query expression. You can delete the saved filter using the delete icon.</p> |

Table 13: Fields on the Threats Page (Continued)

| Field | Description |
|--------------|---|
| View Details | <p>When you hover over the PCAP file, a Detailed View icon appears before the PCAP file. Click the icon to view the log details on the Detailed Log View page.</p> <p>Click on the download icon on the Detailed Log View page to download the packet capture file. If the files are not available, the download fails and you will receive an error message.</p> <p>NOTE: The download icon will only be available for the IPS attack logs.</p> <p>To view the packet capture data on the Threats page, ensure that attack logging notification is enabled. If not:</p> <ol style="list-style-type: none"> 1. Go to Security Services > IPS > Policy. 2. Click the add icon (+) on the upper right side of the Policy page. The Add IDP Policy page appears. 3. Enter the name of the IPS policy and then click +. The Add IPS Rule page appears. 4. Click Advanced and select the check box to configure Enable Attack Logging under Notification. |
| PCAP | <p>Click on the download icon to download the packet capture (PCAP) file of IPS attacks.</p> <p>NOTE: The download icon appears only for the IPS attack logs.</p> <p>The PCAP file will be downloaded to your system from the <code>/var/log/pcap/</code> folder. If the files are not available, the download fails and you will receive an error message.</p> |
| Time | Displays the time when the threats log was received. |
| Log Type | Displays the threats log type. For example, IPS, Antivirus, Antispam, and so on. |
| Name | Displays the name of the event. |
| Severity | Displays the severity of the threat. |
| Source Zone | Displays the source zone of the threats. |

Table 13: Fields on the Threats Page (Continued)

| Field | Description |
|-----------------------|---|
| Source IP | Displays the source IP address from where the threats log occurred. |
| Source Port | Displays the port number of the source. |
| User | Displays the username from whom the threat log is generated. |
| Destination Zone | Displays the destination zone of the threats. |
| Destination IP | Displays the destination IP of the threats occurred. |
| Destination Port | Displays the port number of the destination. |
| Application | Displays the nested application or application name from which the threats are generated. |
| Action | Displays the action taken from the threats. |
| Session ID | Displays the traffic session ID of the threats. |
| Closure Reason | Displays the reason for the session closure. |
| Profile | Displays the threat profile name. |
| Category | Displays the threat category. |
| URL | Displays the accessed URL name that triggered the event. |
| Object | Displays the object name of the threats. |
| Destination Interface | Displays the interface name of the destination. |

Table 13: Fields on the Threats Page (Continued)

| Field | Description |
|------------------|--|
| Source Interface | Displays the interface name of the source. |
| Policy | Displays the policy name that triggered the threats log. |
| Rule | Displays the rule name of the threats log. |
| Protocol | Displays the protocol ID in the threats log. |
| CVE-ID | Displays the Common Vulnerabilities and Exposures (CVE) identifiers information for the threat. |
| Elapsed Time | Displays the time elapsed since the last time interval began. |
| Packet Log ID | Displays the packets ID received before and after the attack for further offline analysis of attacker behavior. |
| XFF | Displays X-Forwarded-For (XFF) header added to packets by a proxy server that includes the real IP address of the client making the request. |
| File Name | Displays the filename of the threats log. |
| Argument | Displays the arguments that are passed to an event when it is invoked from the threats log. |
| Source Name | Displays the name of the source from where threat is originated. |
| Feed Name | Displays the feed name of the threat detected. |
| Count | Displays the number of threats count. |
| Message Type | Displays the message type for the threat detected. |

Table 13: Fields on the Threats Page (Continued)

| Field | Description |
|-----------|---------------------------------------|
| HTTP Host | Displays the host URL for the threat. |

RELATED DOCUMENTATION

| [Monitor Web Filtering](#) | 81

Monitor Web Filtering

You are here: **Monitor** > **Logs** > **Web Filtering**.

Use this page to view information about the Web filtering events based on web filtering policies, filter options, and grid elements of Web filtering events.

NOTE: Web Filtering page is available on all the SRX Series Firewalls except the SRX5000 line of devices.

[Table 14 on page 81](#) describes the fields on the Web Filtering page.

Table 14: Fields on the Web Filtering Page

| Field | Description |
|---------|--|
| Last | Select the time from the list to view the activity that you are most interested in. Once the time is selected, all of the data presented in your view is refreshed automatically. You can also use Customize to set a custom date and click Apply to view the specified Web filtering event logs. |
| Refresh | Click the refresh icon to get the latest Web filtering event information. |

Table 14: Fields on the Web Filtering Page (Continued)

| Field | Description |
|-------------------|--|
| Show Hide Columns | <p>This icon is represented by three vertical dots.</p> <p>Enables you to show or hide a column in the grid.</p> |
| Export to CSV | <p>You can export the Web filtering event data to a comma-separated value (.csv) file.</p> <p>Select the three vertical dots on the right-side of the page and click Export to CSV. The CSV file is downloaded to your local machine. You can download only maximum of 100 sessions data.</p> |

Table 14: Fields on the Web Filtering Page (Continued)

| Field | Description |
|-----------------|--|
| Filter Criteria | <p>Use the filter text box present above the table grid. The search includes the logical operators as part of the filter string.</p> <p>NOTE: Starting in Junos OS 23.1R1 Release, J-Web supports the following operators:</p> <ul style="list-style-type: none"> • = (equal to) • AND • != (not equal to) • >= (greater than or equal to) • <= (less than or equal to) • Nested and/or <p>J-Web also supports Netmask when searching for IP addresses.</p> <p>In the filter text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.</p> <p>The following filters are available:</p> <ul style="list-style-type: none"> • Source IP • Destination IP • Session ID • Log type • User • Application • Source Zone • Destination Zone • Source Country • Destination Country |

Table 14: Fields on the Web Filtering Page (Continued)

| Field | Description |
|------------------|---|
| | <ul style="list-style-type: none"> • Source Port • Destination Port |
| X | Click X to clear your search filter. |
| Save Filter | <p>Click Save Filter to save filters after you specify the filtering criteria.</p> <p>To save a filter:</p> <ol style="list-style-type: none"> 1. Enter the filter criteria you are looking for in the advanced search box. 2. Click Save Filter. 3. Enter a name for the filter and click the tick icon to save it. |
| Load Filter | <p>Displays the saved filters list.</p> <p>Hover over the saved filter name to view the query expression. You can delete the saved filter using the delete icon.</p> |
| Time | Displays the time when the Web filtering event log was received. |
| Log Type | Displays the Web filtering event log type. |
| Source Zone | Displays the source zone of the Web filtering event. |
| Source IP | Displays the source IP address from where the Web filtering event occurred. |
| User | Displays the username from whom the Web filtering event log is generated. |
| Destination Zone | Displays the destination zone of the Web filtering event. |
| Destination IP | Displays the destination IP of the Web filtering event occurred. |

Table 14: Fields on the Web Filtering Page *(Continued)*

| Field | Description |
|-------------------|---|
| Destination Port | Displays the destination port of the Web filtering event. |
| Application | Displays the application name for which the Web filtering event logs are generated. |
| Action | Displays the action taken for the event: deny, permit, or redirect. |
| Session ID | Displays the traffic session ID of the Web filtering event log. |
| Closure Reason | Displays the reason for the Web filtering event log generation closure. |
| URL Category Risk | Displays the Web filtering URL risk level. |
| Profile | Displays the Web filtering profile name. |
| Category | Displays the Web filtering URL category. |
| URL | Displays the accessed URL name that triggered the event. |
| Obj | Displays the object name of the Web filtering event log. |

RELATED DOCUMENTATION

[Monitor ATP | 85](#)

Monitor ATP

You are here: **Monitor** > **Logs** > **ATP**.

Use the monitoring functionality to view the ATP page. Analyzing the Juniper ATP logs yields information such as malware name, action taken, infected host, source of an attack, and destination of an attack.

NOTE: ATP page is available on all the SRX Series Firewalls except the SRX5000 line of devices.

Table 15 on page 86 describes the fields on the ATP page.

Table 15: Fields on the ATP Page

| Field | Description |
|-------------------|---|
| Last | <p>Select the time from the list to view the activity that you are most interested in. Once the time is selected, all of the data presented in your view is refreshed automatically.</p> <p>You can also use Customize to set a custom date and click Apply to view the specified ATP logs.</p> |
| Refresh | Click the refresh icon to get the latest ATP log information. |
| Show Hide Columns | <p>This icon is represented by three vertical dots.</p> <p>Enables you to show or hide a column in the grid.</p> |
| Export to CSV | <p>You can export the ATP log data to a comma-separated value (.csv) file.</p> <p>Select the three vertical dots on the right-side of the page and click Export to CSV. The CSV file is downloaded to your local machine. You can download only maximum of 100 ATP log data.</p> |

Table 15: Fields on the ATP Page *(Continued)*

| Field | Description |
|-----------------|--|
| Filter Criteria | <p>Use the filter text box present above the table grid. The search includes the logical operators as part of the filter string.</p> <p>NOTE: Starting in Junos OS 23.1R1 Release, J-Web supports the following operators:</p> <ul style="list-style-type: none"> • = (equal to) • AND • != (not equal to) • >= (greater than or equal to) • <= (less than or equal to) • Nested and/or <p>J-Web also supports Netmask when searching for IP addresses.</p> <p>In the filter text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.</p> <p>The following filters are available:</p> <ul style="list-style-type: none"> • Source IP • Destination IP • Session ID • Log type • User • Application • Source Zone • Destination Zone • Source Country • Destination Country |

Table 15: Fields on the ATP Page (Continued)

| Field | Description |
|------------------|---|
| | <ul style="list-style-type: none"> • Source Port • Destination Port • Protocol |
| X | Click X to clear your search filters. |
| Save Filter | <p>Click Save Filter to save filters after you specify the filtering criteria.</p> <p>To save a filter:</p> <ol style="list-style-type: none"> 1. Enter the filter criteria you are looking for in the advanced search box. 2. Click Save Filter. 3. Enter a name for the filter and click the tick icon to save it. |
| Load Filter | <p>Displays the saved filters list.</p> <p>Hover over the saved filter name to view the query expression. You can delete the saved filter using the delete icon.</p> |
| Time | Displays the time when the ATP log was received. |
| Log Type | Displays the ATP log type: Action, Malware event, SMTP action, and IMAP action. |
| Source Zone | Displays the source zone of the ATP log. |
| Source IP | Displays the source IP address from where the ATP log occurred. |
| Source Port | Displays the port number of the source. |
| User | Displays the username who downloaded the possible malware. |
| Destination Zone | Displays the destination zone of the ATP log. |

Table 15: Fields on the ATP Page (Continued)

| Field | Description |
|------------------|---|
| Destination IP | Displays the destination IP of the ATP log occurred. |
| Destination Port | Displays the destination port of the ATP log. |
| Application | Displays the application name from which the ATP logs are generated. |
| Action | Displays the action taken from the event: log, permit, and log and permit. |
| Session ID | Displays the session ID of the ATP log. |
| Policy | Displays the name of policy that enforced this action. |
| List Hit | Displays the number of times the C&C server has attempted to contact hosts on your network. |
| URL | Displays the accessed URL name that triggered the event. |
| Sample SHA256 | Displays the SHA-256 hash value of the downloaded file. |
| File Hash Lookup | Displays the hash of the file sent for matching against known malware. |
| File Name | Displays the name of the file, including the extension. |
| Protocol | Displays the protocol that the C&C server used to attempt communication. |
| File Category | Displays the type of file. Examples: PDF, executable, document. |
| Hostname | Displays the hostname of device that downloaded the possible malware. |
| Verdict Number | Displays the a score or threat level for a file. |

Table 15: Fields on the ATP Page (Continued)

| Field | Description |
|--------------|---|
| Malware Info | Displays the malware name or brief description. |
| Send To | Displays the email address. |
| Send From | Displays the email address. |
| Tenant ID | Displays the internal unique identifier. |

RELATED DOCUMENTATION

| [Monitor VPN | 90](#)

Monitor VPN

You are here: **Monitor** > **Logs** > **VPN**.

Use the monitoring functionality to view comprehensive stream log details of VPN in a tabular format that includes sortable columns. A VPN provides a means by which remote computers communicate securely across a public WAN such as the Internet.

NOTE: VPN page is available on all the SRX Series Firewalls except the SRX5000 line of devices.

[Table 16 on page 91](#) describes the fields on the VPN page.

Table 16: Fields on the VPN Page

| Field | Description |
|-------------------|---|
| Last | <p>Select the time from the list to view the activity that you are most interested in. Once the time is selected, all of the data presented in your view is refreshed automatically.</p> <p>You can also use Customize to set a custom date and click Apply to view the specified VPN events.</p> |
| Refresh | Click the refresh icon at the upper-right corner to display the fresh content. |
| Show Hide Columns | <p>This icon is represented by three vertical dots.</p> <p>Enables you to show or hide a column in the grid.</p> |
| Export to CSV | <p>You can export the VPN data to a comma-separated value (.csv) file.</p> <p>Select the three vertical dots on the right-side of the page and click Export to CSV. The CSV file is downloaded to your local machine. You can download only maximum of 100 VPN data.</p> |
| Filter Criteria | <p>Use the filter text box present above the table grid. The search includes the logical operators as part of the filter string.</p> <p>NOTE: Starting in Junos OS 23.1R1 Release, J-Web supports the following operators:</p> <ul style="list-style-type: none"> • = (equal to) • AND • != (not equal to) • >= (greater than or equal to) • <= (less than or equal to) • Nested and/or <p>J-Web also supports Netmask when searching for IP addresses.</p> <p>In the filter text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.</p> <p>The available filter option is Log type.</p> |

Table 16: Fields on the VPN Page *(Continued)*

| Field | Description |
|----------------|---|
| X | Click X to clear your search filter. |
| Save Filter | <p>Click Save Filter to save filters after you specify the filtering criteria.</p> <p>To save a filter:</p> <ol style="list-style-type: none"> 1. Enter the filter criteria you are looking for in the advanced search box. 2. Click Save Filter. 3. Enter a name for the filter and click the tick icon to save it. |
| Load Filter | <p>Displays the saved filters list.</p> <p>Hover over the saved filter name to view the query expression. You can delete the saved filter using the delete icon.</p> |
| Time | Displays the time when the VPN log was received. |
| Log Type | <p>Displays the VPN log type:</p> <ul style="list-style-type: none"> • Bad SPI • Replay • PV decryption • PV encryption • PV sm keygen • PV replay • Decrypt bad pad • AUTH fail • D3P ERR |
| Interface Name | Displays the external interface name for the VPN. |

Table 16: Fields on the VPN Page (Continued)

| Field | Description |
|-----------------|--|
| Tunnel ID | Displays the VPN tunnel ID. |
| Source IP | Displays the source IP address from where the VPN connection is established. |
| Destination IP | Displays the destination IP to where the VPN connection is established. |
| Length | Displays the total packet length in Bytes. |
| Type | Displays the VPN type: ESP or AH protocol. |
| Index | Displays the index number of the IKE SA. |
| Sequence Number | Displays the sequence number of the packets sent for the VPN event. |
| Message | Displays the error message for the VPN event. |

RELATED DOCUMENTATION

| [Monitor All Events](#) | 93

Monitor All Events

You are here: **Monitor** > **Logs** > **All Events**.

Use this page to view event details associated with session, content filtering, antispy, antivirus, IPS, screen, security intelligence, Web filtering, ATP, and VPN.

NOTE: All Events page is available on all the SRX Series Firewalls except the SRX5000 line of devices.

Table 17 on page 94 describes the fields on the All Events page.

Table 17: Fields on the All Events Page

| Field | Description |
|-------------------|---|
| Last | <p>Select the time from the list to view the activity that you are most interested in. Once the time is selected, all of the data presented in your view is refreshed automatically.</p> <p>You can also use Customize to set a custom date and click Apply to view the specified event logs.</p> |
| Refresh | <p>Click the refresh icon to get the latest event information.</p> |
| Show Hide Columns | <p>This icon is represented by three vertical dots.</p> <p>Enables you to show or hide a column in the grid.</p> |
| Export to CSV | <p>You can export the event data to a comma-separated value (.csv) file.</p> <p>Select the three vertical dots on the right-side of the page and click Export to CSV. The CSV file is downloaded to your local machine. You can download only maximum of 100 event data.</p> |

Table 17: Fields on the All Events Page (*Continued*)

| Field | Description |
|-----------------|--|
| Filter Criteria | <p>Use the filter text box present above the table grid. The search includes the logical operators as part of the filter string.</p> <p>NOTE: Starting in Junos OS 23.1R1 Release, J-Web supports the following operators:</p> <ul style="list-style-type: none"> • = (equal to) • AND • != (not equal to) • >= (greater than or equal to) • <= (less than or equal to) • Nested and/or <p>J-Web also supports Netmask when searching for IP addresses.</p> <p>In the filter text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.</p> <p>The following filters are available:</p> <ul style="list-style-type: none"> • Source IP • Destination IP • Session ID • Log type • User • Application • Source Zone • Destination Zone • Source Country • Destination Country |

Table 17: Fields on the All Events Page (Continued)

| Field | Description |
|--------------|--|
| | <ul style="list-style-type: none"> • Source Port • Destination Port • Protocol |
| X | Click X to clear your search filter. |
| Save Filter | <p>Click Save Filter to save filters after you specify the filtering criteria.</p> <p>To save a filter:</p> <ol style="list-style-type: none"> 1. Enter the filter criteria you are looking for in the advanced search box. 2. Click Save Filter. 3. Enter a name for the filter and click the tick icon to save it. |
| Load Filter | <p>Displays the saved filters list.</p> <p>Hover over the saved filter name to view the query expression. You can delete the saved filter using the delete icon.</p> |
| View Details | <p>When you hover over the PCAP file, a Detailed View icon appears before the PCAP file. Click the icon to view the log details on the Detailed Log View page.</p> <p>Click on the download icon on the Detailed Log View page to download the packet capture file. If the files are not available, the download fails and you will receive an error message.</p> <p>NOTE: The download icon will only be available for the IPS attack logs and session close logs.</p> |
| PCAP | <p>Click the download icon to download the packet capture file.</p> <p>The PCAP file will be downloaded to your system from the <code>/var/log/pcap/</code> folder. If the files are not available, the download fails and you will receive an error message.</p> <p>NOTE: The download icon will only be available for the IPS attack logs and session close logs.</p> |

Table 17: Fields on the All Events Page (Continued)

| Field | Description |
|----------------------|---|
| Time | Displays the time when the event log was received. |
| Log Type | Displays the event log type. |
| Source Zone | Displays the source zone of the event. |
| Source IP | Displays the source IP address from where the event occurred. |
| Destination Zone | Displays the destination zone of the event. |
| Destination IP | Displays the destination IP of the event occurred. |
| Destination Port | Displays the destination port of the event. |
| Application | Displays the application name for which the event logs are generated. |
| Action | Displays the action taken for the event: warning, allow, and block. |
| Policy | Displays the destination country of the event log. |
| NAT Source IP | Displays the translated (or natted) source IP address. It can contain IPv4 or IPv6 addresses. |
| NAT Source Port | Displays the translated source port. |
| NAT Destination IP | Displays the translated (also called natted) destination IP address. |
| NAT Destination Port | Displays the translated destination port. |
| Protocol | Displays the protocol ID in the event log. |

Table 17: Fields on the All Events Page (Continued)

| Field | Description |
|-----------------------|--|
| Session ID | Displays the traffic session ID of the event log. |
| User | Displays the username from whom the event log is generated. |
| Source Interface | Displays the source interface of the event log. |
| Destination Interface | Displays the destination interface of the event log. |
| Closure Reason | Displays the reason for the log generation. For example, a connection tear down may have an associated reason such as authentication failed. |
| Packets From Client | Displays the number of packets received from the client. |
| Bytes From Client | Displays the number of bytes received from the client. |
| Packets From Server | Displays the number of packets received from the server. |
| Bytes From Server | Displays the number of bytes received from the server. |
| Elapsed Time | Displays the time elapsed since the last time interval began. |
| Source Port | Displays the port number of the source. |
| Sequence Number | Displays the sequence number of the packets sent. |
| Message Type | Displays the message type for the event detected. |
| Count | Displays the number of events count. |
| Severity | Displays the severity of the threat. |

Table 17: Fields on the All Events Page *(Continued)*

| Field | Description |
|------------------|--|
| CVE-ID | Displays the Common Vulnerabilities and Exposures (CVE) identifiers information. |
| Packet log ID | Displays the packets ID received before and after the attack for further offline analysis of attacker behavior. |
| XFF | Displays the X-Forwarded-For (XFF) header added to packets by a proxy server that includes the real IP address of the client making the request. |
| Profile | Displays the event profile name. |
| File Name | Displays the filename of the event log. |
| Argument | Displays the arguments that are passed from the event log. |
| Message | Displays the message ID for negotiation. |
| Bandwidth | Displays the bandwidth utilization for the event log. |
| Malware Info | Displays the malware name or brief description. |
| Hostname | Displays the hostname of device that downloaded the possible malware. |
| File Category | Displays the type of file. Examples: PDF, executable, document. |
| Verdict Number | Displays the a score or threat level for a file. |
| List Hit | Displays the number of times the C&C server has attempted to contact hosts on your network. |
| File Hash Lookup | Displays the hash of the file sent for matching against known malware. |

Table 17: Fields on the All Events Page (Continued)

| Field | Description |
|-------------------|---|
| Sample SHA256 | Displays the SHA-256 hash value of the downloaded file. |
| File Name | Displays the name of the file, including the extension. |
| URL | Displays the accessed URL name that triggered the event. |
| Send To | Displays the email address. |
| Send From | Displays the email address. |
| Category | Displays the threat/event category. |
| Object | Displays the object name of the event log. |
| URL Category Risk | Displays the Web filtering URL category risk level. |
| Virus Name | Displays the detected virus name. |
| Source Name | Displays the name of the source from where event is originated. |
| Feed Name | Displays the feed name of the event detected. |
| Rule | Displays the rule name of the threats/events log. |
| Length | Displays the total packet length in Bytes |
| Type | Displays the event type. |
| Index | Displays the index number of the IKE SA. |

RELATED DOCUMENTATION

Monitor Alarms | 103

Monitor System

You are here: **Monitor** > **Logs** > **System**.

NOTE: Starting in Junos OS Release 23.2R1, J-Web supports new **System** sub-menu under **Monitor** menu. This sub-menu is not supported for SRX300 line of Firewalls and SRX550HM Firewall.

Use this page to view information about system events such as routine operations, failure and error conditions, and emergency or critical conditions.

[Table 18 on page 101](#) describes the fields on the System page.

Table 18: Fields on the System Page

| Field | Description |
|-------------------|--|
| Show logs of file | <p>Select the system log file name to view logs.</p> <p>NOTE: You cannot configure system log message file options using J-Web. To configure the device to log system messages, use the CLI configuration: <code>set system syslog</code>.</p> |
| Duration | <p>Select the time from the list to view the activity that you are most interested in. Once you select the time, all the data presented in your view refreshes automatically.</p> <p>You can also use Customize to set a custom date and click Apply to view the specified system log.</p> <p>By default, grid will show last one hour data from selected syslog file.</p> |

Table 18: Fields on the System Page (Continued)

| Field | Description |
|-----------------|--|
| Refresh | Click the refresh icon to get the latest system logs information. |
| Filter Criteria | <p>In the filter text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.</p> <p>NOTE: Only =(equal to) operator is supported in the filter queries.</p> <p>The following filters are available:</p> <ul style="list-style-type: none"> • Event • Message <p>Click X to clear the search entries.</p> |
| Time | Displays the date and time when the log was received. |
| Event | Displays the name of the event for the log. |
| Message | Displays the message for the log. |
| Process | Displays the process which generates the log. By default, this option is hidden. |
| Detailed View | When you hover over the selected system log file, a Detailed View icon appears before the system log file. Click the icon to view the log details on the System Log Details page. |

RELATED DOCUMENTATION

Monitor All Events | 93

Monitor Alarms

You are here: **Monitor** > **Logs** > **Alarms**.

Use this page to view the alarms details such as time, severity, type, and descriptions of the alarm.

[Table 19 on page 103](#) describes the fields on the Alarms page.

Table 19: Fields on the Alarms Page

| Field | Description |
|------------------------|--|
| Show Hide Columns icon | Enables you to show or hide a column in the grid. |
| Filter Criteria | <p>Enter or select the criteria or parameter on which you want to construct the filter statement.</p> <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. <p>Click X to clear the search entries.</p> |
| Time | Displays the date and time that the alarm was registered. |
| Type | <p>Specifies the type of alarm to monitor:</p> <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. |

Table 19: Fields on the Alarms Page (Continued)

| Field | Description |
|-------------|---|
| Severity | <p>Specifies the alarm severity that you want to monitor</p> <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 | <p>Displays the brief synopsis of the alarms you want to monitor.</p> |

RELATED DOCUMENTATION

| [Monitor Traffic Map](#) | 105

Maps and Charts

IN THIS CHAPTER

- [Monitor Traffic Map | 105](#)
- [Monitor Threats Map | 108](#)
- [Monitor Applications | 115](#)
- [Monitor Users | 118](#)

Monitor Traffic Map

IN THIS SECTION

- [Field Descriptions | 106](#)
- [Tasks You Can Perform | 108](#)

You are here: **Monitor > Maps and Charts > Traffic Map.**

NOTE: Traffic Map page is available on all the SRX Series Firewalls except the SRX5000 line of devices.

J-Web supports monitoring traffic through a map. Use this page to visualize inbound and outbound traffic between geographic regions. You can click or hover over the bubble to view more details on the inbound or outbound traffic. The size of the bubble indicates the session count or the bandwidth utilization for a traffic. Traffic with unknown geographical IP addresses and private IP addresses are displayed as question mark icon and lock icon, respectively.

NOTE: To view the data on the Traffic Map page, ensure that security logging is enabled. If not, go to **Device Administration > Basic Settings > Security Logging** and enable **Stream mode Logging** and **On-box reporting**.

Application Risk Category

The color code of the bubble indicates the risk associated with the application. [Table 20 on page 106](#) shows the application risk categories and the risk values.

Table 20: Application Risk Category and Risk Value

| Application Risk Category | Risk Value |
|---------------------------|--------------------|
| Critical | ≥ 5 |
| High | ≥ 4 and < 5 |
| Unsafe | ≥ 3 and < 4 |
| Moderate | ≥ 2 and < 3 |
| Low | ≥ 0 and < 2 |

You can calculate the average risk value using the following formula:

$$\text{Average risk value for a country} = \text{Application risk total} / \text{Session count total}$$

Field Descriptions

[Table 21 on page 107](#) displays the fields of the Traffic Map page.

Table 21: Fields on the Traffic Map Page

| Field | Description |
|------------------|--|
| By Volume | Displays the bandwidth utilization. This is the default value. |
| By Session | Displays the total number of traffic sessions. |
| Inbound Traffic | Displays the traffic coming through the device from the source countries. |
| Outbound Traffic | Displays the traffic goes through the device to the destination countries. This is the default value. |
| Top Sources | <p>Displays the top 10, 20 (default value), or 50 source countries with the following details:</p> <ul style="list-style-type: none"> • Country—Displays the country name. • Risk level—Displays the risk level category. For example, low, critical, unsafe. • Avg. risk—Displays the average risk count. • Sessions or Bandwidth—Displays the session count or bandwidth utilization. |
| Top Destinations | <p>Displays the top 10, 20 (default value), or 50 destination countries with the following details:</p> <ul style="list-style-type: none"> • Country—Displays the country name. • Risk level—Displays the risk level category. For example, low, critical, unsafe. • Avg. risk—Displays the average risk count. • Sessions or Bandwidth—Displays the session count or bandwidth utilization. |
| View Data | <p>Displays the traffic data for the defined time interval. By default, traffic data for the last five minutes is displayed. You can select the predefined time interval or click Customize to customize the time interval by entering date and time.</p> <p>NOTE: Starting in Junos OS Release 21.4R1, the default duration is changed from Last 1 hour to Last 5 minutes to speed up the J-Web UI loading process.</p> |

Table 21: Fields on the Traffic Map Page (Continued)

| Field | Description |
|--------|--|
| Search | Enter the country name for which you want to view the data and click the search icon. You can view the country flags before the country names. Click on the country name to view its data. |

Tasks You Can Perform

You can perform the following tasks from this page:

- Zoom in and out of the page—Click the zoom in (+) and zoom out (-) icons to zoom in and out of the page.
- Refresh the data on the page—Click the refresh icon available below the zoom out icon.
- Pan the page—Click and drag the mouse to pan the page.
- View country-specific details—Hover over the bubble to view the country specific details.

RELATED DOCUMENTATION

| [Monitor Threats Map](#) | 108

Monitor Threats Map

IN THIS SECTION

- [Field Descriptions](#) | 109
- [Threat Types](#) | 110
- [Tasks You Can Perform](#) | 112

You are here: **Monitor** > **Maps and Charts** > **Threats Map**.

NOTE: Threats Map page is available on all the SRX Series Firewalls except the SRX5000 line of devices.

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 ATP Cloud, 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 **Device Administration > Basic Settings > Security Logging** and enable **Stream mode Logging**.
- Required firewall policy is configured on the device.
- Required licenses are configured for IPS and antivirus.
- Your device is enrolled to the Juniper ATP Cloud 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 are displayed at the upper right and a legend is displayed at the lower 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 22 on page 110](#) displays the fields of the Threats Map (Live) page.

Table 22: 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 > Logs > All Events) page (filtered view of the Grid View tab), where you can view more information about the IPS, virus, spam, Juniper ATP Cloud, and screen events. |
| Threats Blocked & Allowed | Displays the total number of threats blocked and allowed by the following categories: <ul style="list-style-type: none"> • IPS Threats • Virus • Spam • Screen • Juniper ATP Cloud |
| Top Destination Countries | Displays the top five destination countries and the number of threats per country. |
| Top Source Countries | Displays the top five source countries and the number of threats per country. |

Threat Types

The Threats Map page displays blocked and allowed threat events based on feeds from IPS, antivirus, antispam engines, Juniper ATP Cloud, and screen options. [Table 23 on page 111](#) describes different types of threats blocked and allowed.

Table 23: 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 > Logs > Threats 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 > Logs > Threats 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 > Logs > Threats page) includes information about:</p> <ul style="list-style-type: none"> • Specific events names • Specific event names with source country |
| Juniper ATP Cloud | <p>Events that are detected based on Juniper ATP Cloud policies.</p> <p>The information reported about the attack (displayed on the Screen (Monitor > Logs > ATP page) includes information about:</p> <ul style="list-style-type: none"> • Specific events names • Specific event names with either source or destination country |

Table 23: Types of Threats (Continued)

| Attack | Description |
|--------|---|
| Screen | <p>Events that are detected based on screen options.</p> <p>The information reported about the attack (displayed on the Screen (Monitor > Logs > Threats 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 24 on page 112](#) provides more details on the country-specific threat information.

Table 24: Country-Specific Threat Information

| Field | Description |
|---|-------------|
| Displayed in Country-Name pop-up | |

Table 24: Country-Specific Threat Information (Continued)

| Field | Description |
|---|---|
| <i>Number of threat events</i> Threat Events since 12:00 am | Displays the total number of threat events (inbound and outbound) since midnight for that country. |
| Inbound (<i>Number of threat events</i>) | 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. Click View All to view all the destination IP address with threat events count. |
| Outbound (<i>Number of threat events</i>) | 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. Click View All to view all the source IP address with threat events count. |

View Details—Displayed in Country-Name (Details) panel

| | |
|---|--|
| <i>Number of threat events</i> Threat Events since 12:00 am | Displays the total number of threat events (inbound and outbound) since midnight for that country. |
|---|--|

Table 24: 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 ATP Cloud <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 ATP Cloud <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> |

RELATED DOCUMENTATION

| [Monitor Applications](#) | 115

Monitor Applications

You are here: **Monitor** > **Maps and Charts** > **Applications**.

Use this page to view information about bandwidth consumption, session establishment, and 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.

NOTE: Applications page is available on all the SRX Series Firewalls except the SRX5000 line of devices.

NOTE: To view the data on the Applications page, ensure that:

- On-box traffic logging and reporting is enabled. If not, go to **Device Administration** > **Basic Settings** > **Security Logging**, enable **Stream mode Logging** and **On-box Reporting**.
- Logging is enabled for a matching traffic firewall policy. If not, go to **Security Policies & Objects** > **Security Policies** and enable **Logging** options under Rule Options.
- Application tracking is enabled for a security zone. If not, go to **Security Policies & Objects** > **Zones/Screens** and enable **Application Tracking** in the Add Zone page.

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

- **Grid View**—View the comprehensive details of applications in a tabular format that includes sortable columns. You can group the applications using Top users by volume, Top apps by volume, timespan, username, and so on. The table includes information such as the application name, volume, users and so on. [Table 25 on page 116](#) describes the fields on the Grid View page.
- **Chart View**—View a brief summary of all the applications. It shows 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. [Table 26 on page 117](#) describes the widgets on the Chart View page.

Table 25: Applications—Fields on the Grid View Page

| Field | 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. |
| Time Span | Allows you to select a time period. Click Custom to select a preferred date. |
| View App Logs | Enables you to view the application logs. |
| Search | Enables you to search a particular content from the data. |
| 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. |

Table 25: Applications—Fields on the Grid View Page (Continued)

| Field | Description |
|-----------------|--|
| Sub-Category | <p>Subcategory of the application. For example, social networking, news, and advertisements.</p> <p>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.</p> |
| 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> |

Table 26: Applications—Widgets on the Chart View Page

| Field | Description |
|---------------------|---|
| Top 50 Applications | <p>Displays the top 50 application consuming maximum bandwidth in your network.</p> <p>The data is presented graphically as a bubble graph, heat map, or zoomable bubble graph.</p> |
| Show By | <p>Allows you to reorder the bubble graph by bandwidth or by number of sessions from the drop down.</p> <p>If Bandwidth is selected, the size of the bubble depends on the bandwidth used. Whereas, if Number of Session is selected, the size of the bubble depends upon the number of sessions.</p> |
| Time Span | Allows you to select a time. Click Custom to select a preferred date. |
| Group By | Allows you to group the bubble graph by bandwidth or by number of sessions from the drop down based on risk or categories. |

RELATED DOCUMENTATION

Monitor Users | 118

Monitor Users

You are here: **Monitor** > **Maps and Charts** > **Users**.

Use this page to view information about top users accessing high bandwidth-consuming applications and establishing higher number of sessions on your network. Based on this information, network administrators can control the user by rate-limit a device that is accessing applications which consume large bandwidth or create maximum traffic.

NOTE: Users page is available on all the SRX Series Firewalls except the SRX5000 line of devices.

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

- **Grid View**—View the comprehensive details of users in a tabular format that includes sortable columns. You can group the users using Top users by volume, Top apps by volume, timespan, username etc. The table includes information such as the username, volume, top users by volume and so on. [Table 27 on page 118](#) describes the fields on the Grid View page.
- **Chart View**—View a brief summary of all the users. 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. [Table 28 on page 119](#) describes the widgets on the Chart View page.

Table 27: Users—Fields on the Grid View Page

| Field | 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. |
| Time Span | Allows you to select a time period. Click Custom to select a preferred date. |
| Username | Name of a user. |

Table 27: Users—Fields on the Grid View Page (Continued)

| Field | Description |
|----------------|---|
| 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. |
| Search | Enables you to search a particular content from the data. |

Table 28: Users—Widgets on the Chart View Page

| Field | Description |
|--------------|--|
| Top 50 Users | Displays 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. |
| Show By | Allows you to reorder the bubble graph by bandwidth or by number of sessions from the drop down. If Bandwidth is selected, the size of the bubble depends on the bandwidth used. Whereas, if Number of Session is selected, the size of the bubble depends upon the number of sessions. |
| Time Span | Allows you to select a time. Click Custom to select a preferred date. |

RELATED DOCUMENTATION

| [Monitor Threat Prevention](#) | 120

Statistics

IN THIS CHAPTER

- Monitor Threat Prevention | 120
- Monitor VPN Phase I | 122
- Monitor VPN Phase II | 123
- Monitor DNS Security | 125
- Monitor Encrypted Traffic Insights | 127

Monitor Threat Prevention

You are here: **Monitor** > **Statistics** > **Threat Prevention**.

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

[Table 29 on page 120](#) describes the fields on the Threat Prevention page.

Table 29: Fields on the Threat Prevention Page

| Field | Description |
|---|-------------|
| Advanced Anti Malware Session Statistics | |

Table 29: Fields on the Threat Prevention Page *(Continued)*

| Field | Description |
|---|--|
| Sessions | <p>The following options are available:</p> <ul style="list-style-type: none"> • 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 session. |
| Clear Statistics | Clear the statistics. |
| Graph | Shows the anti-malware session statistics. |
| Security Intelligence Session Statistics | |
| Profiles | Select a profile from the list. |
| Sessions | <p>The following options are available:</p> <ul style="list-style-type: none"> • 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. |

RELATED DOCUMENTATION

Monitor VPN Phase I

You are here: **Monitor** > **Statistics** > **Phase I**.

Use this page to view information related to IKE security associations.

[Table 30 on page 122](#) describes the fields on the Phase I page.

Table 30: Fields on the Phase I Page

| Field | Description |
|----------------------------------|--|
| IKE Security Associations | |
| Refresh Interval (sec) | Indicates the duration of time after which you want the data on the page to be refreshed. |
| Refresh | Click the refresh icon at the upper-right corner to display the fresh content. |
| Clear IKE SA | Clears all the IKE SA numbers on the display. |
| SA Index | Index number of a 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. <p>NOTE: A cookie is aimed at protecting the computing resources from attack without spending excessive CPU resources to determine the cookie's authenticity.</p> |

Table 30: Fields on the Phase I Page (*Continued*)

| Field | Description |
|-------|---|
| 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. |

RELATED DOCUMENTATION

| [Monitor VPN Phase II](#) | 123

Monitor VPN Phase II

You are here: **Monitor** > **Statistics** > **Phase II**.

Use this page to view IPsec statistics and information related to IPsec security associations.

[Table 31 on page 123](#) describes the fields on the Phase II page.

Table 31: Fields on the Phase II Page

| Field | Description |
|------------------------|---|
| Statistics | |
| Refresh interval (sec) | Indicates the duration of time after which you want the data on the page to be refreshed. |
| Refresh | Click the refresh icon at the upper-right corner to display the fresh content. |

Table 31: Fields on the Phase II Page (*Continued*)

| Field | Description |
|--|--|
| Clear | Clears all the data on the display page. |
| IPsec Statistics | |
| –Provides details of the IPsec statistics. | |
| Counter | Displays the ESP (encrypted and decrypted bytes), AH (input and output), and errors statistics. |
| Value | Displays the values for the respective statistics. |
| IPsec SA | |
| IPsec Security Associations | |
| ID | Index number of the SA. |
| 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 | Security parameter index (SPI) identifier. A 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. |
| 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- '—' |

Table 31: Fields on the Phase II Page (Continued)

| Field | Description |
|-------|----------------------------|
| Vsys | Specifies the root system. |

RELATED DOCUMENTATION

| [Monitor DHCP Server Bindings](#) | 63

Monitor DNS Security

You are here: **Monitor** > **Statistics** > **DNS Security**.

Domain Name System (DNS) Domain Generation Algorithm (DGA) generates seemingly random domain names that are used as rendezvous points with potential Command & Control (C&C) servers. DNS DGA detection uses machine learning models and known pre-computed DGA domain names to provide domain verdicts, which helps in-line DNS query blocking and sinkholing on SRX Series Firewalls.

Use this page to verify the statistics of DNS sessions, submissions, and ATP latency.

[Table 32 on page 125](#) describes the fields on the DNS Security page.

Table 32: Fields on the DNS Security Page

| Field | Description |
|-----------------------|---|
| DNS Sessions | |
| Cache Hits | Displays the number of cache hits (domain is present in the cache). |
| Cache Misses | Displays the number of cache misses (domain is not present in the cache). |
| Permitted C2 Sessions | Displays the number of permitted C&C (C2) sessions. |

Table 32: Fields on the DNS Security Page (Continued)

| Field | Description |
|------------------------------|--|
| Dropped C2 Sessions | Displays the number of dropped C2 sessions. |
| Sinkholes C2 Sessions | Displays the number of sinkholed C2 sessions. |
| DNS Submissions | |
| Successful Domain Submission | Displays the number of successful domain submissions. |
| Failed Domain Submission | Displays the number of failed domain submissions. |
| Received Safe Verdicts | Displays the number of safe verdicts received by Juniper ATP cloud. |
| Received C2 Verdicts | Displays the number of C2 verdicts received by Juniper ATP cloud. |
| Detected DNS Tunnels | Displays the number of DNS tunnels detected. |
| ATP Latency | |
| Average Latency | Displays the average response time (in milliseconds) that Juniper ATP Cloud takes to provide a verdict to the SRX Series Firewall. |
| Maximum Latency | Displays the maximum response time (in milliseconds) that Juniper ATP Cloud takes to provide a verdict to the SRX Series Firewall. |
| Minimum Latency | Displays the minimum response time (in millisecond) that Juniper ATP Cloud takes to provide a verdict to the SRX Series Firewall. |

RELATED DOCUMENTATION

[Monitor Encrypted Traffic Insights](#) | 127

Monitor Encrypted Traffic Insights

You are here: **Monitor** > **Statistics** > **ETI**.

Encrypted Traffic Insights (ETI) detects malicious threats that are hidden in encrypted traffic without intercepting and decrypting the traffic.

Benefits of Encrypted Traffic Insights

- Monitors network traffic for threats without breaking the encryption of the traffic, thereby adhering to data privacy laws.
- Erases the need for additional hardware or network changes to set up and manage the network.
- Adds an additional layer of protection beyond traditional information security solutions to help organizations reduce and manage risk.
- Ensures no latency as we do not decrypt the traffic.

Use this page to verify the statistics of ETI sessions and submissions.

[Table 33 on page 127](#) describes the fields on the ETI page.

Table 33: Fields on the ETI Page

| Field | Description |
|---------------------|---|
| ETI Sessions | |
| Session Inspected | Displays the number of HTTPS sessions inspected. |
| Session Allowlisted | Displays the number of HTTPS sessions allowlisted for encrypted traffic analysis. |
| Session Detected | Displays the number of HTTPS sessions detected as potentially malicious. |

Table 33: Fields on the ETI Page *(Continued)*

| Field | Description |
|------------------------|--|
| ETI Submissions | |
| Success | Displays the number of HTTPS record submissions that were successfully submitted to Juniper ATP Cloud. |
| Failure | Displays the number of HTTPS record submissions that failed while submitting to Juniper ATP Cloud. |

RELATED DOCUMENTATION

| [Monitor DNS Security](#) | 125

CHAPTER 7

Reports

IN THIS CHAPTER

- [About Reports Page | 129](#)

About Reports Page

IN THIS SECTION

- [Overview | 130](#)
- [Threat Assessment Report | 135](#)
- [Application and User Usage | 135](#)
- [Top Talkers | 136](#)
- [IPS Threat Environment | 136](#)
- [Viruses Blocked | 136](#)
- [URL Report | 137](#)
- [Virus: Top Blocked | 137](#)
- [Top Firewall Events | 137](#)
- [Top Firewall Deny Destinations | 137](#)
- [Top Firewall Denies | 137](#)
- [Top IPS Events | 137](#)
- [Top Anti-spam Detected | 138](#)
- [Top Screen Attackers | 138](#)
- [Top Screen Victims | 138](#)
- [Top Screen Hits | 138](#)
- [Top Firewall Rules | 138](#)
- [Top Firewall Deny Sources | 138](#)

- [Top IPS Attack Sources | 138](#)
- [Top IPS Attack Destinations | 138](#)
- [Top IPS Rules | 138](#)
- [Top Web Apps | 139](#)
- [Top Applications Blocked | 139](#)
- [Top URLs by User | 139](#)
- [Top Source Zone by Volume | 139](#)
- [Top Applications by User | 139](#)
- [Top Botnet Threats By Source Address via IDP Logs | 139](#)
- [Top Botnet Threats by Destination Address via IDP Logs | 139](#)
- [Top Botnet Threats by Threat Severity via IDP Logs | 140](#)
- [Top Malware Threats by Source Address via IDP Logs | 140](#)
- [Top Malware Threats by Destination Address via IDP Logs | 140](#)
- [Top Malware Threats by Threat Severity via IDP Logs | 140](#)
- [Top Blocked Applications via Webfilter Logs | 140](#)
- [Top Permitted Application Subcategories by Volume via Webfilter Logs | 141](#)
- [Top Permitted Application Subcategories by Count via Webfilter Logs | 141](#)

Overview

IN THIS SECTION

- [Generate Reports | 133](#)

You are here: **Monitor** > **Reports**.

Use the Reports menu to generate reports on demand. There are several predefined reports listed in this page, see [Table 34 on page 131](#) . The generated report is displayed in HTML format. You can group multiple reports and generate a consolidated report.

NOTE: Reports page is available on all the SRX Series Firewalls except the SRX5000 line of devices.

Logical system and tenant support the reports listed in [Table 34 on page 131](#) only for SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, and SRX4600.

Table 34: Predefined Group Reports and Supported Users

| Report Name | Root | Logical System Users | Tenant Users Support |
|--------------------------------|------|----------------------|----------------------|
| Threat Assessment Report | Yes | Yes | Yes |
| Application and User Usage | Yes | Yes | Yes |
| Top Talkers | Yes | Yes | Yes |
| IPS Threat Environment | Yes | Yes | No |
| URL Report | Yes | Yes | Yes |
| Viruses Blocked | Yes | Yes | No |
| Virus: Top Blocked | Yes | Yes | No |
| Top Firewall Events | Yes | Yes | Yes |
| Top Firewall Deny Destinations | Yes | Yes | Yes |
| Top Firewall Denies | Yes | Yes | Yes |
| Top IPS Events | Yes | Yes | No |
| Top Anti-spam Detected | Yes | Yes | No |

Table 34: Predefined Group Reports and Supported Users (Continued)

| Report Name | Root | Logical System Users | Tenant Users Support |
|--|------|----------------------|----------------------|
| Top Screen Attackers | Yes | Yes | Yes |
| Top Screen Victims | Yes | Yes | Yes |
| Top Screen Hits | Yes | Yes | Yes |
| Top Firewall Rules | Yes | Yes | Yes |
| Top Firewall Deny Sources | Yes | Yes | Yes |
| Top IPS Attack Sources | Yes | Yes | Yes |
| Top IPS Attack Destinations | Yes | Yes | No |
| Top IPS Rules | Yes | Yes | No |
| Top Web Apps | Yes | Yes | No |
| Top Applications Blocked | Yes | Yes | No |
| Top URLs by User | Yes | Yes | No |
| Top Source Zone by Volume | Yes | Yes | Yes |
| Top Applications by User | Yes | Yes | Yes |
| Top Botnet Threats By Source Address via IDP Logs | Yes | Yes | No |
| Top Botnet Threats by Destination Address via IDP Logs | Yes | Yes | No |

Table 34: Predefined Group Reports and Supported Users (Continued)

| Report Name | Root | Logical System Users | Tenant Users Support |
|--|------|----------------------|----------------------|
| Top Botnet Threats by Threat Severity via IDP Logs | Yes | Yes | No |
| Top Malware Threats by Source Address via IDP Logs | Yes | Yes | No |
| Top Malware Threats by Destination Address via IDP Logs | Yes | Yes | No |
| Top Malware Threats by Threat Severity via IDP Logs | Yes | Yes | No |
| Top Blocked Applications via Webfilter Logs | Yes | Yes | No |
| Top Permitted Application Subcategories by Volume via Webfilter Logs | Yes | Yes | No |
| Top Permitted Application Subcategories by Count via Webfilter Logs | Yes | Yes | No |

Generate Reports

To generate a report:

1. Click **Reports**.
2. Select the predefined report name and click **Generate Report**.

The Report Title window appears.

NOTE: You can select single or multiple report names or all the predefined report names and generate a consolidated report. But you cannot generate group and individual reports at the same time.

3. Complete the configuration according to the guidelines provided in [Table 35 on page 134](#).
4. Click **Save** to save the generated report in the desired location.

A reported is generated. The report includes, the time when it was generated, the table of contents, and the result (a bar graph, a tabular format, and so on). If there is no data available, the report shows, No data to display.

Table 35: Generate Report Settings

| Field | Action |
|---------------|--|
| Name | Enter a name of the report. Maximum 60 characters. |
| Customer Name | Enter a customer name. Default value is Juniper. |
| Description | Enter a description of the report. |
| Show Top | Use the up and down arrow to select the number of records to display in the report. |
| Show Details | <p>Select an option from the list:</p> <ul style="list-style-type: none"> • Top Selected—Displays only the top selected details in the report. • All—Displays all the details in the report. <p>NOTE: It may take a while to generate reports, depending on the device data size.</p> |
| Time Span | Select a predefined time span from the list for the report. |
| From | <p>Specify a start date and time (in MM/DD/YYYY and HH:MM:SS 12-hour or AM/PM formats) to start the report generation.</p> <p>NOTE: This option is available when you choose Custom for Time Span.</p> |
| To | <p>Specify a start date and time (in MM/DD/YYYY and HH:MM:SS 12-hour or AM/PM formats) to stop the report generation.</p> <p>NOTE: This option is available when you choose Custom for Time Span.</p> |

Sorting Options

Table 35: Generate Report Settings (Continued)

| Field | Action |
|--------------|--|
| Show Details | <p>Click the arrow next to Sorting Options and select one of the options from the list:</p> <ul style="list-style-type: none"> • Largest To Smallest—Display reports from largest to smallest details. • Smallest To Largest—Display reports from smallest to largest details. |

Threat Assessment Report

Threat Assessment report contains the following content:

- Executive Summary
- Application Risk Assessment
- Threat & Malware Assessment
- User and Web Access Assessment

The Threat Assessment report displays a new Filename column in the Malware downloaded by User table. This column helps to identify the malware filename.

Application and User Usage

Application and User Usage report contains the following content:

- Top High Risk Applications by Bandwidth
- Top High Risk Applications By Count
- Top Categories By Bandwidth
- Top Applications By Bandwidth
- Top Categories By Count
- Top Applications By Count
- Top Users Of High Risk Applications By Bandwidth
- Top Users By Bandwidth
- High Risk Applications Allowed Per User
- High Risk Applications Blocked Per User

Top Talkers

Top Talkers report contains the following content:

- Top Source IPs by Bandwidth
- Top Destination IPs by Bandwidth
- Top Source IPs by Session
- Top Destination IPs by Session
- Top Users By Bandwidth
- Top Users By Count

IPS Threat Environment

IPS Threat Environment report contains the following content:

- IPS Attacks by Severity Over Time
- Total IPS Attacks by Severity
- Top IPS Categories Blocked
- Top IPS Attacks Blocked
- Top Targeted Hosts by IP
- Top Targeted Hosts by User

NOTE: IPS Threat Environment report is not supported for tenant users.

Viruses Blocked

Viruses Blocked report contains the following content:

- Total Viruses Blocked Over Time
- Top Viruses Blocked

NOTE: Viruses Blocked is not supported for tenant users.

URL Report

URL Report contains the following content:

- Top URLs by Bandwidth
- Top URLs by Count
- Top URL Categories by Bandwidth
- Top URL Categories by Count
- Total URLs Blocked Over Time
- Top Blocked URLs
- Top Blocked URL Categories by Count
- Users With Most Blocked URLs

Virus: Top Blocked

Virus: Top Blocked report contains Virus: Top Blocked content.

NOTE: Virus: Top Blocked is not supported for tenant users.

Top Firewall Events

Top Firewall Events report contains Top Firewall Events.

Top Firewall Deny Destinations

Top Firewall Deny Destinations report contains Top Firewall Deny Destinations.

Top Firewall Denies

Top Firewall Denies report contains Top Firewall Denies.

Top IPS Events

Top IPS Events report contains Top IPS Events.

NOTE: Top IPS Events is not supported for tenant users.

Top Anti-spam Detected

Top Anti-Spam Detected report Top Anti-spam Detected.

NOTE: Top Anti-spam Detected is not supported for tenant users.

Top Screen Attackers

Top Screen Attackers report contains Top Screen Attackers.

Top Screen Victims

Top Screen Victims report contains Top Screen Victims.

Top Screen Hits

Top Screen Hits report contains Top Screen Hits.

Top Firewall Rules

Top Firewall Rules report contains Top Firewall Rules.

Top Firewall Deny Sources

Top Firewall Deny Sources report contains Top Firewall Deny Sources.

Top IPS Attack Sources

Top IPS Attack Sources report contains Top IPS Attack Sources.

Top IPS Attack Destinations

Top IPS Attack Destinations report contains Top IPS Attack Destinations.

NOTE: Top IPS Attack Destinations is not supported for tenant users.

Top IPS Rules

Top IPS Rules report contains Top IPS Rules.

NOTE: Top IPS Rules is not supported for tenant users.

Top Web Apps

Top Web Apps report contains Top Web Apps.

NOTE: Top Web Apps is not supported for tenant users.

Top Applications Blocked

Top Applications Blocked report contains Top Applications Blocked.

NOTE: Top Applications Blocked is not supported for tenant users.

Top URLs by User

Top URLs by User report contains Top URLs by User.

NOTE: Top URLs by User is not supported for tenant users.

Top Source Zone by Volume

Top Source Zone by Volume report contains Top Source Zone by Volume.

Top Applications by User

Top Applications by User report contains Top Applications by User.

Top Botnet Threats By Source Address via IDP Logs

Top Botnet Threats By Source Address via IDP Logs report contains Top Botnet Threats By Source Address via IDP Logs.

NOTE: Top Botnet Threats By Source Address via IDP Logs is not supported for tenant users.

Top Botnet Threats by Destination Address via IDP Logs

Top Botnet Threats by Destination Address via IDP Logs report contains Top Botnet Threats by Destination Address via IDP Logs.

NOTE: Top Botnet Threats by Destination Address via IDP Logs is not supported for tenant users.

Top Botnet Threats by Threat Severity via IDP Logs

Top Botnet Threats by Threat Severity via IDP Logs report contains Top Botnet Threats by Threat Severity via IDP Logs.

NOTE: Top Botnet Threats by Threat Severity via IDP Logs is not supported for tenant users.

Top Malware Threats by Source Address via IDP Logs

Top Malware Threats by Source Address via IDP Logs report contains Top Malware Threats by Source Address via IDP Logs.

NOTE: Top Malware Threats by Source Address via IDP Logs is not supported for tenant users.

Top Malware Threats by Destination Address via IDP Logs

Top Malware Threats by Destination Address via IDP Logs report contains Top Malware Threats by Destination Address via IDP Logs.

NOTE: Top Malware Threats by Destination Address via IDP Logs is not supported for tenant users.

Top Malware Threats by Threat Severity via IDP Logs

Top Malware Threats by Threat Severity via IDP Logs report contains Top Malware Threats by Threat Severity via IDP Logs.

NOTE: Top Malware Threats by Threat Severity via IDP Logs is not supported for tenant users.

Top Blocked Applications via Webfilter Logs

Top Blocked Applications via Webfilter Logs report contains Top Blocked Applications via Webfilter Logs.

NOTE: Top Blocked Applications via Webfilter Logs is not supported for tenant users.

Top Permitted Application Subcategories by Volume via Webfilter Logs

Top Permitted Application Subcategories by Volume via Webfilter Logs report contains Top Permitted Application Subcategories by Volume via Webfilter Logs.

NOTE: Top Permitted Application Subcategories by Volume via Webfilter Logs is not supported for tenant users.

Top Permitted Application Subcategories by Count via Webfilter Logs

Top Permitted Application Subcategories by Count via Webfilter Logs report contains Top Permitted Application Subcategories by Count via Webfilter Logs.

NOTE: Top Permitted Application Subcategories by Count via Webfilter Logs is not supported for tenant users.

5

PART

Device Administration

Basic Settings | 144

Cluster Management | 164

User & Roles | 190

Multi Tenancy—Resource Profiles | 206

Multi Tenancy—Interconnect Ports | 215

Multi Tenancy—Logical Systems | 226

Multi Tenancy—Tenants | 241

Certificates Management—Certificates | 253

Certificate Management—Certificate Authority Group | 281

License Management | 287

Security Package Management | 291

ATP Management | 306

Operations | 312

Software Management | 319

Configuration Management | 323

Alarm Management | 329

RPM | 340

Tools | 355

Reset Configuration | 390

Basic Settings

IN THIS CHAPTER

- [Configure Basic Settings | 144](#)

Configure Basic Settings

You are here: **Device Administration** > **Basic Settings**.

Use this page to configure your device basic settings.

You can do the following:

- **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.
- Starting in Junos OS Release 23.4R1, J-Web supports SRX1600 and SRX2300 Firewalls.

- **Cancel**—Cancels all your entries and returns to the main configuration page.
- **Commit**—Commits all the basic settings configuration and returns to the main configuration page.
- **Expand all**—Click the arrow pointing outwards icon to expand all the options.
- **Collapse all**—Click the arrow pointing inwards to collapse or hide all the options.

[Table 36 on page 145](#) describes the fields on the Basic Settings page.

Table 36: Fields on the Basic Settings Page

| Field | Action |
|------------------------|--|
| System Identity | |
| Hostname | Enter a hostname for the device. |
| Domain name | Enter a domain name to specify the network or subnetwork to which the device belongs. |
| Root password | Enter 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. |
| Confirm root password | Re-enter the password to confirm. |

Table 36: Fields on the Basic Settings Page *(Continued)*

| Field | Action |
|-------------|--|
| DNS servers | <p>Select an option to specify the DNS server settings:</p> <ul style="list-style-type: none"> • To specify a server that the device can use to resolve hostnames into addresses: <ol style="list-style-type: none"> 1. Click + at the upper-right corner of the DNS Servers table. 2. Enter an IPv4 address of the server. 3. Click the tick mark to save the changes. Else, click the cancel (X) icon to discard the changes. • To edit an existing DNS server hostname: <ol style="list-style-type: none"> 1. Select a DNS server hostname that you want to edit. 2. Click the pencil icon at the upper-right corner of the DNS Servers table or right-click on the hostname and edit the IPv4 address. 3. Click the tick mark to save the changes. Else, click the cancel (X) icon to discard the changes. • To remove an existing DNS server hostname, select it and click the delete icon at the upper-right corner of the DNS Servers table or right-click on the hostname and delete it. |

Table 36: Fields on the Basic Settings Page (Continued)

| Field | Action |
|---------------|--|
| Domain search | <p>Select an option:</p> <ul style="list-style-type: none"> • To add a domain name: <ol style="list-style-type: none"> 1. Click + at the upper-right corner of the Domain Search table. 2. Enter a domain name. <p>The string must contain an alphanumeric character and can include underscores, hyphen, slash and dot. No spaces allowed.</p> 3. Click the tick mark to save the changes. Else, click the cancel (X) icon to discard the changes. • To edit an existing domain name: <ol style="list-style-type: none"> 1. Select a domain name that you want to edit. 2. Click the pencil icon at the upper-right corner of the Domain Search table or right-click on the domain name and edit the name. 3. Click the tick mark to save the changes. Else, click the cancel (X) icon to discard the changes. • To remove an existing domain name, select it and click the delete icon at the upper-right corner of the Domain Search table or right-click on the name and delete it. |
| Time | |
| Time zone | Select the time zone from the list in which the router resides. |
| Time source | Select an option from the list to set the system time: |

Table 36: Fields on the Basic Settings Page (Continued)

| Field | Action |
|---------------------|--|
| | <p>NTP Servers—Synchronizes the system time with the NTP server that you select. Click one of the following options:</p> <ul style="list-style-type: none"> • Add—Click + to add an NTP server. Then, enter the NTP server name, key, and Routing Instance. Select an option from the list for Version and Prefer. • Edit—Select an existing NTP server that you want to edit and click the pencil icon available at the upper right of the NTP Server table. You can also right-click on the NTP server and click Edit Row. Then, edit the key and version and click the tick mark. • Delete—Select an existing NTP server that you want to delete and click the delete icon available at the upper right of the NTP Server table. You can also right-click on the NTP server and click Delete Row. Click Yes to delete the selected server. <hr/> <p>Computer—Uses the computer that you are currently logged into to determine the system time for the device.</p> <p>NOTE: When you select this option, the PC time that will be used is displayed in the Current Date & Time field.</p> <hr/> <p>Manual—Enables you to manually select the date and time for the device.</p> <p>Set the date and time using the calendar pick tool and time fields.</p> <p>NOTE: After you configure the time manually, the session will expire. Log in to J-Web.</p> |
| Device date & time | Displays the device date and time. |
| Current date & time | Displays the current date and time. |

Table 36: Fields on the Basic Settings Page (Continued)

| Field | Action |
|--|---|
| Management and Loopback Address | |
| Management address | Enter IPv4 address for the device. |
| Subnet | Enter subnet of the IPv4 address. |
| Loopback address | Enter IP address and subnet for the loopback address. NOTE: If the SRX Series Firewall does not have a dedicated management port (fxp0), then Loopback Address and Subnet are the only options available for the management access configuration. |
| Subnet | Enter the address, for example, 255.255.255.0. You can also specify the address prefix. Specifies the range of logical addresses within the address space that is assigned to an organization. |
| Default gateway | Enter the default gateway address for IPv4. |
| System Services | |
| Telnet | Select this option to enable telnet. |
| SSH | Select this option to enable SSH connections. |
| FTP | Select this option to enable FTP for secure file transfer. |
| NETCONF | Select this option to enable NETCONF connections. |
| Junoscript over SSL | Select this option to enable Junoscript connections over SSL. |

Table 36: Fields on the Basic Settings Page (Continued)

| Field | Action |
|------------------------|--|
| Junoscript certificate | Select the local certificate for SSL from the list. |
| Interface | Select the interface in order of your preference and click on the left arrow/right arrow to add. |
| HTTPS | Select this option to enable HTTPS connection settings. |
| Interface | 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 from the list. |
| PKI certificate | Select the PKI certificate for HTTPS from the list. NOTE: This option is available only if you select pki-local-certificate in the HTTPS Certificate options. |
| Local certificate | Select the local certificate for HTTPS from the list. NOTE: This option is available only if you select local-certificate in the HTTPS Certificate options. |
| HTTPS port | Click up or down arrow to select the TCP ports for incoming HTTP connections. |

Table 36: Fields on the Basic Settings Page (Continued)

| Field | Action |
|-----------------------------|--|
| Virtual domain certificates | <p>Device certificate configured for a domain which can be used for J-Web access.</p> <ul style="list-style-type: none"> • To add a virtual domain certificate: <ol style="list-style-type: none"> 1. Click + at the upper-right corner of the Virtual Domain Certificates table. 2. Enter a virtual domain name and select a device certificate from the list. <p>NOTE: The domain name string must contain an alphanumeric character and can include underscores, hyphen, and dot. No spaces allowed.</p> <ol style="list-style-type: none"> 3. Click the tick mark to save the changes. Else, click the cancel (X) icon to discard the changes. |
| Management URL | Enter the URL path for web management access. |
| Session | Enable to configure the web management session parameters. |
| Idle timeout | Enter a value or click the up or down arrow to set default timeout of web management sessions. |
| Maximum session | Click the up or down arrow to set maximum number of web management sessions allowed. |
| Web API | Select to enable Web API configuration. |
| Client | Select to enable client for the Web API. |

Table 36: Fields on the Basic Settings Page (Continued)

| Field | Action |
|------------|--|
| Hostname | <p>Provides the address of permitted HTTP/HTTPS request originators.</p> <p>To add, click + and enter the IPv4 address of the permitted HTTP/HTTPS request originator and click tick mark to save the changes.</p> <p>To delete, select the hostname and click the delete icon. Then, click Yes to delete it.</p> |
| HTTP | Select to enable unencrypted HTTP connection settings. |
| HTTP port | Click top or bottom arrows to select the TCP ports for incoming HTTP connections. |
| HTTPS | Select to enable encrypted HTTPS connection settings. |
| HTTPS port | Click top or bottom arrows to select the TCP ports for incoming HTTP connections. |

Table 36: Fields on the Basic Settings Page (Continued)

| Field | Action |
|------------------|---|
| Certificate type | <p>Select to specify the certificate that you want to use to secure the connection from the HTTPS certificates list when you enable HTTPs for Web API:</p> <ul style="list-style-type: none"> • Default—Selects the default system generated certificate. • PKI Certificate—Select a PKI certificate from the list for HTTPS of Web API. • File Path: <ul style="list-style-type: none"> • File Path—Click Browse and select a certificate from your desired location. Or click Upload 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 | Select this option to enable user credentials. |
| Name | Enter a username. |
| Password | Enter the user password. |
| REST API | Enable this option to allow RPC execution over HTTP(S) connection. |

Table 36: Fields on the Basic Settings Page (Continued)

| Field | Action |
|------------------|---|
| Explorer | Select this option to enable REST API explorer. |
| Control | Select this option to enable control the REST API process. |
| Allowed sources | <p>Provides the source IP address.</p> <p>Click + and enter the IPv4 address of the source. Then, click tick mark.</p> <p>To delete, select an existing address and click the delete icon. Then, click Yes to delete it.</p> |
| Connection limit | Click top or bottom arrows to select the number of simultaneous connections. |
| HTTP | Select to enable unencrypted HTTP connections for REST API. |
| Address | <p>Click + and enter the IPv4 address for the incoming connections for HTTP of REST API. Then, click tick mark to add it.</p> <p>To delete, select an existing address and click the delete icon. Then, click Yes to delete it.</p> |
| Port | <p>Click top or bottom arrows to select the HTTP port to accept HTTP connections for REST API.</p> <p>NOTE: The default port for HTTP of REST API is 3000.</p> |
| HTTPS | Select to enable encrypted HTTPS connections for REST API. |

Table 36: Fields on the Basic Settings Page (Continued)

| Field | Action |
|--------------------|--|
| Address | <p>Click + and enter the IPv4 address for the incoming connections for HTTPS of REST API. Then, click tick mark to add it.</p> <p>To delete, select an existing address and click the delete icon. Then, click Yes to delete it.</p> |
| Cipher list | <p>Select the Cipher suites in order of your preference and click on the left arrow or right arrow to add.</p> |
| Port | <p>Click top or bottom arrows to select the HTTPS port to accept the HTTPS connection of REST API.</p> <p>NOTE: The default port for HTTPS of REST API is 3443.</p> |
| Server certificate | <p>Select server certificate from the list. See No Link Title to import a device certificate.</p> |

Table 36: Fields on the Basic Settings Page (Continued)

| Field | Action |
|-------------------------|--|
| CA Profile | <p>Select the certificate authority profile for HTTPS of REST API from the list.</p> <p>To create Certificate Authority inline:</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 *—Enter the 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. |
| Security Logging | |
| Stream mode logging | <p>Select this option to enable logging.</p> <p>NOTE: The Enable Traffic Logs option is available for user logical system and tenants.</p> |
| UTC timestamp | <p>Select this option to enable UTC Timestamp for security log timestamps.</p> |

Table 36: Fields on the Basic Settings Page (Continued)

| Field | Action |
|--------------------|--|
| Log on | <p>Select one of the log on types for logging.</p> <ul style="list-style-type: none"> • Source Address—Select this option to enter the source IP address. • Source Interface—Select this option to select a source interface from the list. |
| IP address | <p>Enter the source IP address.</p> <p>NOTE: This option is available if you select the log on type as Source Address.</p> |
| Format | <p>Specifies the format in which the logs are stored.</p> <p>Select a format in which the logs are stored from the list.</p> <ul style="list-style-type: none"> • binary—Binary encoded text to conserve resources. • SD-Syslog—Structured system log file. • Syslog—Traditional system log file. <p>By default, None logging format is selected.</p> |
| Transport protocol | <p>Select an option from the list to specify the type of logging transport protocol:</p> <ul style="list-style-type: none"> • TCP—Select this option to set the transport protocol to TCP. • UDP—Select this option to set the transport protocol to UDP. • TLS—Select this option to set the transport protocol to TLS. <p>By default, None is selected.</p> |

Table 36: Fields on the Basic Settings Page (Continued)

| Field | Action |
|-------------|--|
| Connections | <p>Select the TCP or TLS connections for logging using up and down arrows.</p> <p>NOTE: This option is available if you select the transport protocol option as TCP or TLS.</p> |
| TLS profile | <p>Select a TLS profile from the list.</p> <p>NOTE: This option is available if you select the transport protocol option as TLS.</p> |

Table 36: Fields on the Basic Settings Page (Continued)

| Field | Action |
|------------------|---|
| Syslog server | <p>Enables you to configure syslog servers. You can configure a maximum of three syslog servers.</p> <p>Perform one of the following tasks:</p> <ol 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 list to save the stream. Type—Select a format in which the logs are stored from the 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 the pencil icon. 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 the delete icon. |
| On-box reporting | <p>Enable this option to generate on-box reports.</p> <p>NOTE: We recommend you use Stream mode logging to syslog server.</p> |
| SNMP | |

Table 36: Fields on the Basic Settings Page (Continued)

| Field | Action |
|----------------------|---|
| Contact information | Enter any contact information for the administrator of the system (such as name and phone number). |
| System description | Enter any information that describes the system. |
| Local engine ID | <p>Enter the MAC address of Ethernet management port 0.</p> <p>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.</p> |
| System location | Enter any location information for the system (lab name or rack name, for example). |
| System name override | <p>Specifies the option to override the system hostname.</p> <p>Enter the name of the system.</p> |
| Community | <p>Specifies the name and authorization for the SNMP community.</p> <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. <p>Click tick mark.</p> |
| Trap groups | |

Table 36: Fields on the Basic Settings Page *(Continued)*

| Field | Action |
|------------|--|
| Name | <p>Click + to add a trap group.</p> <p>Enter the SNMP trap group being configured.</p> |
| Categories | <p>Select 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 |
| Targets | <p>Specifies one or more IP addresses that specify the systems to receive SNMP traps that are generated by the trap group being configured.</p> <p>Click +, enter the target IP address for SNMP trap group, and click tick mark.</p> |

Table 36: Fields on the Basic Settings Page (Continued)

| Field | Action |
|-------------------|---|
| Health monitoring | <p>Enable 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 |
| Interval | <p>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.</p> <p>Select a value from 1 through 24855. The default value is 300 seconds.</p> |
| Rising threshold | <p>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.</p> <p>Select a value from 1 through 100. The default value is 90 seconds.</p> |

Table 36: Fields on the Basic Settings Page (Continued)

| Field | Action |
|-------------------|--|
| Falling threshold | <p>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.</p> <p>Select a value 0 through 100. The default value is 80 seconds.</p> |

Redundant PSU

NOTE: SRX380 devices support power supply redundancy for power management.

| | |
|----------------|--|
| Power Supply 0 | Displays if the power supply is present or not. |
| Power Supply 1 | Displays if the redundant power supply is present or not. |
| PSU Redundancy | <p>Enable this option to manage power on the SRX380 device.</p> <p>NOTE: This option is available only when the device is in the standalone mode.</p> |

RELATED DOCUMENTATION

[Reset Configuration and Rerun Setup Wizard | 390](#)

Cluster Management

IN THIS CHAPTER

- [Configure Cluster \(HA\) Setup | 164](#)
- [About the Cluster Configuration Page | 179](#)
- [Edit Node Settings | 182](#)
- [Add an HA Cluster Interface | 183](#)
- [Edit an HA Cluster Interface | 185](#)
- [Delete an HA Cluster Interface | 185](#)
- [Add a Redundancy Group | 186](#)
- [Edit a Redundancy Group | 188](#)
- [Delete a Redundancy Group | 189](#)

Configure Cluster (HA) Setup

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.

You are here: **Device Administration > Cluster Management > Cluster Configuration.**

The Junos OS provides high availability on SRX Series Firewall by using chassis clustering. SRX Series Firewalls 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.

NOTE: Starting in Junos OS Release 23.4R1, J-Web supports SRX1600 and SRX2300 Firewalls.

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 primary 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).

You can set up chassis cluster using a simplified Cluster (HA) Mode wizard when the standalone SRX Series Firewalls are in factory default. You can also create HA using the same wizard from Device Administration > Reset Configuration 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, SRX345, and SRX380 devices to disconnect the ports between the two nodes. This is to avoid displaying the details of the other nodes.

Device Administration > Cluster Management > Cluster Configuration

To set up cluster (HA):

1. Select **Cluster (HA) Setup**.

NOTE: For the secondary node to be set up or if the primary and secondary nodes are not already connected, click **Proceed**. If you want to set up the primary node, then disconnect back to back connected ports between the two nodes and click **Refresh** to reload the browser.

The Setup Chassis Cluster wizard 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 Firewall. 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 37 on page 166](#).

Table 37: 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 primary device in the VRRP group. | Enter a number from 1 through 255. By default, 200 is assigned. |
| Node 1 Priority | Specifies the device priority for being elected to be the primary 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 | | |

Table 37: Primary Unit Configuration (Continued)

| Field | Description | Action |
|--|---|--|
| 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. |

Table 37: Primary Unit Configuration (Continued)

| Field | Description | Action |
|----------------------------|--|--|
| 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. |
| 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.

Table 37: Primary 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 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 37: 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. |

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 38 on page 170](#).

Table 38: Secondary Unit Configuration

| Field | Description | Action |
|-----------------------------------|-------------|--------|
| Secondary Unit Information | | |

Table 38: Secondary Unit Configuration (Continued)

| Field | Description | Action |
|---|--|---|
| 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 38: 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. |

Table 38: Secondary 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) | <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. |

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 **Cluster Management > Cluster (HA) Setup**.

The Cluster Wizard page will open and displays the Cluster Status step.

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 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 39 on page 174](#) .

Table 39: Fabric Link Configuration

| Field | Description | Action |
|----------------------------|--|------------------------------------|
| Fabric Link Details | | |
| 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. | - |

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 40 on page 175](#) .

NOTE: You can also use the pencil icon to edit the reth interface and delete icon to delete the reth interfaces.

Table 40: 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. |

Table 40: Add Reth Interface (Continued)

| Field | Description | Action |
|------------------|---|---------------------------------|
| Periodicity | <p>Optional. Specifies the interval at which the interfaces on the remote side of the link transmit link aggregation control protocol data units (PDUs).</p> <p>Available options are:</p> <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. |
| Redundancy Group | Specifies the number of the redundancy group that the reth interface belongs to. | - |

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 41 on page 176](#) .**Table 41: 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. |

Table 41: Add Reth Logical Interface (Continued)

| Field | Description | Action |
|--------------------------------|--|---------------------------------------|
| 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. |

18. Click **OK**.

19. To configure zones, complete the configuration according to the guidelines provided in [Table 42 on page 178](#).

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.

Table 42: 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. |
| 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. |

Table 42: Create Zones (Continued)

| Field | Description | Action |
|--------------------------------|--|---|
| 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. |

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.

RELATED DOCUMENTATION

[About the Cluster Configuration Page | 179](#)

About the Cluster Configuration Page

IN THIS SECTION

[Tasks You Can Perform | 180](#)

You are here: **Device Administration** > **Cluster Configuration**.

Use this page to add, edit, or delete chassis cluster configuration.

Tasks You Can Perform

You can perform the following tasks from this page:

- Edit Node settings. See ["Edit Node Settings" on page 182](#) .
- Add an HA cluster interface. See ["Add an HA Cluster Interface" on page 183](#) .
- Edit an HA cluster interface. See ["Edit an HA Cluster Interface" on page 185](#) .
- Delete HA cluster interface. See ["Delete an HA Cluster Interface" on page 185](#) .
- Add a redundancy group. See ["Add a Redundancy Group" on page 186](#) .
- Edit a redundancy group. See ["Edit a Redundancy Group" on page 188](#) .
- Delete redundancy group. See ["Delete a Redundancy Group" on page 189](#) .

Field Descriptions

[Table 43 on page 180](#) and [Table 44 on page 181](#) describes the fields on the Cluster Configuration page.

Table 43: Fields on the Node Settings Page

| Field | Description |
|------------|--|
| Node ID | Displays the node ID. |
| Cluster ID | Displays the cluster ID configured for the node. |
| Host Name | Displays the name of the node. |

Table 43: Fields on the Node Settings Page *(Continued)*

| Field | Description |
|----------------------|--|
| Backup Router | Displays the IP address used while booting. |
| Management Interface | Displays the management interface of the node. |
| IP Address | Displays the management IP address of the node. |
| Status | <p>Displays the state of the redundancy group.</p> <ul style="list-style-type: none"> • Primary—Redundancy group is active. • Secondary—Redundancy group is passive. |

Table 44: Fields on the HA Cluster Settings Page

| Field | Action |
|------------------------------|--|
| Interfaces | |
| Global Settings | <p>To configure the global settings:</p> <ol style="list-style-type: none"> 1. Click Global Settings at the upper-right corner of the Interfaces table. The Global Settings window appears. 2. Enter the number of redundant Ethernet (reth) interfaces allowed. Range is 1 through 128. 3. Click OK to save the changes. If you want to discard your changes, click Cancel. |
| 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. |

Table 44: Fields on the HA Cluster Settings Page (Continued)

| Field | Action |
|-------------------------|--|
| Redundancy Group | |
| Group | Displays the redundancy group identification number. |
| Preempt | Displays the selected Preempt option. <ul style="list-style-type: none"> • True–Primary role can be preempted based on priority. • False–Primary role 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. |

Edit Node Settings

You are here: **Device Administration** > **Cluster Configuration**.

To edit node settings:

1. Select a node setting that you want to edit on the Cluster Configuration page.
2. Click the pencil icon available on the upper-right corner of the page.

The Edit Node Settings page appears with editable fields.

Table 45: Fields on the Edit Node Settings Page

| Field | Description |
|----------------------|-----------------------------|
| Node Settings | |
| Host Name | Enter the name of the host. |

Table 45: Fields on the Edit Node Settings Page (Continued)

| Field | Description |
|--------------------|---|
| Backup Router | Enter the backup router address to be used during failover. |
| Destination | |
| IP | Enter the destination IP address. Click + to add the destination IP address or select an existing IP address and click X to delete it. |
| Interface | |
| Interface | Select an interface available for the router from the list. NOTE: You can add and edit two interfaces for each fabric link. |
| IP | Enter the interface IP address. |
| Add | Click + to add the interface. |
| Delete | Select one or more existing interfaces and click X to delete it. |

RELATED DOCUMENTATION

[About the Cluster Configuration Page | 179](#)

Add an HA Cluster Interface

You are here: **Device Administration** > **Cluster Configuration**.

To add an HA cluster interface:

1. Click + on the upper-right corner of the Cluster Configuration page.
The Add HA Cluster Interface page appears.
2. Complete the configuration according to the guidelines provided in [Table 46 on page 184](#).

3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 46: Fields on the Add HA Cluster Interface Page

| Field | Action |
|-----------------------------|---|
| Fabric Link | |
| Fabric Link 0 (fab0) | |
| Interface | Enter the interface IP address for fabric link 0 and click + to add it. Select an existing interface and click X to delete the interface. |
| Fabric Link 1 (fab1) | |
| Interface | Enter the interface IP address for fabric link 1 and click + to add it. Select an existing interface and click X to delete the interface. |
| Redundant Ethernet | |
| Interface | Enter the logical interface. This specifies a logical interface consisting of two physical Ethernet interfaces, one on each chassis. |
| IP | Enter redundant Ethernet IP address. |
| Redundancy Group | Select one of the redundancy group from the list. Else, enter a redundancy group. |
| lacp | Select an option from list: <ul style="list-style-type: none"> • active—Initiate transmission of LACP packets. • passive—Respond to LACP packets. |
| periodic | Select an option from list for periodic transmission of LACP packets. The options are fast or slow. |
| + | Click + to add the redundant Ethernet configuration. |

Table 46: Fields on the Add HA Cluster Interface Page (*Continued*)

| Field | Action |
|-------|--|
| X | Select one or more existing redundant Ethernet configurations and click X to delete it. |

RELATED DOCUMENTATION

[Edit an HA Cluster Interface | 185](#)

[Delete an HA Cluster Interface | 185](#)

[Add a Redundancy Group | 186](#)

Edit an HA Cluster Interface

You are here: **Device Administration** > **Cluster Configuration**.

To edit a HA cluster interface:

1. Select an existing HA cluster interface that you want to edit on the Cluster Configuration page.
2. Click the pencil icon available on the upper-right corner of the page.

The Edit HA Cluster Interface page appears with editable fields. For more information on the options, see "[Add an HA Cluster Interface](#)" on page 183 .

3. Click **Save** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

[About the Cluster Configuration Page | 179](#)

[Delete an HA Cluster Interface | 185](#)

Delete an HA Cluster Interface

You are here: **Device Administration** > **Cluster Configuration**.

To delete HA cluster interface(s):

1. Select one or more existing HA cluster interfaces that you want to edit on the Cluster Configuration page.
2. Click the delete icon available on the upper-right corner of the page.
3. Click **Yes** to delete or click **No** to retain the HA cluster interface.

RELATED DOCUMENTATION

[Add an HA Cluster Interface](#) | 183

[Edit an HA Cluster Interface](#) | 185

Add a Redundancy Group

You are here: **Device Administration** > **Cluster Configuration**.

To add a redundancy group:

1. Click **+** on the upper-right corner of the Cluster Configuration page.
The Add Redundancy Group page appears.
2. Complete the configuration according to the guidelines provided in [Table 47 on page 186](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 47: Fields on the Add Redundancy Group Page

| Field | Action |
|---------------------------------|---|
| Redundancy Group | Enter the redundancy group name. |
| Allow preemption of primaryship | Select the check box to allow 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). |

Table 47: Fields on the Add Redundancy Group Page (Continued)

| Field | Action |
|--------------------------|---|
| Gratuitous ARP Count | <p>Enter a value. The range is 1 through 16. The default is 4.</p> <p>This specifies the number of gratuitous Address Resolution Protocol requests that a newly elected primary sends out on the active redundant Ethernet interface child links to notify network devices of a change in primary role on the redundant Ethernet interface links.</p> |
| node0 priority | <p>Enter the node priority number for a redundancy group.</p> <p>Range: 1 through 254.</p> |
| node1 priority | Enter the node priority number as 1 for a redundancy group. |
| Interface Monitor | |
| Interface | Select an interface from the list. |
| Weight | Enter a value to specify the weight for the interface to be monitored. The range is from 1 through 125. |
| + | Click + to add the interface monitor configuration. |
| X | Select one or more existing interfaces and click X to delete them. |
| IP Monitoring | |
| Weight | Enter a value to specify the weight for IP monitoring. The range is 0 through 225. |
| Threshold | Enter a value to specify the global threshold for IP monitoring. The range is 0 through 225. |
| Retry Count | Enter a value to specify the number of retries needed to declare reachability failure. The range is 5 through 15. |

Table 47: Fields on the Add Redundancy Group Page (Continued)

| Field | Action |
|---------------------------------------|---|
| Retry Interval | Enter a value to specify the time interval in seconds between retries. The range is 1 through 30. |
| IPv4 Addresses to be monitored | |
| IP | Enter an IPv4 address to be monitored for reachability. You select an existing IP address and can click X to delete it. |
| Weight | Enter a value to specify the weight for the redundancy group interface to be monitored. |
| Interface | Enter a value to specify the logical interface to monitor this IP address |
| Secondary IP Address | Enter the secondary IP address for monitoring packets on a secondary link. |
| + | Click + to add the IPv4 Addresses to be monitored configuration. |

RELATED DOCUMENTATION

[Edit a Redundancy Group | 188](#)

[Delete a Redundancy Group | 189](#)

[About the Cluster Configuration Page | 179](#)

Edit a Redundancy Group

You are here: **Device Administration** > **Cluster Configuration**.

To edit a redundancy group:

1. Select an existing redundancy group that you want to edit on the Cluster Configuration page.
2. Click the pencil icon available on the upper-right corner of the page.

The Edit Redundancy Group page appears with editable fields. For more information on the options, see ["Add a Redundancy Group" on page 186](#) .

3. Click **Save** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

[Delete a Redundancy Group | 189](#)

[About the Cluster Configuration Page | 179](#)

Delete a Redundancy Group

You are here: **Device Administration** > **Cluster Configuration**.

To delete redundancy group(s):

1. Select one or more existing redundancy groups that you want to edit on the Cluster Configuration page.
2. Click the delete icon available on the upper-right corner of the page.
3. Click **Yes** to delete or click **No** to retain the redundancy group.

RELATED DOCUMENTATION

[Add a Redundancy Group | 186](#)

[Edit a Redundancy Group | 188](#)

CHAPTER 10

User & Roles

IN THIS CHAPTER

- [About the Users Page | 190](#)
- [Create a User | 192](#)
- [Edit a User | 197](#)
- [Delete a User | 198](#)
- [About the Roles Page | 198](#)
- [Create a Role | 202](#)
- [Edit a Role | 204](#)
- [Delete a User | 204](#)

About the Users Page

IN THIS SECTION

- [Tasks You Can Perform | 190](#)
- [Field Descriptions | 191](#)

You are here: **Device Administration** > **Users & Roles** > **Users**.

Using this page, you can configure user details, authentication methods, and passwords.

Tasks You Can Perform

You can perform the following tasks from this page:

- **Save**—Saves all the users configuration.

- Cancel—Cancels all your entries.
- Add a user. See ["Create a User" on page 192](#) .
- Edit a user. See ["Edit a User" on page 197](#) .
- Delete a user. See ["Delete a User" on page 198](#) .

Field Descriptions

[Table 48 on page 191](#) describes the fields on the Users page.

Table 48: Fields on the Users Page

| Field | Description |
|---------------------------------|---|
| User Details | |
| 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 |
| Authentication Methods | |
| Authentication Method And Order | <p>Enable authentication methods and drag and drop to change the authentication order. The options available are:</p> <ul style="list-style-type: none"> • Password • RADIUS Servers • TACACS+Servers |
| RADIUS Servers | |
| RADIUS Servers | <p>Displays the RADIUS server details. Click Configure to add a new RADIUS server.</p> |

Table 48: Fields on the Users Page (Continued)

| Field | Description |
|--|---|
| TACACS | |
| TACACS Servers | Displays the TACACS server details. Click Configure to add a new TACACS server. |
| Password Settings | |
| NOTE: 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 | Displays the number of old passwords which should not match the new password. Range: 1 through 20 |
| Maximum Lifetime | Displays the duration of a password (in days), where the password expires after the maximum duration is reached. Range: 30 through 365 |
| Minimum Lifetime | Displays the duration of a password (in days) before the password can be changed. Range: 1 through 30 |

RELATED DOCUMENTATION[Create a User | 192](#)[Edit a User | 197](#)[Delete a User | 198](#)**Create a User**You are here: [Device Administration](#)>[Users & Roles](#)>[Users](#).

To add a user:

1. Click **+** on the upper-right corner of the User Details table.
The Create User page appears.
2. Complete the configuration according to the guidelines provided in [Table 49 on page 193](#) .
3. Click **OK** to return to the Users page. If you want to discard your changes, click **Cancel**.
4. Click **Save** to save the newly added user configurations. If you want to discard your changes, click **Cancel**.

Table 49: Fields on the Create User Page

| Field | Description |
|-------------------------|--|
| Username | 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. Range: 100 through 64000. |
| 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. |
| Confirm password | Reenter the password for the user. |

Table 49: Fields on the Create User Page *(Continued)*

| Field | Description |
|---------------------------------|--|
| Role Scope | <p>NOTE: This option is only available on the SRX Series Firewalls that support multi-tenancy.</p> <p>Select one of the role scopes to assign to the user:</p> <ul style="list-style-type: none"> • Default—Assigns the role to root logical systems user. • Tenant—Assigns the role to tenant user. • Logical System—Assigns the role to logical system user. |
| Tenant | <p>Select the tenant profile from the list for which you want to assign the role.</p> <p>NOTE: This option is only available if you select Tenant in the Role scope field.</p> |
| Logical System | <p>Select the logical system profile from the list for which you want to assign the role.</p> <p>NOTE: This option is only available if you select Logical System in the Role scope field.</p> |
| Role | Select the user's role from the list. |
| Authentication Methods | |
| Authentication Method And Order | <p>Enable authentication methods and drag and drop to change the authentication order. The options available are:</p> <ul style="list-style-type: none"> • Password • RADIUS Servers • TACACS+Servers |
| RADIUS Servers | |

Table 49: Fields on the Create User Page *(Continued)*

| Field | Description |
|----------------|---|
| RADIUS Servers | <p>Specifies the details of RADIUS servers.</p> <p>To add a new RADIUS server:</p> <ol style="list-style-type: none"> 1. Click Configure. The RADIUS Servers page appears. 2. Click + and enter the following details: <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 IP Address—Enter the source IP address of the server. • Retry Attempts—Specify the number of times that the server should try to verify the user’s credentials. 3. Click OK to save the changes. <p>To delete an existing RADIUS server, select it and click the Delete icon.</p> |
| TACACS | |

Table 49: Fields on the Create User Page (Continued)

| Field | Description |
|---|--|
| TACACS Servers | <p>Specifies the details of TACACS servers.</p> <p>To add a new TACACS server:</p> <ol style="list-style-type: none"> 1. Click Configure. The TACACS Servers page appears. 2. Click + and enter the following details: <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 IP Address—Enter the source IP address of the server. • Timeout—Specify the amount of time (in seconds) the device should wait for a response from the server. 3. Click OK to save the changes. <p>To delete an existing TACACS server, select it and click the Delete icon.</p> |
| <p>Password Settings</p> <p>NOTE: J-Web interface does not support configuring the number of characters by which the new password should be different from the existing password.</p> | |
| Minimum Reuse | <p>Click up or down arrow to specify the number of old passwords which should not match the new password.</p> <p>Range: 1 through 20</p> |
| Maximum Lifetime | <p>Click up or down arrow to specify the duration of a password (in days), where the password expires after the maximum duration is reached.</p> <p>Range: 30 through 365</p> |

Table 49: Fields on the Create User Page *(Continued)*

| Field | Description |
|------------------|--|
| Minimum Lifetime | <p>Click up or down arrow to specify the duration of a password (in days) before the password can be changed.</p> <p>Range: 1 through 30</p> |

RELATED DOCUMENTATION

[About the Users Page | 190](#)

[Edit a User | 197](#)

[Delete a User | 198](#)

Edit a User

You are here: **Device Administration**>**Users & Roles**>**Users**.

To edit a user:

1. Select an existing user profile that you want to edit on the Users page.
2. Click the pencil icon available on the upper-right corner of the page.
The Edit User page appears with editable fields. For more information on the options, see "[Create a User](#)" on page 192 .
3. Click **OK** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

[About the Users Page | 190](#)

[Create a User | 192](#)

[Edit a User | 197](#)

Delete a User

You are here: **Device Administration**>**Users & Roles**>**Users**.

To delete user(s):

1. Select one or more users that you want to delete from the Users page.
2. Click the delete icon available on the upper-right corner of the page.
3. Click **Yes** to delete or click **No** to retain the user.

RELATED DOCUMENTATION

[About the Users Page | 190](#)

[Create a User | 192](#)

[Edit a User | 197](#)

About the Roles Page

IN THIS SECTION

- [Tasks You Can Perform | 200](#)
- [Field Descriptions | 201](#)

You are here: **Device Administration** > **Users & Roles** > **Roles**.

J-Web supports users' authentication and authorization based on their roles. When root, tenant, or logical-system users log in to J-Web, their roles and access permissions determine the J-Web menus they can access and the tasks they can perform. For logical system and tenant users, the J-Web UI does not display menus for the restricted features.

[Table 50 on page 199](#) lists the details of the user role type, role scope, and access privileges.

Table 50: User Role Type, Role Scope, and Access Privileges

| User Details | Description |
|---|--|
| Role Type | |
| Predefined roles | <p>System-defined roles with a set of predefined access privileges assigned to a user to perform tasks within the J-Web UI. During Junos OS installation, predefined roles (super-user) are generated in the system.</p> <p>NOTE: A device-read-only role is a J-Web specific read-only predefined role. User with this role assigned can only view all the device details in the J-Web UI.</p> |
| Custom roles | <p>Customized (user-defined) roles with a set of access privileges assigned to a user to perform tasks within the J-Web UI. This includes the J-Web UI main menu and first-level sub-menu items (for example, Monitor, Device Administration, and Commit Configuration).</p> <p>NOTE:</p> <ul style="list-style-type: none"> • Users can only create roles if they are user administrators or super administrators, or if they have the create role permission. • You can only create, edit, or delete a customized role but not the predefined roles. • To view the CLI configuration changes before you commit the newly created role, select the role on the Roles page and click Commit> View Configuration Changes. The View Configuration Changes window displays which menus are read-only and hidden, allowed and denied configurations, and for which you have permissions. |
| <p>Role Scope—A role scope defines the capabilities of the user.</p> <p>NOTE: The role scope option is only available on the SRX Series Firewalls that support multi-tenancy.</p> | |
| Default | Users who are assigned with this role scope can view, configure, and manage root logical systems. |

Table 50: User Role Type, Role Scope, and Access Privileges (*Continued*)

| User Details | Description |
|--|---|
| Tenant | Users who are assigned with this role scope view, configure, and manage tenant system. |
| Logical System | Users who are assigned with this role scope view, configure, and manage logical system. |
| Access Privileges —A user role can be assigned with the access privileges and actions to access J-Web UI menus and sub-menus. | |
| Full access | Users can perform all the menu actions. |
| Read-only access | Users have view-only permissions for the respective menus. |
| No access | Users do not have permission to perform the action. |

Tasks You Can Perform

You can perform the following tasks from the Roles page:

- Associate a role to users. To do this, click **Users** link available below the Roles page title to directly navigate to the Users page. Then, click **+** to add a new user with a role or select the existing user and click the pencil icon to modify the role. For more information, see "[Create a User](#)" on page 192 .
- View the details of a role. To do this, select an existing role and follow the available options:
 - Click **More** and select **Detailed View**.
 - Right-click on the selected role and select **Detailed View**.
 - Hover over to the left of the selected role name and click the **Detailed View** icon.
- Create a role. See "[Create a Role](#)" on page 202 .
- Edit a role. See "[Edit a Role](#)" on page 204 .
- Delete a role. See No Link Title.

- Show or hide columns in the Roles table. To do this, click the Show Hide Columns icon in the top right corner of the Roles table. Then, select the options you want to view or clear the options you want to hide on the page.
- Advance search for roles. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

NOTE: You can search only by role name.

For an advanced search:

1. Enter the search string in the text box.
2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.

3. Press Enter to display the search results in the grid.

Field Descriptions

Table 51 on page 201 describes the fields on the Roles page.

Table 51: Fields on the Roles Page

| Field | Action |
|------------|---|
| Name | Displays the name of the role. |
| Role Scope | <p>Displays the role scope. For example, Default, Tenant: <i><tenant-name></i>, and Logical System: <i><logical-system name></i>.</p> <p>NOTE: This option is only available on the SRX Series Firewalls that support multi-tenancy.</p> |

Table 51: Fields on the Roles Page (Continued)

| Field | Action |
|-------------------|--|
| Predefined/Custom | Displays whether the role is a predefined role or a custom role. |

RELATED DOCUMENTATION

| [About the Users Page](#) | 190

Create a Role

You are here: **Device Administration** > **Users & Roles** > **Roles**.

To create a role:

1. Click the add icon (+) on the upper right side of the Roles page.
The Create Role page appears.
2. Complete the configuration according to the guidelines provided in [Table 52 on page 202](#).
3. Click **OK** to save the newly added role. If you want to discard your changes, click **Cancel**.

After you create roles, go to **Device Administration** > **Users & Roles** > **Users** and assign them to users.

Table 52: Fields on the Create Role Page

| Field | Action |
|-------|---|
| Name | Enter a unique string that consists of alphanumeric characters, hyphens, and underscores; 64-character maximum. |

Table 52: Fields on the Create Role Page (Continued)

| Field | Action |
|-------------------|--|
| Role scope | <p>NOTE: This option is only available on the SRX Series Firewalls that support multi-tenancy.</p> <p>Select the scope of the role:</p> <ul style="list-style-type: none"> • Default—Creates the role to root logical systems. • Tenant—Creates the role to tenant profiles. • Logical System—Creates the role to logical system profiles. |
| Tenant | <p>Select the tenant profile from the list for which you want to assign the role.</p> <p>NOTE: This option is only available if you select Tenant in the Role scope.</p> |
| Logical System | <p>Select the logical system profile from the list for which you want to assign the role.</p> <p>NOTE: This option is only available if you select Logical System in the Role scope.</p> |
| Access Privileges | <p>Select one or more privilege types (Full Access, Read-Only Access, or No Access) to assign the role for the specified actions and menus. A role must have at least one access privilege.</p> <p>NOTE: By default, Full Access privilege is selected. You can select:</p> <ul style="list-style-type: none"> • Read-Only Access if you want to assign the access permissions as read-only. • No Access if you do not want to assign any access permissions. |

RELATED DOCUMENTATION

[About the Roles Page | 198](#)

[Edit a Role | 204](#)

No Link Title

Edit a Role

You are here: **Device Administration** > **Users & Roles** > **Roles**.

To edit a role:

1. Select an existing role that you want to edit on the Roles page.

NOTE: Alternatively, you can right-click on the selected role and select **Edit**.

2. Click the pencil icon available on the upper right side of the page.

The Edit Role page appears with editable fields. For more information on the options, see "[Create a Role](#)" on page 202 .

3. Click **OK** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

[About the Roles Page | 198](#)

No Link Title

Delete a User

You are here: **Device Administration**>**Users & Roles**>**Users**.

To delete user(s):

1. Select one or more users that you want to delete from the Users page.
2. Click the delete icon available on the upper-right corner of the page.
3. Click **Yes** to delete or click **No** to retain the user.

RELATED DOCUMENTATION

[About the Users Page | 190](#)

[Create a User | 192](#)

[Edit a User | 197](#)

Multi Tenancy—Resource Profiles

IN THIS CHAPTER

- [About the Resource Profiles Page | 206](#)
- [Global Settings | 208](#)
- [Add a Resource Profile | 209](#)
- [Edit a Resource Profile | 213](#)
- [Delete a Resource Profile | 213](#)

About the Resource Profiles Page

IN THIS SECTION

- [Tasks You Can Perform | 206](#)
- [Field Descriptions | 208](#)

You are here: **Device Administration** > **Multi Tenancy** > **Resource Profiles**.

NOTE: This menu is supported for only SRX4000 Series Firewalls, SRX5000 Series Firewalls, SRX1500, SRX1600, and SRX2300 Firwalls.

You can view Resource profile for logical systems. Resource profiles are mandatory for creating logical systems.

Tasks You Can Perform

You can perform the following tasks from this page:

- Global Settings. See ["Global Settings" on page 208](#) .
- Create a resource profile. See ["Add a Resource Profile" on page 209](#) .
- Edit a resource profile. See ["Edit a Resource Profile" on page 213](#) .
- Delete a resource profile. See ["Delete a Resource Profile" on page 213](#) .
- View the details of a resource profile—To do this, select the resource profile for which you want to view the details and follow the available options:
 - Click **More** and select **Detailed View**.
 - Right-click on the selected resource profile and select **Detailed View**.
 - Mouse over to the left of the selected resource profile and click **Detailed View**.
- Filter the resource profiles based on select criteria. To do this, select the filter icon at the upper-right corner of the Resource Profiles 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 resource profiles table. To do this, click the Show Hide Columns icon in the upper-right corner of the Resource Profiles table and select the options you want to view or deselect the options you want to hide on the page.
- Advance search for resource profiles. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

NOTE: You can search only the resource profile name.

For an advanced search:

1. Enter the search string in the text box.

Based on your input, a list of items from the filter context menu appears.

2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.

3. Press Enter to display the search results in the grid.

Field Descriptions

Table 53 on page 208 describes the fields on the Resource Profiles page.

Table 53: Fields on the Resource Profiles Page

| Field | Description |
|-------------------------|---|
| Profile Name | Displays the resource (security) profile names. |
| Configured Resource | Displays the configured resource(s). |
| Logical Systems/Tenants | Displays the logical system or tenants created. |

RELATED DOCUMENTATION

[Global Settings | 208](#)

[Add a Resource Profile | 209](#)

[Edit a Resource Profile | 213](#)

[Delete a Resource Profile | 213](#)

Global Settings

You are here: **Device Administration** > **Multi Tenancy** > **Resource Profiles**.

To add global settings:

1. Click the **Global Settings** on the upper-right corner of the Resource Profiles page.
The Global Settings page appears.
2. Complete the configuration according to the guidelines provided in [Table 54 on page 209](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 54: Fields on the Global Settings page

| Field | Action |
|------------------|--|
| Enable CPU limit | Enable or disable the CPU limit. |
| CPU Target | Specify the targeted CPU utilization allowed for the whole system (0 through 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 you 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. |

RELATED DOCUMENTATION

[About the Resource Profiles Page | 206](#)

[Add a Resource Profile | 209](#)

[Edit a Resource Profile | 213](#)

[Delete a Resource Profile | 213](#)

Add a Resource Profile

You are here: **Device Administration** > **Multi Tenancy** > **Resource Profiles**.

To add a resource profile:

1. Click **+** available on the upper-right corner of the Resource Profile page.
The Add Resource Profile page appears.
2. Complete the configuration according to the guidelines provided in [Table 55 on page 209](#) .
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 55: Fields on the Add Resource Profile Page

| Field | Description |
|----------------|-------------|
| General | |

Table 55: Fields on the Add Resource Profile Page (Continued)

| Field | Description |
|----------------------------|--|
| Profile Name | Enter a name of the security profile. The string must contain an alphanumeric character and can include underscores; no spaces allowed; 31 characters maximum. |
| IPS Policy | Select the IPS policy from the list. |
| Resource Allocation | |
| nat-pat-portnum | Specify the maximum quantity and the reserved quantity of ports for the logical system as part of its security profile. |
| dslite-softwire-initiator | Specify 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 primary 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 primary administrator can configure for a primary logical system or user logical system when the security profile is bound to the logical systems. |
| nat-interface-port-ol | Specify the number of application firewall rule set configurations that a primary administrator can configure for a primary 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 primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems. |

Table 55: Fields on the Add Resource Profile Page (Continued)

| Field | Description |
|----------------------|---|
| nat-cone-binding | Specify the number of NAT cone binding configurations that user logical system administrators and primary 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 primary 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 primary 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 primary 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 primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems. |
| nat-pat-address | Specify the number of NAT with port address translation (PAT) configurations that user logical system administrators and primary 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 primary 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 primary 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 primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems. |

Table 55: Fields on the Add Resource Profile Page *(Continued)*

| Field | Description |
|----------------------------|--|
| flow-session | Specify the number of flow sessions that user logical system administrators and primary 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 primary 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 primary 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 primary 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 primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems. |
| address-book | Specify the application firewall profile quota of a logical system. |
| 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. |

RELATED DOCUMENTATION

[About the Resource Profiles Page | 206](#)

[Global Settings | 208](#)

[Edit a Resource Profile | 213](#)

[Delete a Resource Profile | 213](#)

Edit a Resource Profile

You are here: **Device Administration** > **Multi Tenancy** > **Resource Profiles**.

To edit a resource profile:

1. Select the existing resource profiles that you want to edit on the Resource Profiles page.
2. Click the pencil icon available on the upper-right corner of the page.

The Edit Resource Profiles page appears with editable fields. For more information on the options, see "[Add a Resource Profile](#)" on page 209 .

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[About the Resource Profiles Page | 206](#)

[Global Settings | 208](#)

[Add a Resource Profile | 209](#)

[Delete a Resource Profile | 213](#)

Delete a Resource Profile

You are here: **Device Administration** > **Multi Tenancy** > **Resource Profile**.

To delete Resource Profile(s):

1. Select the resource profiles that you want to delete on the Resource Profiles page.
2. Click the delete icon available on the upper-right corner of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the Resource Profiles Page | 206](#)

[Global Settings | 208](#)

[Add a Resource Profile | 209](#)

[Edit a Resource Profile | 213](#)

Multi Tenancy—Interconnect Ports

IN THIS CHAPTER

- [About the Interconnect Ports Page | 215](#)
- [Add a LT Logical Interface | 217](#)
- [Edit a LT Logical Interface | 224](#)
- [Delete a Logical Interface | 224](#)
- [Search for Text in an Interconnect Ports Table | 224](#)

About the Interconnect Ports Page

IN THIS SECTION

- [Tasks You Can Perform | 215](#)
- [Field Descriptions | 216](#)

You are here: **Device Administration** > **Multi Tenancy** > **Interconnect Ports**.

On SRX Series Firewalls, 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.

NOTE: This menu is available only for SRX4000 line of devices and SRX5000 line of devices.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a LT Logical Interface. See ["Add a LT Logical Interface" on page 217](#) .
- Edit a LT Logical Interface. See ["Edit a LT Logical Interface" on page 224](#) .
- Delete an Interconnect Interface. See ["Delete a Logical Interface" on page 224](#) .
- Search for Text in an Interconnect Ports table. See ["Search for Text in an Interconnect Ports Table" on page 224](#) .

Field Descriptions

[Table 56 on page 216](#) describes the fields on the Interconnect ports page.

Table 56: Fields on the Interconnect Ports Page

| Field | Description |
|-------------------------|---|
| 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. |

Table 56: Fields on the Interconnect Ports Page *(Continued)*

| Field | Description |
|-----------------------|---|
| Peer Interface | Displays the peer details. |
| Peer Encapsulation | Displays the peer encapsulation mode. |
| Peer LSYS/VPLS Switch | Displays the name of the peer logical system and VPLS Switch. |
| Type | Displays the type for logical interface—Logical System, Tenant, or VPLS Switch. |

RELATED DOCUMENTATION

[Add a LT Logical Interface](#) | 217

Add a LT Logical Interface

You are here: **Device Administration** > **Multi Tenancy** > **Interconnect Ports**.

To add a LT logical interface:

1. Click **+** available on the upper-right corner of the Interconnect Ports page.
The Create LT Logical Interface page appears.
2. Complete the configuration according to the guidelines provided in [Table 57 on page 217](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.
If you click **OK**, a new LT logical interface with the provided configuration is created.

[Table 57 on page 217](#) provides guidelines on using the fields on the Create LT Logical Interface page.

Table 57: Fields on the Create LT Logical Interface Page

| Field | Description |
|-------|-------------|
|-------|-------------|

Local Details

Table 57: Fields on the Create LT Logical Interface Page (*Continued*)

| Field | Description |
|----------------|--|
| Unit | Enter the Logical unit number for interface. |
| Type | Select a logical interface type from the list. The options available are Logical System, Tenant, and VPLS Switch. |
| Logical System | <p>This option is available when you select the logical interface type as Logical System.</p> <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 auto complete the logical system names when you type the partial name.</p> |
| Tenant | <p>This option is available when you select the logical interface type as Tenant.</p> <p>Select a tenant from the list.</p> <p>NOTE: Starting from Junos OS 19.1R1, the user interface will auto complete the tenant names when you type the partial name.</p> |
| VPLS Switch | <p>This option is not available if the logical interface type is VPLS Switch.</p> <p>Select a VPLS switch from the list.</p> |
| Description | Enter description for the interface. |

Table 57: Fields on the Create LT Logical Interface Page (*Continued*)

| Field | Description |
|--------------|---|
| IPv4 Address | <p>NOTE: This option is not available if the logical interface type is VPLS Switch.</p> <p>Specify the IPv4 address.</p> <p>To add an IPv4 address:</p> <ol style="list-style-type: none"> 1. Click + at the upper right of the IPv4 Address table. 2. Enter the following details: <ul style="list-style-type: none"> • IPv4 address—Enter an 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. 3. Click the tick mark to add the IPv4 address or click X to discard the changes. <p>To edit an IPv4 address:</p> <ol style="list-style-type: none"> 1. Select an existing IPv4 address and click the pencil icon at the upper right of the IPv4 Address table. 2. Edit the IPv4 address and prefix length. 3. Click the tick mark to add the IPv4 address or click X to discard the changes. <p>To delete an IPv4 address:</p> <ol style="list-style-type: none"> 1. Select one or more existing IPv4 addresses and click the delete icon at the upper right of the IPv4 Address table. 2. Click OK to delete the IPv4 address. If you want to discard the changes, click Cancel. |

Table 57: Fields on the Create LT Logical Interface Page (*Continued*)

| Field | Description |
|---------------------|---|
| IPv6 Address | <p>NOTE: This option is not available if the logical interface type is VPLS Switch.</p> <p>Specify the IPv6 address.</p> <p>To add an IPv6 address:</p> <ol style="list-style-type: none"> 1. Click + at the upper right of the IPv6 Address table. 2. Enter the following details: <ul style="list-style-type: none"> • IPv6 address—Enter an 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. 3. Click the tick mark to add the IPv6 address or click X to discard the changes. <p>To edit an IPv6 address:</p> <ol style="list-style-type: none"> 1. Select an existing IPv6 address and click the pencil icon at the upper right of the IPv6 Address table. 2. Edit the IPv6 address and prefix length. 3. Click the tick mark to add the IPv6 address or click X to discard the changes. <p>To delete an IPv6 address:</p> <ol style="list-style-type: none"> 1. Select one or more existing IPv6 addresses and click the delete icon at the upper right of the IPv6 Address table. 2. Click OK to delete the IPv6 address. If you want to discard the changes, click Cancel. |
| Peer Details | |
| Type | <p>Select any one of the connection types from the list:</p> <ul style="list-style-type: none"> • Logical system • Tenant • VPLS Switch |

Table 57: Fields on the Create LT Logical Interface Page (Continued)

| Field | Description |
|----------------|---|
| Logical System | <p>This option is available when you select the connection type as Logical System.</p> <p>Select a logical system from the list. If not present in the list, then we need to create a logical system.</p> |
| Tenant | <p>This option is available when you select the connection type as Tenant.</p> <p>Select a tenant from the list.</p> |
| VPLS Switch | <p>This option is available when you select the connection type as VPLS Switch.</p> <p>Select a VPLS switch from the list.</p> |
| Unit | <p>Enter the peering logical system unit number.</p> |
| Description | <p>Specify the interface description.</p> <p>Enter description for the interface.</p> |

Table 57: Fields on the Create LT Logical Interface Page (*Continued*)

| Field | Description |
|--------------|---|
| IPv4 Address | <p>NOTE: This option is not available if the logical interface type is VPLS Switch.</p> <p>Specify the IPv4 address.</p> <p>To add an IPv4 address:</p> <ol style="list-style-type: none"> 1. Click + at the upper right of the IPv4 Address table. 2. Enter the following details: <ul style="list-style-type: none"> • IPv4 address—Enter an 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. 3. Click the tick mark to add the IPv4 address or click X to discard the changes. <p>To edit an IPv4 address:</p> <ol style="list-style-type: none"> 1. Select an existing IPv4 address and click the pencil icon at the upper right of the IPv4 Address table. 2. Edit the IPv4 address and prefix length. 3. Click the tick mark to add the IPv4 address or click X to discard the changes. <p>To delete an IPv4 address:</p> <ol style="list-style-type: none"> 1. Select one or more existing IPv4 addresses and click the delete icon at the upper right of the IPv4 Address table. 2. Click OK to delete the IPv4 address. If you want to discard the changes, click Cancel. |

Table 57: Fields on the Create LT Logical Interface Page (*Continued*)

| Field | Description |
|--------------|---|
| IPv6 Address | <p>NOTE: This option is not available if the logical interface type is VPLS Switch.</p> <p>Specify the IPv6 address.</p> <p>To add an IPv6 address:</p> <ol style="list-style-type: none"> 1. Click + at the upper right of the IPv6 Address table. 2. Enter the following details: <ul style="list-style-type: none"> • IPv6 address—Enter an 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. 3. Click the tick mark to add the IPv6 address or click X to discard the changes. <p>To edit an IPv6 address:</p> <ol style="list-style-type: none"> 1. Select an existing IPv6 address and click the pencil icon at the upper right of the IPv6 Address table. 2. Edit the IPv6 address and prefix length. 3. Click the tick mark to add the IPv6 address or click X to discard the changes. <p>To delete an IPv6 address:</p> <ol style="list-style-type: none"> 1. Select one or more existing IPv6 addresses and click the delete icon at the upper right of the IPv6 Address table. 2. Click OK to delete the IPv6 address. If you want to discard the changes, click Cancel. |

RELATED DOCUMENTATION

[Edit a LT Logical Interface](#) | 224

Edit a LT Logical Interface

You are here: **Device Administration** > **Multi Tenancy** > **Interconnect Ports**.

To edit a LT logical interface:

1. Select an existing logical interface that you want to edit on the Interconnect Ports page.
2. Click the pencil icon available on the upper-right corner of the page.

The Edit LT Logical Interface page appears with editable fields. For more information on the fields, see ["Add a LT Logical Interface" on page 217](#) .

3. Click **OK** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

| [Delete a Logical Interface](#) | 224

Delete a Logical Interface

You are here: **Device Administration** > **Multi Tenancy** > **Interconnect Ports**.

To delete logical interface(s):

1. Select one or more the logical interfaces that you want to delete on the Interconnect Ports page.
2. Click the delete icon available on the upper-right corner of the page.
3. Click **Yes** to delete or click **No** to retain the logical interface.

RELATED DOCUMENTATION

| [Search for Text in an Interconnect Ports Table](#) | 224

Search for Text in an Interconnect Ports Table

You are here: **Device Administration** > **Multi Tenancy** > **Interconnect Ports**.

You can use the search icon in the upper-right corner of the Interconnect Ports page to search for text containing letters and special characters on that page.

To search for text:

1. Click the search icon and enter partial text or full text of the keyword in the search bar.
The search results are displayed.
2. Click **X** next to a search keyword or click **Clear All** to clear the search results.

RELATED DOCUMENTATION

| [About the Interconnect Ports Page | 215](#)

Multi Tenancy—Logical Systems

IN THIS CHAPTER

- [About the Logical Systems Page | 226](#)
- [Add a Logical System | 228](#)
- [Edit a Logical System | 239](#)
- [Delete a Logical System | 240](#)
- [Search Text in Logical Systems Table | 240](#)

About the Logical Systems Page

IN THIS SECTION

- [Tasks You Can Perform | 226](#)
- [Field Descriptions | 227](#)

You are here: **Device Administration** > **Multi Tenancy** > **Logical Systems**.

NOTE: This menu is supported for only SRX4000 Series Firewalls, SRX5000 Series Firewalls, SRX1500, SRX1600, and SRX2300 Firwalls.

Use this page to view, add, and delete Logical System.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a logical system. See ["Add a Logical System" on page 228](#) .
- Edit a logical system. See ["Edit a Logical System" on page 239](#) .
- Delete a logical system. See ["Delete a Logical System" on page 240](#) .
- Search for Text in a logical system table. See ["Search Text in Logical Systems Table" on page 240](#) .
- View the details of the logical systems—To do this, select the logical systems for which you want to view the details and follow the available options:
 - Click **More** and select **Detailed View**.
 - Right-click on the selected tenant and select **Detailed View**.
 - Mouse over to the left of the selected tenant and click **Detailed View**.
- Filter the logical systems based on select criteria. To do this, select the filter icon at the upper-right corner of the logical systems 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 logical systems table. To do this, click the Show Hide Columns icon in the upper-right corner of the logical systems table and select the options you want to view or deselect the options you want to hide on the page.
- Root users can switch to Logical system context. To do this, click **Enter LSYS** on the upper right of the table. See [Table 59 on page 228](#) .

Field Descriptions

[Table 58 on page 227](#) describes the fields on the Logical Systems page.

Table 58: Fields on the Logical Systems Page

| Field | Description |
|---------------------|--|
| 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. |

Table 58: Fields on the Logical Systems Page (Continued)

| Field | Description |
|-------|--|
| Zone | Displays the zone of the resource profile. |

Table 59 on page 228 describes the options on the LSYS page.

Table 59: Enter LSYS Page Options

| Field | Description |
|---------------|--|
| Select Widget | <p>Specifies the following widgets:</p> <ul style="list-style-type: none"> • Logical System Profile. • Logical System CPU Profile. • Logical System FW No Hits. <p>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.</p> |
| Add Tabs | Click + to add a dashboard. |

RELATED DOCUMENTATION

[Add a Logical System | 228](#)

[Edit a Logical System | 239](#)

[Delete a Logical System | 240](#)

[Search Text in Logical Systems Table | 240](#)

Add a Logical System

You are here: **Device Administration** > **Multi Tenancy** > **Logical Systems**.

To add a logical system:

1. Click **+** available on the upper-right corner of the Logical Systems page.
The Create Logical Systems page appears.
2. Complete the configuration according to the guidelines provided in [Table 60 on page 229](#) .
3. Click **Finish** to save the changes. If you want to discard your changes, click **Cancel**.

Table 60: Fields on the Add Logical Systems Page

| Field | Description |
|---|---|
| General Details | |
| Name | <p>Enter a logical system name of a selected Resource Profile. Only one Resource Profile can be selected, per logical system.</p> <p>The string must contain alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed; maximum length is 63 characters.</p> |
| Logical System Resource Profile | |
| 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 | <p>Enter a name of the security profile.</p> <p>The string must contain an alphanumeric character and can include underscores; no spaces allowed; 31 characters maximum.</p> |
| IPS Policy | Select an IPS policy from the list. |
| Resource Allocation | |

Table 60: Fields on the Add Logical Systems Page (Continued)

| Field | Description |
|---------------|---|
| Resource Name | <p data-bbox="513 363 808 390">Displays the resource name.</p> <ul style="list-style-type: none"> <li data-bbox="513 426 1369 489">• nat-pat-portnum—Specify the maximum quantity and the reserved quantity of ports for the logical system as part of its security profile. <li data-bbox="513 525 1360 625">• dslite-softwire-initiator—Specify 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 primary logical system. <li data-bbox="513 661 1401 724">• cpu—Specify the percentage of CPU utilization that is always available to a logical system. <li data-bbox="513 760 1390 861">• appfw-rule—Specify the number of application firewall rule configurations that a primary administrator can configure for a primary logical system or user logical system when the security profile is bound to the logical systems. <li data-bbox="513 896 1360 1035">• nat-interface-port-ol—Specify the number of application firewall rule set configurations that a primary administrator can configure for a primary logical system or user logical system when the security profile is bound to the logical systems. <li data-bbox="513 1071 1382 1134">• nat-rule-referenced-prefix—Specify the security NAT interface port overloading the quota of a logical system. <li data-bbox="513 1169 1393 1308">• nat-port-ol-ipnumber—Specify the number of NAT port overloading IP number configurations that user logical system administrators and primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems. <li data-bbox="513 1344 1386 1482">• nat-cone-binding—Specify the number of NAT cone binding configurations that user logical system administrators and primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems. <li data-bbox="513 1518 1369 1659">• nat-static-rule—Specify the number of NAT static rule configurations that user logical system administrators and primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems. <li data-bbox="513 1694 1393 1757">• nat-destination-rule—Specify the number of NAT destination rule configurations that user logical system administrators and primary logical system administrators |

Table 60: Fields on the Add Logical Systems Page (Continued)

| Field | Description |
|-------|--|
| | <p>can configure for their logical systems if the security profile is bound to the logical systems.</p> <ul style="list-style-type: none"> • nat-source-rule—Specify the NAT source rule configurations that user logical system administrators and primary 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 primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems. • nat-pat-address—Specify the number of NAT with port address translation (PAT) configurations that user logical system administrators and primary 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 primary 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 primary 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 primary 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 primary 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 primary 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. |

Table 60: Fields on the Add Logical Systems Page (Continued)

| Field | Description |
|------------------|--|
| | <ul style="list-style-type: none"> • scheduler—Specify the number of schedulers that user logical system administrators and primary 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 primary 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 primary logical system administrators can configure for their logical systems if the security profile is bound to the logical systems. • 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. |
| Range | Display range for each resource. |
| Edit | Select a resource and click on the pencil icon to edit Reserved and Maximum fields. |
| Reserved | Specify reserved quota that guarantees that the resource amount specified is always available to the logical system. |
| Maximum | Specify the maximum allowed quota. |
| IPS Max Sessions | Enter maximum number of sessions. Use up and down arrow keys to increase or decrease the number. |

Users

Click one:

- Add icon (+)—Create users.
- Edit icon (/)—Edit the selected users.
- Delete icon (X)—Delete the selected users.

Table 60: Fields on the Add Logical Systems Page (Continued)

| Field | Description |
|--------------------------|---|
| Create-Edit users | |
| Username | Enter a username. Maximum length is 64 characters. |
| Role | <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> |
| Password | Enter a password for the user which is more than 6 characters but less than 128 characters. |
| Confirm Password | Re-enter the new password to confirm. |

Interfaces

Click One:

- **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**General**

| | |
|-------------------------|--|
| Physical Interface Name | Displays the name of the Physical Interface. |
| Logical Interface Unit | Enter the logical Interface Unit |

Table 60: Fields on the Add Logical Systems Page (Continued)

| Field | Description |
|---|--|
| Description | Enter the description. |
| VLAN ID | Enter the VLAN ID. VLAN ID is mandatory. |
| IPv4 Address | |
| IPv4 Address | Click + and enter a valid IP address. |
| Subnet Mask | Enter a valid subnet mask. |
| Delete | Select the IPv4 address and click the delete icon to delete the address. |
| IPv6 Address | |
| IPv6 Address | Enter a valid IP address. |
| Subnet Mask | Enter a valid subnet mask. |
| Delete | Select the IPv6 address and click the delete icon to delete the address. |
| Zones | |
| Click One: | |
| <ul style="list-style-type: none"> • Add icon (+)—Create security zones. • Edit icon (/)—Edit the selected security zones. • Delete icon (X)—Delete the selected security zone. • Search icon—Search for a security zone. | |
| Create-Edit Security Zones | |
| General | |

Table 60: Fields on the Add Logical Systems Page (Continued)

| Field | Description |
|----------------------|---|
| Name | Enter a valid name of the zone. |
| Description | Enter a description of the zone. |
| Application Tracking | Enables the application tracking support. |
| Source Identity Log | Enable source identity log for this zone. |
| Interfaces | Select an interface from the Available column and move it to Selected column. |
| Selected interfaces | Displays the selected interfaces. |

Table 60: Fields on the Add Logical Systems Page (Continued)

| Field | Description |
|-----------------|---|
| System Services | <p>Select system services from the following options:</p> <p>NOTE: Select the Except check box to allow services other than the selected services.</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. |

Table 60: Fields on the Add Logical Systems Page (*Continued*)

| Field | Description |
|-------|--|
| | <ul style="list-style-type: none"> • 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. • 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. |

Table 60: Fields on the Add Logical Systems Page (Continued)

| Field | Description |
|-------------------------|--|
| Protocols | <p>Select a protocol from the following options:</p> <p>NOTE: Select the Except check box to allow protocols other than the selected protocols.</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 | Enable this option to send RST for NON-SYN packet not matching TCP session. |

RELATED DOCUMENTATION

[About the Logical Systems Page | 226](#)

[Add a Logical System | 228](#)

[Edit a Logical System | 239](#)

[Delete a Logical System | 240](#)

[Search Text in Logical Systems Table | 240](#)

Edit a Logical System

You are here: **Device Administration** > **Multi Tenancy** > **Logical Systems**.

To edit a logical system profile:

1. Select the existing logical system profile that you want to edit on the Logical System Profile page.
2. Click the pencil icon available on the upper-right corner of the page.

The Edit a Logical System Profile page appears with editable fields. For more information on the options, see "[Add a Logical System](#)" on [page 228](#) .

NOTE: Starting in Junos OS 22.3R1 release, you can assign the customized user role to the logical systems users. To do that:

- a. Select an existing logical system profile and click the pencil icon.
- b. Expand User Details and click +.
The Create User page appears.
- c. Select the logical systems customized role from the list in the Role field.
- d. Click **OK**.

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[About the Logical Systems Page | 226](#)

[Add a Logical System | 228](#)

[Delete a Logical System | 240](#)

[Search Text in Logical Systems Table | 240](#)

Delete a Logical System

You are here: **Device Administration** > **Multi Tenancy** > **Logical Systems**.

To delete a logical system:

1. Select the logical system that you want to delete on the Logical System page.
2. Click the delete icon available on the upper-right corner of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the Logical Systems Page | 226](#)

[Add a Logical System | 228](#)

[Edit a Logical System | 239](#)

[Search Text in Logical Systems Table | 240](#)

Search Text in Logical Systems Table

You are here: **Device Administration** > **Multi Tenancy** > **Logical Systems**.

You can use the search icon in the upper-right corner of a page to search for text containing letters and special characters on that page.

To search for text:

1. Click the search icon and enter a partial text or full text of the keyword in the search bar and execute.
The search results are displayed.
2. Click **X** next to a search keyword or click **Clear All** to clear the search results.

RELATED DOCUMENTATION

[About the Logical Systems Page | 226](#)

[Add a Logical System | 228](#)

[Edit a Logical System | 239](#)

[Delete a Logical System | 240](#)

Multi Tenancy—Tenants

IN THIS CHAPTER

- [About the Tenants Page | 241](#)
- [Add a Tenant | 243](#)
- [Edit a Tenant | 251](#)
- [Delete a Tenant | 251](#)
- [Search Text in Tenants Table | 252](#)

About the Tenants Page

IN THIS SECTION

- [Tasks You Can Perform | 241](#)
- [Field Descriptions | 242](#)

You are here: **Device Administration** > **Multi Tenancy** > **Tenants**.

You can use this page to add, view, and delete Tenants.

NOTE: This menu is supported for only SRX4000 Series Firewalls, SRX5000 Series Firewalls, SRX1500, SRX1600, and SRX2300 Firewalls.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a tenant. See ["Add a Tenant" on page 243](#).

- Edit a tenant. See ["Edit a Tenant" on page 251](#) .
- Delete a tenant. See ["Delete a Tenant" on page 251](#) .
- Search for Text in a tenants table. See ["Search Text in Tenants Table" on page 252](#) .
- View the details of the tenants—To do this, select the tenant for which you want to view the details and follow the available options:
 - Click **More** and select **Detailed View**.
 - Right-click on the selected tenant and select **Detailed View**.
 - Mouse over to the left of the selected tenant and click **Detailed View**.
- Filter the tenant based on select criteria. To do this, select the filter icon at the upper-right corner of the tenant 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 tenant table. To do this, click the Show Hide Columns icon in the upper-right corner of the tenant table and select the options you want to view or deselect the options you want to hide on the page.

Field Descriptions

[Table 61 on page 242](#) describes the fields on the Tenants page.

Table 61: Fields on the Tenants Page

| Field | Description |
|---------------------|---|
| 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. |

RELATED DOCUMENTATION

[Add a Tenant | 243](#)

[Edit a Tenant | 251](#)

[Delete a Tenant | 251](#)

[Search Text in Tenants Table | 252](#)

Add a Tenant

You are here: **Device Administration** > **Multi Tenancy** > **Tenants**.

To add a tenant:

1. Click **+** available on the upper-right corner of the Tenants page.
The Create Tenant page appears.
2. Complete the configuration according to the guidelines provided in [Table 62 on page 243](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 62: Fields on the Create Tenant Page

| Field | Description |
|--------------------------------|---|
| 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 | |
| Profile Name | Displays the name of the resource profile. |
| Configured Resources | Displays the resources and its reserved or maximum quantity assigned for this resource profile. |

Table 62: Fields on the Create Tenant Page (Continued)

| Field | Description |
|-------------------------|--|
| 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 ["Add a Resource Profile" on page 209](#) 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

| | |
|----------|---|
| Username | Enter a username. Maximum length is 64 characters. |
|----------|---|

Table 62: Fields on the Create Tenant Page (*Continued*)

| Field | Description |
|------------------|--|
| Role | <p>Select an option from the list to specify the role of the user:</p> <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> |
| Password | Specify the password for the user. |
| Confirm Password | Confirm the password. |

Assign Interfaces

Only one logical interface can be part of one tenant, whereas a tenant can have multiple logical interfaces.

Click One:

- **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

General

| | |
|-------------------------|--|
| Physical Interface Name | Displays the name of the Physical Interface. |
| Logical Interface Unit | Enter the logical interface unit. |
| Description | Enter the description. |
| VLAN ID | Enter the VLAN ID. VLAN ID is mandatory. |

Table 62: Fields on the Create Tenant Page (Continued)

| Field | Description |
|---|--|
| IPV4 Address | |
| IPV4 Address | Click + and enter a valid IP address. |
| Subnet Mask | Enter a valid subnet mask. |
| Delete | Select the IPv4 address and click the delete icon to delete the address. |
| IPV6 Address | |
| IPV6 Address | Enter a valid IP address. |
| Subnet Mask | Enter a valid subnet mask. |
| Delete | Select the IPv6 address and click the delete icon to delete the address. |
| Zone Configuration | |
| Click One: | |
| <ul style="list-style-type: none"> • Add icon (+) – Create security zones. • Edit icon (/) –Edit the selected security zones. • Delete icon (X)–Delete the selected security zone. • Search - Search for a security zone. | |
| Create-Edit Security Zones | |
| General | |
| Name | Enter a valid name of the zone. |
| Description | Enter a description of the zone. |

Table 62: Fields on the Create Tenant Page (Continued)

| Field | Description |
|----------------------|---|
| Application Tracking | Enables the application tracking support. |
| Source Identity Log | Enable source identity log for this zone. |
| Interfaces | Select an interface from the Available column and move it to Selected column. |
| Selected interfaces | Displays the selected interfaces. |

Table 62: Fields on the Create Tenant Page (*Continued*)

| Field | Description |
|-------------------------|---|
| System Services Options | <p>Select system services from the following options:</p> <p>NOTE: Select the Except check box to allow services other than the selected services.</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. |

Table 62: Fields on the Create Tenant Page (*Continued*)

| Field | Description |
|-------|--|
| | <ul style="list-style-type: none"> • 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. • 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. |

Table 62: Fields on the Create Tenant Page (*Continued*)

| Field | Description |
|-------------------------|---|
| Protocols | <p>Select a protocol from the following options:</p> <p>NOTE: Select the Except check box to allow protocols other than the selected protocols.</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 | Enable this option to send RST for NON-SYN packet not matching TCP session. |

RELATED DOCUMENTATION

[About the Tenants Page | 241](#)

[Edit a Tenant | 251](#)

[Delete a Tenant | 251](#)

[Search Text in Tenants Table | 252](#)

Edit a Tenant

You are here: **Device Administration** > **Multi Tenancy** > **Tenants**.

To edit a tenant:

1. Select the existing tenant that you want to edit on the Tenants page.
2. Click the pencil icon available on the upper-right corner of the page.

The Edit a Tenant page appears with editable fields. For more information on the options, see "[Add a Tenant](#)" on page 243 .

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[About the Tenants Page | 241](#)

[Add a Tenant | 243](#)

[Delete a Tenant | 251](#)

[Search Text in Tenants Table | 252](#)

Delete a Tenant

You are here: **Device Administration** > **Multi Tenancy** > **Tenants**.

To delete tenant(s):

1. Select one or more existing tenants that you want to delete on the Tenants page.
2. Click the delete icon available on the upper-right corner of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the Tenants Page | 241](#)

[Add a Tenant | 243](#)

[Edit a Tenant | 251](#)

[Search Text in Tenants Table | 252](#)

Search Text in Tenants Table

You are here: **Device Administration** > **Multi Tenancy** > **Tenants**.

You can use the search icon in the upper-right corner of a page to search for text containing letters and special characters on that page.

To search for text:

1. Click the search icon and enter a partial text or full text of the keyword in the search bar and execute. The search results are displayed.
2. Click **X** next to a search keyword or click **Clear All** to clear the search results.

RELATED DOCUMENTATION

[About the Tenants Page | 241](#)

[Add a Tenant | 243](#)

[Edit a Tenant | 251](#)

[Delete a Tenant | 251](#)

Certificates Management—Certificates

IN THIS CHAPTER

- [About the Certificates page | 253](#)
- [Create a Device Certificate | 255](#)
- [Add a Certificate Authority \(CA\) | 270](#)
- [Export a Device Certificate | 274](#)
- [Edit a CA Certificate | 275](#)
- [Delete a Certificate | 275](#)
- [Search Text in the Certificates Table | 276](#)
- [Re-Enroll a Device Certificate | 276](#)
- [Load CA Certificate | 277](#)
- [Reload CA Certificate | 279](#)

About the Certificates page

You are here: **Device Administration** > **Certificate Management** > **Certificates**.

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.

You can perform the following tasks:

- View the page by device certificates, certificate authorities (CA), or all.
- Export a device certificate or CSR from the default location to a specific location in your local machine. See [Export a Device Certificate](#) "[Export a Device Certificate](#)" on page 274 .
- Create a device certificate or a CA. Click **Create** available on the upper-right corner of the Certificates page and select **Device Certificates** or **Certificate Authority**.

For more information, see ["Create a Device Certificate" on page 255](#) and ["Add a Certificate Authority \(CA\)" on page 270](#).

- View the details of a certificate. View the details of a certificate—To do this, select the certificate of which you want to view the details and follow the available options:
 - Click **More** and select **Detailed View**.
 - Right-click on the selected certificate and select **Detailed View**.
 - Mouse over to the left of the selected certificate and click **Detailed View**.
- Edit a CA certificate. See ["Edit a CA Certificate" on page 275](#).
- Delete a certificate. See ["Delete a Certificate" on page 275](#).
- Refresh the Certificates page.
- Search for text in a certificate table. See ["Search Text in the Certificates Table" on page 276](#).
- Filter the certificates information based on select criteria. To do this, select the filter icon at the upper-right 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 Certificates table. To do this, use the **Show Hide Columns** icon in the upper-right corner of the page and select the options you want to show or deselect to hide options on the page.

[Table 63 on page 254](#) provides the details of the fields on the Certificates page.

Table 63: Fields on the Certificates Page

| Field | Action |
|---------------------|--|
| Name | Displays the certificate name. |
| Certificate Chain | Displays an ordered list of certificates, containing a certificate chain name. For example, ROOT CA. This enables receiver to verify that the sender and all CA's are trustworthy. |
| Type | Displays the certificate type. |
| Issuer Organization | Displays the details of the authority that issued the certificate. |

Table 63: Fields on the Certificates Page (Continued)

| Field | Action |
|-------------------|---|
| Status | <p>Displays whether the status of the certificate is valid, expired, and so on.</p> <p>You can also:</p> <ol style="list-style-type: none"> 1. Renew a Local Self-Signed device certificate. 2. Re-enroll an already enrolled device certificate. See "Re-Enroll a Device Certificate" on page 276 . 3. Load a CA certificate. See "Load CA Certificate" on page 277 . 4. Re-load a CA certificate. See "Reload CA Certificate" on page 279 . |
| Expiry Date | Displays certificate expiry date. |
| Digital Signature | Displays the digital signature associated with the certificate. |

Create a Device Certificate

IN THIS SECTION

- [Create Device Certificate \(Let's Encrypt\) | 256](#)
- [Create Device Certificate \(Local Self-Signed\) | 257](#)
- [Create Device Certificate \(SCEP\) | 260](#)
- [Create Device Certificate \(ACME\) | 262](#)
- [Create Device Certificate \(CMPv2\) | 264](#)
- [Create Device Certificate \(CSR\) | 266](#)
- [Load Signed Device Certificate \(Externally Generated\) | 269](#)

You are here: **Device Administration** > **Certificate Management** > **Certificates**.

The device certificate options available are:

- Let's Encrypt. See ["Create Device Certificate \(Let's Encrypt\)" on page 256](#) .
- Local Self-Signed. See ["Create Device Certificate \(Local Self-Signed\)" on page 257](#) .
- SCEP. See ["Create Device Certificate \(SCEP\)" on page 260](#) .
- ACME. See ["Create Device Certificate \(ACME\)" on page 262](#) .
- CMPv2. See ["Create Device Certificate \(CMPv2\)" on page 264](#) .
- CSR. See ["Create Device Certificate \(CSR\)" on page 266](#) .
- Externally Generated. See ["Load Signed Device Certificate \(Externally Generated\)" on page 269](#) .

Create Device Certificate (Let's Encrypt)

You are here: **Device Administration** > **Certificate Management** > **Certificates**.

To create a let's encrypt device certificate:

1. Click **Create** available on the upper-right corner of the Certificates page.
2. Click **Device Certificate** and select **Let's Encrypt**.
The Create Device Certificate (Let's Encrypt) page appears.
3. Select **I agree to the Let's encrypt subscriber terms and conditions**.
4. Complete the configuration according to the guidelines provided in [Table 64 on page 256](#) .
5. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.
If you click **OK**, a new device certificate with the provided configuration is created.

Table 64: Fields on the Create Device Certificate (Let's Encrypt) page

| Field | Action |
|---------------------|---|
| CA certificate name | Select one of the CA certificate names from the list or click Add CA certificate to add a new CA Certificate. For details on adding a CA certificate, see "Add CA Certificate" on page 270 . |
| Digital signature | Select a digital signature from the list. That is, RSA-1024, RSA-2048, or RSA-4096. By default, RSA-2048 is selected. |
| Name | Enter a certificate name. |

Table 64: Fields on the Create Device Certificate (Let's Encrypt) page *(Continued)*

| Field | Action |
|---------------------------|---|
| Contact email | Enter contact email address. |
| Auto re-enrollment | |
| Trigger time | Set the auto re-enrollment trigger time (in days). Default is 65 days and maximum trigger time of 85 days is allowed. |
| Re-generate key pair | Enable this option to automatically generate a new key pair when a device certificate is automatically re-enrolled. |
| Subject Alt Name | |
| Domain names | Click + to add new domain name that you want to associate with the certificate. This can be an FQDN that resolves to an SRX Series Firewall external IP address. Maximum of domain names allowed is five. |

RELATED DOCUMENTATION

[About the Certificates page | 253](#)

[Add CA Certificate | 270](#)

[Create Device Certificate \(Local Self-Signed\) | 257](#)

Create Device Certificate (Local Self-Signed)

You are here: **Device Administration** > **Certificate Management** > **Certificates**.

To create a local self-signed device certificate:

1. Click **Create** available on the upper-right corner of the Certificates page.
2. Click **Device Certificate** and select **Local Self-Signed**.

The Create Device Certificate (Local Self-Signed) page appears.

3. Complete the configuration according to the guidelines provided in [Table 65 on page 258](#) .
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.
If you click **OK**, a new CA certificate with the provided configuration is created.

Table 65: Fields on the Create Device Certificate (Local Self-Signed) page

| Field | Action |
|--|--|
| Digital signature | Select one of the digital signatures from the list. That is, RSA, DSA, ECDSA, and so on. By default, RSA-2048 is selected. |
| Name | Enter a certificate name. |
| Subject (Minimum of one field required) | |
| Domain component | Enter the domain component that you want to associate with the certificate. |
| Common name | Enter a common name for the certificate. |
| Organizational unit name | Enter the name of the organizational unit that you want to associate with the certificate. |
| Organizational name | Enter the name of the organization that you want to associate with this certificate. |
| Serial number | Device serial number is autopopulated. |
| Locality | Enter the origin locality name. |
| State | Enter the origin state name. |
| Country | Enter the origin country name. |

Table 65: Fields on the Create Device Certificate (Local Self-Signed) 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 email address of the entity owning the certificate. |
| 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 that you want to associate with the local certificate. For local self-signed certificate (RSA/DSA/ECDSA) options are: SHA-1 digests or SHA-256 digests. |
| Signing certificate | Enable or disable to sign other certificates. |

RELATED DOCUMENTATION

[About the Certificates page | 253](#)

[Add CA Certificate | 270](#)

[Create Device Certificate \(Let's Encrypt\) | 256](#)

[Create Device Certificate \(SCEP\) | 260](#)

Create Device Certificate (SCEP)

You are here: **Device Administration** > **Certificate Management** > **Certificates**.

To create an SCEP certificate:

1. Click **Create** available on the upper-right corner of the Certificates page.
2. Click **Device Certificate** and select **SCEP**.
The Create Device Certificate (SCEP) page appears.
3. Complete the configuration according to the guidelines provided in [Table 66 on page 260](#) .
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.
If you click **OK**, a new CA certificate with the provided configuration is created.

Table 66: Fields on the Create Device Certificate (SCEP) page

| Field | Action |
|------------------------------|---|
| CA certificate name | Select one of the CA certificate names from the list or click Add CA certificate to add a new CA Certificate. For details on adding a CA certificate, see "Add CA Certificate" on page 270 . |
| Digital signature | Select a digital signature from the list. That is, RSA-1024, RSA-2048, or RSA-4096. By default, RSA-2048 is selected. |
| Name | Enter a device certificate name. |
| Enrollment Parameters | |
| Challenge password | Enter the CA challenge password for certificate enrollment and revocation. This challenge password must be the same used when the certificate was originally configured. |
| Digest | Select the digest from the list that you want to associate with the certificate. The options are: MD-5 Digests or SHA-1 digests. |

Table 66: Fields on the Create Device Certificate (SCEP) page (Continued)

| Field | Action |
|--|---|
| Encryption | Select the encryption method from the list for the CA certificate. The options are: DES Encryption or DES-3 Encryption. |
| Auto re-enrollment | Enable this option to request that the issuing CA replace a certificate before its specified expiration date. |
| Renew trigger time | Set the renew trigger time (in days). Default is 65 days and maximum is 85 days. |
| Re-generate key pair | Enable this option to automatically generate a new key pair when a device certificate is automatically re-enrolled. |
| Subject (Minimum of one field required) | |
| Domain component | Enter the domain component that you want to associate with the certificate. |
| Common name | Enter a common name for the certificate. |
| Organizational unit name | Enter the name of the organizational unit that you want to associate with the certificate. |
| Organizational name | Enter the name of the organization that you want to associate with this certificate. |
| Serial number | Device serial number is autopopulated. |
| Locality | Enter the origin locality name. |
| State | Enter the origin state name. |

Table 66: Fields on the Create Device Certificate (SCEP) page *(Continued)*

| Field | Action |
|-------------------------|---|
| Country | Enter the origin country name. |
| Subject Alt Name | |
| Domain name | Enter a domain name that you want to associate with the certificate. |
| Email | Enter an email address of the entity owning the certificate. |
| IPv4 address | Enter the IPv4 address of the device. |
| IPv6 address | Enter the IPv6 address of the device. |
| Advanced | |
| Digest | Select the digest from the list. The options are: SHA-1 digests or SHA-256 digests. |

RELATED DOCUMENTATION

[About the Certificates page | 253](#)

[Add CA Certificate | 270](#)

[Create Device Certificate \(Local Self-Signed\) | 257](#)

[Create Device Certificate \(ACME\) | 262](#)

Create Device Certificate (ACME)

You are here: **Device Administration** > **Certificate Management** > **Certificates**.

To add an ACME certificate:

1. Click **Create** available on the upper-right corner of the Certificates page.

2. Click **Device Certificate** and select **ACME**.

The Create Device Certificate (ACME) page appears.

3. Complete the configuration according to the guidelines provided in [Table 67 on page 263](#) .

4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

If you click **OK**, a new CA certificate with the provided configuration is created.

Table 67: Fields on the Create Device Certificate (ACME) page

| Field | Action |
|---------------------------|--|
| CA certificate name | Select a CA certificate name from the list or click Add CA certificate to add a CA Certificate. For details on adding a CA certificate, see "Add CA Certificate" on page 270 . |
| Digital signature | Select a digital signature from the list. That is, RSA-1024, RSA-2048, or RSA-4096. By default, RSA-2048 is selected. |
| Name | Enter a device certificate name. |
| Contact email | Enter contact email address. |
| Auto Re-enrollment | |
| Trigger time | Set the auto re-enrollment trigger time (in days). Default is 65 days and maximum trigger time is 85 days. |
| Re-generate key pair | Enable to automatically generate a new key pair when a device certificate is automatically re-enrolled. |
| Domain names | Click + to add new domain name that you want to associate with the certificate. This can be an FQDN that resolves to an SRX Series Firewall external IP address. Maximum of domain names allowed is five. |

RELATED DOCUMENTATION

[About the Certificates page | 253](#)

[Add CA Certificate | 270](#)

[Create Device Certificate \(SCEP\) | 260](#)

[Create Device Certificate \(CMPv2\) | 264](#)

Create Device Certificate (CMPv2)

You are here: **Device Administration** > **Certificate Management** > **Certificates**.

To create a CMPv2 device certificate:

1. Click **Create** available on the upper-right corner of the Certificates page.
2. Click **Device Certificate** and select **CMPv2**.
The Create Device Certificate (CMPv2) page appears.
3. Complete the configuration according to the guidelines provided in [Table 68 on page 264](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

If you click **OK**, a new CA certificate with the provided configuration is created.

Table 68: Fields on the Create Device Certificate (CMPv2) page

| Field | Action |
|------------------------------|---|
| CA certificate name | Select a CA certificate name from the list or click Add CA certificate to add a CA Certificate. For details on adding a CA certificate, see "Add CA Certificate" on page 270 . |
| Digital signature | Select a digital signature from the list. That is, RSA, DSA, ECDSA, and so on. By default, RSA-2048 is selected. |
| Name | Enter a device certificate name. |
| Enrollment Parameters | |
| CA secret | Enter the out-of-band secret value received from the CA server. |

Table 68: Fields on the Create Device Certificate (CMPv2) page (Continued)

| Field | Action |
|--|--|
| 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 option 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. |
| Auto re-enrollment | Enable this option to request that the issuing CA replace a certificate before its specified expiration date. |
| Renew trigger time | Set the renew trigger time (in days). Default is 65 days and maximum is 85 days. |
| Regenerate key pair | Enable this option to automatically generate a new key pair when a device certificate is automatically re-enrolled. |
| Subject (Minimum of one field required) | |
| Domain component | Enter the domain component that you want to associate with the certificate. |
| Common name | Enter a common name for the certificate. |
| Organizational unit name | Enter the name of the organizational unit that you want to associate with the certificate. |
| Organizational name | Enter the name of the organization that you want to associate with this certificate. |

Table 68: Fields on the Create Device Certificate (CMPv2) page *(Continued)*

| Field | Action |
|-------------------------|--|
| Serial number | Device serial number is autopopulated. |
| Locality | Enter the origin locality name. |
| State | Enter the origin state name. |
| Country | Enter the origin country name. |
| Subject Alt Name | |
| Domain name | Enter a domain name that you want to associate with the certificate. |
| Email | Enter an email address of the entity owning the certificate. |
| IPv4 address | Enter the IPv4 address of the device. |
| IPv6 address | Enter the IPv6 address of the device. |

RELATED DOCUMENTATION

[About the Certificates page | 253](#)

[Add CA Certificate | 270](#)

[Create Device Certificate \(ACME\) | 262](#)

[Create Device Certificate \(CSR\) | 266](#)

Create Device Certificate (CSR)

You are here: **Device Administration** > **Certificate Management** > **Certificates**.

To create a CSR device certificate:

1. Click **Create** available on the upper-right corner of the Certificates page.
2. Click **Device Certificate** and select **CSR**.
The Create Device Certificate (CSR) page appears.
3. Complete the configuration according to the guidelines provided in [Table 69 on page 267](#) .
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 with status as **Pending Signing**.
5. Click **Load Certificate**.
The Load Certificate window appears.
6. Click **Browse** to upload the signed certificate and click **OK**.
7. Once you upload the certificate, status changes from **Pending Signing** to **Valid** and type changes from **CSR** to **Device Certificate**.

Table 69: Fields on the Create Device Certificate (CSR) page

| Field | Action |
|--|--|
| Digital signature | Select a digital signature from the list. That is, RSA, DSA, ECDSA, and so on. By default, RSA-2048 is selected. |
| Name | Enter a device certificate name. |
| Subject (Minimum of one field required) | |
| Domain component | Enter the domain component that you want to associate with the certificate. |
| Common name | Enter a common name for the certificate. |
| Organizational unit name | Enter the name of the organizational unit that you want to associate with the certificate. |
| Organizational name | Enter the name of the organization that you want to associate with this certificate. |
| Serial number | Device serial number is autopopulated. |

Table 69: Fields on the Create Device Certificate (CSR) page *(Continued)*

| Field | Action |
|-------------------------|---|
| Locality | Enter the origin locality name. |
| State | Enter the origin state name. |
| Country | Enter the origin country name. |
| Subject Alt Name | |
| Domain name | Enter a domain name that you want to associate with the certificate. |
| Email | Enter an email address of the entity owning the certificate. |
| IPv4 address | Enter the IPv4 address of the device. |
| IPv6 address | Enter the IPv6 address of the device. |
| Advanced | |
| Digest | Select the digest from the list. The options are: SHA-1 digests or SHA-256 digests. |

RELATED DOCUMENTATION

[About the Certificates page | 253](#)

[Add CA Certificate | 270](#)

[Create Device Certificate \(CMPv2\) | 264](#)

[Load Signed Device Certificate \(Externally Generated\) | 269](#)

Load Signed Device Certificate (Externally Generated)

You are here: **Device Administration** > **Certificate Management** > **Certificates**.

To upload a signed device certificate for an externally generated certificate:

1. Click **Create** available on the upper-right corner of the Certificates page.
2. Click **Device Certificate** and select **Externally Generated**.
The Load Signed Device Certificate (Externally Generated) page appears.
3. Complete the configuration according to the guidelines provided in [Table 70 on page 269](#) .
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

If you click **OK**, a signed device certificate with the provided configuration is loaded.

Table 70: Fields on the Load Signed Device Certificate (Externally Generated) page

| Field | Action |
|---------------------------|---|
| Certificate ID | Enter the certificate ID of the externally generated certificate. |
| Upload device certificate | Browse and upload the device certificate that is stored. Recommended file formats are .crt, .pem, .der, and .cert. |
| Upload private key | Browse and upload the device certificate that is stored. Recommended file formats are .crt, .pem, .der, and .cert. |
| Password | Enter a password. |

RELATED DOCUMENTATION

[About the Certificates page](#) | 253

[Add CA Certificate](#) | 270

[Create Device Certificate \(CSR\)](#) | 266

Add a Certificate Authority (CA)

IN THIS SECTION

- [Add CA Certificate](#) | 270

You are here: **Device Administration** > **Certificate Management** > **Certificates**.

The CA options available are:

- CA Certificate. See "[Add CA Certificate](#)" on page 270 .
- Juniper Bundle. Loads default CA certificates with prefix `juniper_bundle_` and suffixed with an auto incremented value from 1 to 255.

NOTE: In J-Web UI, you cannot edit Juniper Bundle CA certificates.

Add CA Certificate

You are here: **Device Administration** > **Certificate Management** > **Certificates**.

To add a CA certificate:

1. Click **Create** available on the upper-right corner of the Certificates page.
2. Click **Certificate Authority** and select **CA Certificate**.
The Add CA Certificate page appears.
3. Complete the configuration according to the guidelines provided in [Table 71 on page 270](#) .
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.
If you click **OK**, a new CA certificate with the provided configuration is created.

Table 71: Fields on the Add CA Certificate Page

| Field | Action |
|-------|------------------------------|
| Name | Enter a CA certificate name. |

Table 71: Fields on the Add CA Certificate Page (Continued)

| Field | Action |
|------------------------------------|--|
| Revocation check | <p>Select an option from the list:</p> <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 | <p>For OCSP, enter HTTP addresses for OCSP responders.</p> <p>For CRL, enter the name of the location from which to retrieve the CRL through HTTP or Lightweight Directory Access Protocol (LDAP).</p> |
| On connection failure | <p>Enable this option to skip the revocation check if the OCSP responder is not reachable.</p> <p>NOTE: This option is applicable only for OCSP.</p> |
| Disable responder revocation check | <p>Enable this option to disable revocation check for the CA certificate received in an OCSP response.</p> <p>NOTE: This option is applicable only for OCSP.</p> |
| Accept unknown status | <p>When set to enable, accepts the certificate with unknown status.</p> <p>NOTE: This option is applicable only for OCSP.</p> |

Table 71: Fields on the Add CA Certificate 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> |
| 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> |
| Load CA certificate | <p>Select an option whether you want to load the CA certificate manually or automatically.</p> |
| Upload CA certificate | <p>Click Browse to upload the CA certificate that is stored.</p> <p>NOTE: This option is only available if you choose to load the CA certificate manually.</p> |
| Enrollment URL | <p>Enter the enrollment URL.</p> <p>NOTE: Enrollment URL is optional for manual upload and mandatory for automatic upload.</p> |
| Advanced | |
| Administrator email | <p>Enter an administrator email address.</p> |

Table 71: Fields on the Add CA Certificate Page (*Continued*)

| Field | Action |
|------------------|--|
| Routing instance | Select an option from the list of configured routing instances. |
| 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. |
| Proxy profile | <p>Select an option from the list. Or to create a new proxy profile inline:</p> <ol style="list-style-type: none"> Click Create. Create Proxy Profile page appears. 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 or down arrow. Range: 0 through 65535 Click OK. |

RELATED DOCUMENTATION

[About the Certificates page | 253](#)

[Load Signed Device Certificate \(Externally Generated\) | 269](#)

[Load CA Certificate | 277](#)

Export a Device Certificate

You are here: **Device Administration** > **Certificate Management** > **Certificates**.

To export a device certificate:

1. Click **Export** on the Certificates page.

The Export page appears.

NOTE: Once you click Export, CSR certificate gets downloaded automatically on your local system.

2. Complete the configuration according to the guidelines provided in [Table 72 on page 274](#).
3. 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 72: Fields on the Export Device Certificate page

| Field | Action |
|----------|--|
| 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. |
| Password | Enter password. NOTE: This option is available only when you enable key pair. |

RELATED DOCUMENTATION

[About the Certificates page](#) | 253

[Add CA Certificate](#) | 270

[Edit a CA Certificate](#) | 275

Edit a CA Certificate

You are here: **Device Administration** > **Certificate Management** > **Certificates**.

To edit a CA certificate:

1. Select a CA certificate you want to edit on the Certificates page.
2. Click the edit icon available on the upper-right corner of the Certificates page.

The Edit CA Certificate page appears with editable fields. For more information on the options, see [Table 71 on page 270](#)

3. Click **OK** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

[About the Certificates page | 253](#)

[Export a Device Certificate | 274](#)

[Delete a Certificate | 275](#)

Delete a Certificate

You are here: **Device Administration** > **Certificate Management** > **Certificates**.

To delete a certificate:

1. Select the certificate you want to delete on the Certificates page.
2. Click the delete icon available on the upper-right corner of the Certificates page.

A confirmation window appears.

3. Click **Yes** to delete.

RELATED DOCUMENTATION

[About the Certificates page | 253](#)

[Edit a CA Certificate | 275](#)

[Search Text in the Certificates Table | 276](#)

Search Text in the Certificates Table

You are here: **Device Administration** > **Certificate Management** > **Certificates**.

To search for text:

1. Click the search icon in the upper-right corner of the Certificates page.
2. Enter partial text or full text of the keyword in the search bar and click the search icon.
The search results are displayed.
3. Click **X** next to a search keyword or click **Clear All** to clear the search results.

RELATED DOCUMENTATION

[About the Certificates page | 253](#)

[Delete a Certificate | 275](#)

[Re-Enroll a Device Certificate | 276](#)

Re-Enroll a Device Certificate

You are here: **Device Administration** > **Certificate Management** > **Certificates**.

To re-enroll a device certificate with protocols (SCEP/ACME/CMPv2/Let's Encrypt):

1. Click **Re-enroll** available in the status column of the Certificates table.
The Re-enroll Device Certificate page appears.
2. Complete the configuration according to the guidelines provided in [Table 73 on page 276](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

Table 73: Fields on the Re-enroll Device Certificate page

| Field | Action |
|---------------------|--|
| Name | Displays the certificate ID. |
| CA certificate name | Select the CA certificate name from the list that you want to add. |

Table 73: Fields on the Re-enroll Device Certificate page (*Continued*)

| Field | Action |
|----------------------|---|
| Protocol | Select the protocol that you want to associate with the certificate. |
| Password | Enter password. NOTE: This option is available only when you select SCEP protocol. |
| Digest | Select the digest from the list that you want to associate with the certificate. NOTE: This option is available only when you select SCEP protocol. |
| Encryption | Select an encryption method from the list for the CA certificate. NOTE: This option is available only when you select SCEP protocol. |
| Re-generate key pair | Enable to automatically re-generate a key pair. |

RELATED DOCUMENTATION

[About the Certificates page | 253](#)

[Search Text in the Certificates Table | 276](#)

[Load CA Certificate | 277](#)

Load CA Certificate

You are here: **Device Administration** > **Certificate Management** > **Certificates**.

To load a CA certificate:

1. Click **Load Certificate** available in the status column of the Certificates table.
The Load CA Certificate page appears.
2. Complete the configuration according to the guidelines provided in [Table 74 on page 278](#) .
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

Table 74: Fields on the Load CA Certificate page

| Field | Action |
|--|--|
| Name | Displays the certificate ID. |
| Load CA certificate | Select how you want to load the certificate. That is, manual upload or automatic. |
| Manual Upload Fields | |
| Upload CA certificate | Click Browse to upload the CA certificate that is stored on your local machine. |
| Upload CRL | Click Browse to upload the CRL certificate that is stored on your local machine. |
| Automatic Upload Fields | |
| NOTE: Automatic is enabled only if the enrollment URL is configured for the CA certificate. | |
| Protocol | Select the protocol from the list that you want to associate with the CA certificate. |
| Device certificate | Device certificate is generated based on the enrollment protocol specified. NOTE: This option is available when you select Let's Encrypt, CMPv2, or ACME protocol. |

RELATED DOCUMENTATION

[About the Certificates page](#) | 253

[Re-Enroll a Device Certificate | 276](#)

[Reload CA Certificate | 279](#)

Reload CA Certificate

You are here: **Device Administration** > **Certificate Management** > **Certificates**.

To reload a CA certificate:

1. Click **Reload Certificate** available in the status column of the Certificates table.
The Reload CA Certificate page appears.
2. Complete the configuration according to the guidelines provided in [Table 75 on page 279](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

Table 75: Fields on the Reload CA Certificate page

| Field | Action |
|--|---|
| Name | Displays the certificate ID. |
| Load CA certificate | Select how you want to load the certificate. That is, manual upload or automatic. |
| Manual Upload Fields | |
| Upload CA certificate | Click Browse to upload the CA certificate that is stored on your local machine. |
| Upload CRL | Click Browse to upload the CRL certificate that is stored on your local machine. |
| Automatic Upload Fields | |
| NOTE: Automatic is enabled only if the enrollment URL is configured for the CA Certificate. | |
| Protocol | Select the protocol from the list that you want to associate with the CA certificate. |

Table 75: Fields on the Reload CA Certificate page (*Continued*)

| Field | Action |
|--------------------|--|
| Device certificate | Device certificate is generated based on the enrollment protocol specified. NOTE: This option is available when you select Let's Encrypt, CMPv2, or ACME protocol. |

RELATED DOCUMENTATION

[About the Certificates page | 253](#)

[Add CA Certificate | 270](#)

[Load CA Certificate | 277](#)

Certificate Management—Certificate Authority Group

IN THIS CHAPTER

- [About the Certificate Authority Group Page | 281](#)
- [Import a Trusted CA Group | 282](#)
- [Add a CA Group | 283](#)
- [Edit a CA Group | 284](#)
- [Delete a CA Group | 285](#)
- [Search Text in the Certificate Authority Group Table | 285](#)

About the Certificate Authority Group Page

You are here: **Device Administration** > **Certificate Management** > **Trusted Certificate Authority**.

Multiple CA profiles can be grouped in one trusted CA group for a given topology. The CA group can be used either in SSL or IPsec.

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.

You can perform the following tasks:

- Import a CA group to manually load the CA group. See ["Import a Trusted CA Group" on page 282](#) .
- Add a CA group. See ["Add a CA Group" on page 283](#) .

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 ["Edit a CA Group" on page 284](#) .
- Delete a CA group. See ["Delete a CA Group" on page 285](#) .
- Search for text in a CA group table. See ["Search Text in the Certificate Authority Group Table" on page 285](#) .
- Filter the CA group information based on select criteria. To do this, select the filter icon at the upper-right 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 upper-right corner of the page and select the options you want to show or deselect to hide options on the page.

[Table 76 on page 282](#) provides the details of the fields of the Certificate Authority Group Page.

Table 76: 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. |

Import a Trusted CA Group

You are here: **Device Administration > Certificate Management > Trusted Certificate Authority.**

To import a trusted CA group:

1. Click **Import.**

The Import Trusted CA Group page appears.

2. Complete the configuration according to the guidelines provided in [Table 77 on page 283](#) .

3. 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 an SSL proxy.

Table 77: 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. |

RELATED DOCUMENTATION

[About the Certificate Authority Group Page | 281](#)

[Add a CA Group | 283](#)

[Edit a CA Group | 284](#)

[Delete a CA Group | 285](#)

[Search Text in the Certificate Authority Group Table | 285](#)

Add a CA Group

You are here: **Device Administration** > **Certificate Management** > **Trusted Certificate Authority**.

To add a CA group:

1. Click **+**.
The Add CA Group page appears.
2. Complete the configuration according to the guidelines provided in [Table 78 on page 284](#).
3. 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 78: Fields on the Add CA Group Page

| Field | Action |
|---------------|--|
| CA Group Name | Enter a unique CA group name. |
| CA Profiles | 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. NOTE: You can add up to maximum of 20 CA profiles per trusted CA group. |

RELATED DOCUMENTATION

[About the Certificate Authority Group Page | 281](#)

[Import a Trusted CA Group | 282](#)

[Edit a CA Group | 284](#)

[Delete a CA Group | 285](#)

[Search Text in the Certificate Authority Group Table | 285](#)

Edit a CA Group

You are here: **Device Administration** > **Certificate Management** > **Trusted Certificate Authority**.

To edit a CA group:

1. Select a CA group.
2. Click the pencil icon available on the upper-right corner of the Certificate Authority Group page.
See "[Add a CA Group](#)" on [page 283](#) for the options available for editing on the Edit CA Group page.
3. Click **OK**

RELATED DOCUMENTATION

[About the Certificate Authority Group Page | 281](#)

[Import a Trusted CA Group | 282](#)

[Add a CA Group | 283](#)

[Delete a CA Group | 285](#)

[Search Text in the Certificate Authority Group Table | 285](#)

Delete a CA Group

You are here: **Device Administration** > **Certificate Management** > **Trusted Certificate Authority**.

To delete a CA group:

1. Select a CA group.
2. Click the delete icon available on the upper-right corner of the Certificate Authority Group page.
A confirmation window appears.
3. Click **Yes** to delete.

RELATED DOCUMENTATION

[About the Certificate Authority Group Page | 281](#)

[Import a Trusted CA Group | 282](#)

[Add a CA Group | 283](#)

[Edit a CA Group | 284](#)

[Search Text in the Certificate Authority Group Table | 285](#)

Search Text in the Certificate Authority Group Table

You are here: **Device Administration** > **Certificate Management** > **Trusted Certificate Authority**.

You can use the search icon in the upper-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.

RELATED DOCUMENTATION

[About the Certificate Authority Group Page | 281](#)

[Import a Trusted CA Group | 282](#)

[Add a CA Group | 283](#)

[Edit a CA Group | 284](#)

[Delete a CA Group | 285](#)

License Management

IN THIS CHAPTER

- [Manage Your Licenses | 287](#)

Manage Your Licenses

IN THIS SECTION

- [About License Management Page | 287](#)
- [Add License | 288](#)
- [Delete Installed Licenses | 289](#)
- [Update Installed Licenses | 289](#)
- [Update Trial Licenses | 289](#)
- [Display License Keys | 289](#)
- [Download License Keys | 290](#)
- [Software Feature Licenses | 290](#)

About License Management Page

You are here: **Device Administration** > **License Management**.

You can add a new license key, delete one or more license keys, update, or download license keys.

[Table 79 on page 288](#) describes the fields on the License Management page.

Table 79: Fields on the License Maintenance Page

| Field | Function |
|--------------------|--|
| Feature | Displays the name of the licensed feature. |
| 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. |

Add License

To add a new license key with the J-Web license manager:

1. Perform one of the following:

- **License File URL**—Enter the full URL to the destination file containing the license key.

NOTE: Use this option to send a subscription-based license key entitlement (such as Content Security) to the Juniper Networks licensing server for authorization. If authorized, the server downloads the license to the device and activates it.

- **License Key**—Paste the license key text, in plain-text format, for the license.

Use a blank line to separate multiple license keys.

NOTE: Use this option to activate a perpetual license directly on the device. (Most feature licenses are perpetual.)

2. Click **OK** to add the license key or click **Cancel** to return to the License Management page.

Delete Installed Licenses

To delete one or more license keys with the J-Web license manager:

1. Select the check box of the license or licenses you want to delete.
2. Click **Delete**.

NOTE: If you have deleted the SRX100 Memory Upgrade license, the device reboots immediately and comes back up as a low-memory device.

3. Click **OK** to delete the selected license or licenses or click **Cancel** to return to the License Management page.

Update Installed Licenses

To send license update to the License Management Server (LMS):

1. Click **Update**.
The Update Licenses page appears.
2. Click **OK** to send license update to LMS.

Update Trial Licenses

To send license update to the LMS and to update the trial licenses:

1. Click **Update Trial**.
The Update Trial Licenses page appears.
2. Click **OK** to update the trial licenses.

Display License Keys

To display the license keys installed on the device with the J-Web license manager:

1. Click **Display Keys** to view all of the license keys installed on the device.
2. Click **Back** to return to the License Management page.

Download License Keys

Downloads the license keys installed on the device with the J-Web license manager.

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. Each license allows you to run the specified advanced software features on a single device. Platform support depends on the Junos OS release in your installation. For more information on the software feature licenses for SRX Series Firewalls, see [Licenses for SRX Series](#).

RELATED DOCUMENTATION

| [Enroll Your Device with Juniper ATP Cloud](#) | 306

Security Package Management

IN THIS CHAPTER

- [About the Security Package Management Page | 291](#)
- [Install or Upload IPS Signatures Package | 295](#)
- [IPS Signatures Settings | 297](#)
- [Install Application Signatures Package | 299](#)
- [Application Signatures Settings | 299](#)
- [Manage URL Categorization | 301](#)
- [Check URL Recategorization Status | 302](#)
- [Install URL Category Package | 302](#)
- [URL Categories Settings | 303](#)

About the Security Package Management Page

IN THIS SECTION

- [Field Descriptions | 292](#)

You are here: **Device Administration** > **Security Package Management**

Use this page to configure the SRX Series Firewall to install, upload, and automatically download the updated security packages from the specified URL.

You can perform the following tasks from this page:

- IPS signatures:
 - Install and upload IPS signatures package. See "[Install or Upload IPS Signatures Package](#)" on page [295](#).

- Configure IPS signatures settings. See ["IPS Signatures Settings" on page 297](#) .
- Application signatures:
 - Install an application signature package. See ["Install Application Signatures Package" on page 299](#) .
 - Configure application signature package install settings. See ["Application Signatures Settings" on page 299](#) .
- URL categories:
 - Manage URL categorization. See ["Manage URL Categorization" on page 301](#) .
 - Check URL recategorization status. See ["Check URL Recategorization Status" on page 302](#) .
 - Install an URL category package. See ["Install URL Category Package" on page 302](#) .
 - Configure URL category package install settings. See ["URL Categories Settings" on page 303](#) .

Field Descriptions

[Table 80 on page 292](#) to [Table 82 on page 294](#) describes the fields on the Security Package Management page.

Table 80: Fields on the IPS Signatures Page

| Field | Description |
|--|--|
| Installed IPS Signature Package | |
| Version | Displays the security package version that is currently installed on the device. |
| Status | Displays the following statuses of the security package installation: <ul style="list-style-type: none"> • <i><Version number></i> installation in progress • Installed successfully • Failed |
| Published Date | Displays the security package released date and time. |

Table 80: Fields on the IPS Signatures Page (Continued)

| Field | Description |
|-----------------|--|
| Detector | Displays the detector version number that is currently installed on the device. |
| Rollback Action | Displays the previously installed security package version on the system. Click the version number to rollback to the previous version. |

Latest IPS Signature Package

| | |
|--------------|---|
| Version | Displays the ten latest security package versions. |
| View Details | Click View Details to learn more about the security package version. |
| Install | You can choose either of the options: <ul style="list-style-type: none"> • Install package—Installs the selected security package version on the device. • Upload package—Uploads a selected package version to install it on the device. |
| Settings | You can configure a proxy server to download and install security package. You can also schedule an automatic installation of security packages for a later date and time. |

Table 81: Fields on the Application Signatures Page

| Field | Description |
|--|--|
| Installed Application Signature Package | |
| Version | Displays the security package version that is currently installed on the device. |

Table 81: Fields on the Application Signatures Page (Continued)

| Field | Description |
|-----------------|--|
| Status | <p>Displays the following statuses of the security package installation:</p> <ul style="list-style-type: none"> • <Version number> installation in progress • Installed successfully • Failed |
| Published Date | Displays the security package released date and time. |
| Rollback Action | <p>Displays the previously installed security package version on the system.</p> <p>Click the version number to roll back to the previous version.</p> |

Latest Application Signature Package

| | |
|------------------|--|
| Version | Displays the ten latest security package versions. |
| View Details | Click View Details to learn more about the security package version. |
| Install | You can choose to install the selected security package version on the device. |
| Install Settings | You can configure a proxy server to download and install security package. You can also schedule an automatic installation of security packages for a later date and time. |

Table 82: Fields on the URL Categories Page

| Field | Description |
|-----------------------------|--|
| URL Category Package | |
| Version | Displays the Enhanced Web Filtering (EWF) or Juniper NextGen categories package version that is currently installed on the device. |

Table 82: Fields on the URL Categories Page (Continued)

| Field | Description |
|--------------------|---|
| Status | <p>Displays the following statuses of the security package installation:</p> <ul style="list-style-type: none"> • <i><Version number></i> installation in progress • Installed successfully • Failed |
| Base Filter | Click the base filter name (ng-default-filter or ewf-default-filter) to view the available URL categories. |
| URL Categorization | You can manage URL categorization or check URL categorization status. |
| Install | Installs the latest EWF or Juniper NextGen category package on the device. |
| Install Settings | You can configure a proxy server to download and install EWF or Juniper NextGen categories package. You can also schedule an automatic installation of EWF or Juniper NextGen categories package for a later date and time. |

RELATED DOCUMENTATION

[Install or Upload IPS Signatures Package | 295](#)

[Install Application Signatures Package | 299](#)

[Install URL Category Package | 302](#)

[IPS Signatures Settings | 297](#)

[Application Signatures Settings | 299](#)

[URL Categories Settings | 303](#)

Install or Upload IPS Signatures Package

You are here: **Device Administration > Security Package Management.**

You can choose to install the selected security package version or upload a selected package version to install it on the device.

NOTE: When using either of the installation methods, you can continue to configure the other features while the installation is in progress. Once the installation is complete, you will see a notification on the UI.

To install the security packages:

1. Select a security package version you want to install and then click **Install** available at the upper-right corner of the Latest IPS Signature Package table.
2. Click **Install package** to install the selected security package version.
The installation status is shown in the Status column of the Installed IPS Signature Package table.

To upload the security packages (offline security packages installation):

1. Click **Install** available at the upper-right corner of the Latest IPS Signature Package table. Then, select **Upload package**.
2. Click **Browse** to upload a downloaded security package version and then click **OK**.

The installation starts automatically and the status is shown in the Status column of the Installed IPS Signature Package table.

To download the security package on the host machine:

- a. Go to <https://support.juniper.net/support/downloads/>.
- b. Select **All Products** from the list and enter the *SRX Series model*. For example, SRX300.
- c. Press **Enter** or click **Find a Product**.
- d. Scroll down and go to **Related Software** section.
- e. Click **+** and click on the Offline Signature Files.

You are directed to the Download Results page.

- f. Click **+** to choose any one of the following:
 - Offline APPID Sigpack Files—This includes only the App ID files.
 - Offline Sigpack Files—This includes both IPS and App ID files.
- g. Click the **gz** link of the package you want to download from the Downloads column.

You are directed to the Web download site.

- h. Log in with your username and password.
- i. Select **I agree** for the EULA information and click **Proceed**.
- j. On the Download Software page that appears, the following options are available:
 - If you want to download the package on your host machine, click the **CLICK HERE** link and save the file to your machine.
 - If you want to download the package on your device, copy the URL and install it on the device using the CLI commands.

RELATED DOCUMENTATION

[About the Security Package Management Page | 291](#)

[Install Application Signatures Package | 299](#)

[Install URL Category Package | 302](#)

IPS Signatures Settings

You are here: **Device Administration** > **Security Package Management**

You can configure a proxy server to download and install security package. You can also schedule an automatic installation of security packages for a later date and time.

To configure the security package installation settings:

1. Click the Settings icon available at the upper-right corner of the Latest IPS Signature Package table. The Settings page appears.
2. Complete the configuration according to the guidelines provided in [Table 83 on page 298](#) .
3. Click **OK**.
The security package will automatically install in the scheduled interval. The installation status is shown in the Status column of the Installed IPS Signature Package table.

Table 83: Fields on the Settings Page

| Field | Action |
|-------------------------|---|
| Security Package URL | Displays the URL from where the security package is downloaded. Default URL is https://signatures.juniper.net/cgi-bin/index.cgi . |
| Routing Instance | <p>Select a routing instance from the list to reach the proxy server.</p> <p>To create a new routing instance, click Create New. For more information on the fields, see "Add a Routing Instance" on page 567 .</p> |
| Proxy profile | <p>This is optional. Select a proxy profile from the list. The proxy profile acts as a proxy server to download the security package.</p> <p>To create a new proxy profile, click Create New. For more information on the fields, see "Add a Proxy Profile" on page 845 .</p> |
| Schedule Install | |
| Schedule | <p>Enable the option to schedule automatic download and installation of security package at a specific date, time, and interval.</p> <p>NOTE: The package also includes application signatures. If you've set up a separate schedule for installing application signatures, then this schedule will take precedence.</p> |
| Start Time | <p>Select a time to start automatic download and to install the updated security package from the specified URL.</p> <p>Format: YYYY-MM-DD.hh:mm (24 hours).</p> |
| Interval | <p>Amount of time (in hours) that the device waits before updating the security package.</p> <p>Range: 1 through 336</p> |

RELATED DOCUMENTATION

[About the Security Package Management Page | 291](#)

[Install Application Signatures Package | 299](#)

[Install Application Signatures Package | 299](#)

[Install URL Category Package | 302](#)

Install Application Signatures Package

You are here: **Device Administration** > **Security Package Management**.

You can choose to install the selected security package version on the device.

To install the security packages:

1. Select a security package version you want to install and then click **Install** available at the upper-right corner of the Latest Application Signature Package table.
2. Click **Install package** to install the selected security package version.

The installation status is shown in the Status column of the Installed Application Signature Package table.

RELATED DOCUMENTATION

[About the Security Package Management Page | 291](#)

[Install or Upload IPS Signatures Package | 295](#)

[Install URL Category Package | 302](#)

Application Signatures Settings

You are here: **Device Administration** > **Security Package Management**

You can configure a proxy server to download and install security package. You can also schedule an automatic installation of security packages for a later date and time.

To configure the security package installation settings:

1. Click the Settings icon available at the upper-right corner of the Latest Application Signature Package table.

The Install Settings page appears.

2. Complete the configuration according to the guidelines provided in [Table 84 on page 300](#) .

3. Click **OK**.

The security package will automatically install in the scheduled interval. The installation status is shown in the Status column of the Installed Application Signature Package table.

Table 84: Fields on the Install Settings Page

| Field | Action |
|-------------------------|---|
| Security Package URL | Displays the URL from where the security package is downloaded. Default URL is https://signatures.juniper.net/cgi-bin/index.cgi . |
| Proxy profile | <p>This is optional. Select a proxy profile from the list. The proxy profile acts as a proxy server to download the security package.</p> <p>To create a new proxy profile, click Create New. For more information on the fields, see "Add a Proxy Profile" on page 845 .</p> |
| Schedule Install | |
| Schedule | <p>Enable the option to schedule automatic download and installation of security package at a specific date, time, and interval.</p> <p>NOTE: If IPS signatures package installation is already scheduled, then it also includes application signatures package. If you want to set up a separate schedule for installing application signatures, then disable the Schedule option for IPS signatures.</p> |
| Start Time | <p>Select a time to start automatic download and to install the updated security package from the specified URL.</p> <p>Format: YYYY-MM-DD.hh:mm (24 hours).</p> |
| Interval | <p>Amount of time (in hours) that the device waits before updating the security package.</p> <p>Range: 1 through 336</p> |

RELATED DOCUMENTATION

[About the Security Package Management Page | 291](#)

[Install or Upload IPS Signatures Package | 295](#)

[Install Application Signatures Package | 299](#)

[Install URL Category Package | 302](#)

Manage URL Categorization

You are here: **Device Administration** > **Security Package Management**.

Use this page to add a new URL to a category or change the category of an existing URL.

To manage the URL categorization:

1. Click the **URL CATEGORIES** tab.
2. Click the **URL Categorization** option available at the upper-right corner of the URL Category Package table and click **Manage URL Categorization**.
The Manage URL Categorization page appears.
3. Complete the configuration according to the guidelines provided in [Table 85 on page 301](#).
4. Click **OK**.

Table 85: Fields on the Manage URL Categorization page

| Field | Action |
|----------|---|
| Action | Select one of the following options. <ul style="list-style-type: none"> • Update the category for an existing URL • Add a new URL to a category |
| URL | Enter the URL domain name or IP address. For example, www.abc.com. |
| Category | Select the application or IPS signature category to which you want to add the URL. NOTE: Leave this field blank if you are unsure what to choose. |

RELATED DOCUMENTATION

[About the Security Package Management Page | 291](#)

[URL Categories Settings | 303](#)

[Check URL Recategorization Status | 302](#)

Check URL Recategorization Status

You are here: **Device Administration** > **Security Package Management**.

Use this page to check the URL recategorization status. To do this:

1. Click the **URL CATEGORIES** tab.
2. Click the **URL Categorization** option available at the upper-right corner of the URL Category Package table and click **Check URL Recategorization Status**.
The Check URL Recategorization Status page appears.
3. Enter a valid URL and click **Check Status**.
'The URL category is updated' message is displayed if the recategorization for the URL you entered is successful.

NOTE: Once the request is submitted, the status shows as 'Your request is being processed'. The request undergo review and update the corresponding status.
Contact Juniper customer support if the URL category change request is rejected.

4. Click **Close**.

RELATED DOCUMENTATION

[About the Security Package Management Page | 291](#)

[URL Categories Settings | 303](#)

[Manage URL Categorization | 301](#)

Install URL Category Package

You are here: **Device Administration** > **Security Package Management**.

You can choose to install the latest URL category package version to install it on the device.

To install the latest URL category package:

1. Click **Install** available at the upper-right corner of the URL Category Package table.
2. Click **Install package** to install the latest URL category package version.

The installation status is shown in the Status column of the URL Category Package table.

RELATED DOCUMENTATION

[About the Security Package Management Page | 291](#)

[Install or Upload IPS Signatures Package | 295](#)

[Install Application Signatures Package | 299](#)

[URL Categories Settings | 303](#)

URL Categories Settings

You are here: **Device Administration** > **Security Package Management**

You can configure a proxy server to download and install EWF or Juniper NextGen categories package. You can also schedule an automatic installation of EWF or Juniper NextGen categories package for a later date and time.

To configure the EWF or Juniper NextGen categories package installation settings:

1. Click the Settings icon available at the upper-right corner of the URL Category Package table.
The Install Settings page appears.
2. Complete the configuration according to the guidelines provided in [Table 86 on page 303](#).
3. Click **OK**.

The EWF or Juniper NextGen categories package will automatically install in the scheduled interval. The installation status is shown in the Status column of the URL Category Package table.

Table 86: Fields on the Install Settings Page

| Field | Action |
|----------------------|---|
| Security Package URL | Displays the URL from where the EWF or Juniper NextGen categories package is downloaded. Default URL is https://signatures.juniper.net/ . |

Table 86: Fields on the Install Settings Page *(Continued)*

| Field | Action |
|-------------------------|---|
| Routing Instance | <p>Select a routing instance from the list to reach the proxy server.</p> <p>To create a new routing instance, click Create New. For more information on the fields, see "Add a Routing Instance" on page 567 .</p> |
| Proxy profile | <p>This is optional. Select a proxy profile from the list. The proxy profile acts as a proxy server to download the EWF or Juniper NextGen categories package.</p> <p>To create a new proxy profile, click Create New. For more information on the fields, see "Add a Proxy Profile" on page 845 .</p> |
| Schedule Install | |
| Schedule | <p>Enable the option to schedule automatic download and installation of EWF or Juniper NextGen categories package at a specific date, time, and interval.</p> |
| Start Time | <p>Select a time to start automatic download and to install the updated EWF or Juniper NextGen categories package from the specified URL.</p> <p>Format: YYYY-MM-DD.hh:mm (24 hours).</p> |
| Interval | <p>Amount of time (in hours) that the device waits before updating the EWF or Juniper NextGen categories package.</p> <p>Range: 1 through 336</p> |

RELATED DOCUMENTATION

[About the Security Package Management Page](#) | 291

[Install or Upload IPS Signatures Package](#) | 295

ATP Management

IN THIS CHAPTER

- [Enroll Your Device with Juniper ATP Cloud | 306](#)
- [About the Diagnostics Page | 309](#)

Enroll Your Device with Juniper ATP Cloud

Before enrolling a device:

- Ensure that you have a Juniper ATP Cloud account with an associated license (free, basic, or premium) to configure a Juniper ATP Cloud realm. The license controls the features of the Juniper ATP Cloud. For more information on the Juniper ATP Cloud account, see [Registering a Juniper Advanced Threat Prevention Cloud Account](#).
- Decide which region the realm you create will cover because you must select a region when you configure a realm.
- Ensure the device is registered in the ATP cloud portal.
- In the CLI mode, configure `set security forwarding-process enhanced-services-mode` on your SRX300, SRX320, SRX340, SRX345, and SRX550M devices to open ports and get the device ready to communicate with ATP cloud.
- ATP cloud requires that both your Routing Engine (control plane) and Packet Forwarding Engine (data plane) can connect to the Internet.
- ATP cloud requires the following ports to be open on the SRX Series Firewall: 80, 8080, and 443.

You are here: **Device Administration** > **ATP Management** > **Enrollment**.

Use this page to enroll your SRX Series Firewall with Juniper Advanced Threat Prevention Cloud (Juniper ATP Cloud).

Juniper ATP Cloud is a cloud-based threat identification and prevention solution. It protects your device from malware and sophisticated cyber threats by inspecting e-mail and web traffic for advanced threats.

Juniper ATP Cloud integrates with the SRX Series Firewalls to simplify its deployment and enhance the anti-threat capabilities of the SRX Series Firewalls.

ATP uses a Junos OS operation (op) script to help you configure your SRX Series Firewall to connect to the ATP cloud service.

The Junos OS operation (op) script performs the following tasks:

- Downloads and installs certificate authority (CAs) licenses onto your SRX Series Firewall.
- Creates local certificates and enrolls them with the cloud server.
- Performs basic ATP cloud configuration on the SRX Series Firewall.
- Establishes a secure connection to the cloud server.

To enroll your device with Juniper ATP Cloud from J-Web:

1. Proxy Profile Configuration (Optional)

- a.** Select an option in the Proxy Profile list and proceed with Step 2.

NOTE:

- The list displays the existing proxy profiles that you have created using the Proxy Profile page (Security Policies & Objects > Proxy Profiles).
- The SRX Series Firewall and Juniper ATP Cloud communicates through the proxy server if a proxy profile is configured. Otherwise, they directly communicate with each other.

- b.** Or click **Create Proxy** to create a proxy profile.

The Create Proxy Profile page appears.

- c.** Complete the configuration by using the guidelines in [Table 87 on page 308](#) .

- d.** Click **OK**.

A new proxy profile is created.

- e.** Click **Apply Proxy**.

Applying proxy enables the SRX Series Firewall and Juniper ATP Cloud to communicate through the proxy server.

Table 87: Fields on the Create Proxy Profile Page

| Field | Action |
|-----------------|---|
| Profile Name | Enter a name for the proxy profile. |
| Connection Type | Select the connection type server from the list that proxy profile uses: <ul style="list-style-type: none"> • Server IP—Enter the IP address of the proxy server. • Host Name—Enter the name of the proxy server. |
| Port Number | Select a port number for the proxy profile. Range is 0 to 65535. |

2. Enroll SRX Series Firewall with ATP Cloud

a. Click **Enroll**.

The ATP Cloud Enrollment page appears.

NOTE: If there are any existing configuration changes, a message appears for you to commit the changes and then to proceed with the enrollment process.

b. Complete the configuration by using the guidelines in [Table 88 on page 309](#) .

c. Click **OK**.

The SRX Series Firewall enrollment progress, successful message, or any errors will be shown at the end of the ATP Cloud Enrollment page.

NOTE:

- A new realm is created if you have enabled **Create New Realm** and then the SRX Series Firewall is enrolled to Juniper ATP Cloud. If there is any existing enrollment for the same SRX Series Firewall, CLI sends the data to Juniper ATP Cloud portal to do the duplicate validation during the enrollment process. You cannot check for the duplicate validation through J-Web.
- Click **Diagnostics** to troubleshoot any enrollment errors.

- Click **UnEnroll** if you wish to disenroll your device from ATP

Table 88: Fields on the ATP Cloud Enrollment Page

| Field | Description |
|------------------|---|
| Create New Realm | <p>By default, this option will be disabled if you have an ATP Cloud account with an associated license.</p> <p>Enable this option to add a new realm if you do not have an ATP Cloud account with an associated license.</p> |
| Location | Select a region of the world from the list. |
| Email | Enter your E-mail address. |
| Password | Enter a unique string at least eight characters long. It must include both uppercase letters, lowercase letters, and at least one number. It can also include special characters. No spaces are allowed and you cannot use the same sequence of characters that are in your e-mail address. |
| Confirm Password | Reenter the password. |
| Company Name | Enter a company name to enroll into the realm. A company name can only contain alphanumeric characters, special characters (underscore and dash). |
| Realm | Enter a name for the security realm. This should be a name that is meaningful to your organization. A realm name can only contain alphanumeric characters and the dash symbol. Once created, this name cannot be changed. |

About the Diagnostics Page

You are here: **Device Administration** > **ATP Management** > **Diagnostics**.

Use this page to diagnose and verify threat prevention.

Table 89 on page 310 describes the fields on the Diagnostics page.

Table 89: Fields on the Diagnostics Page

| Field | Description |
|---------------------------|---|
| Diagnostics | |
| ATP Diagnostics | Select an option from the list to diagnose. |
| Diagnostics Logs | Displays the diagnostic logs for the selected option. |
| Run Diagnostics | Enables you to see the diagnostics of a certain region. |
| Check Connectivity | |
| Check | Click Check to verify the connectivity. |
| 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. |

Table 89: Fields on the Diagnostics Page (Continued)

| Field | Description |
|-----------------------------|--|
| 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. |

RELATED DOCUMENTATION

| [Monitor Threat Prevention](#) | 120

Operations

IN THIS CHAPTER

- [Maintain Files | 312](#)
- [Maintain Reboot Schedule | 315](#)
- [Maintain System Snapshots | 317](#)

Maintain Files

IN THIS SECTION

- [About Files Page | 312](#)
- [Clean Up Files | 312](#)
- [Download and Delete Files | 313](#)

About Files Page

You are here: **Device Administration** > **Operations** > **Files**.

You can clean up files, download, or delete files.

Clean Up Files

To maintain files:

1. Click **Clean Up Files**.

The device will perform the following tasks:

- 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.

The J-Web interface displays the files that you can delete and the amount of space that will be freed on the file system.

2. Click one:

- **OK**—Deletes the files and returns to the Files page.
- **Cancel**—Cancels your entries and returns to the Files page.

Download and Delete Files

[Table 90 on page 313](#) provides the maintenance options to download and delete files.

Table 90: Download and Delete Files Maintenance Options

| File Type | Function |
|-----------------|--|
| Log Files | <p>Lists the log files located in the /var/log directory on the device.</p> <p>Select an option:</p> <ul style="list-style-type: none"> • Delete—Deletes files. • Download—Downloads files. |
| Temporary Files | <p>Lists the temporary files located in the /var/tmp directory on the device.</p> <p>Select an option:</p> <ul style="list-style-type: none"> • Delete—Deletes files. • Download—Downloads files. |

Table 90: Download and Delete Files Maintenance Options (*Continued*)

| File Type | Function |
|------------------------|---|
| Jailed Temporary Files | <p>Lists the jailed temporary files located in the <code>/var/jail/tmp</code> directory on the device.</p> <p>Select an option:</p> <ul style="list-style-type: none"> • Delete—Deletes files. • Download—Downloads files. |
| Old JUNOS Software | <p>Lists the software images located in the <code>/var/sw/pkg</code> (*.tgz files) directory on the device.</p> <p>Select an option:</p> <ul style="list-style-type: none"> • Delete—Deletes files. • Download—Downloads files. |
| Crash (Core) File | <p>Lists the core files located in the <code>/var/crash</code> directory on the device.</p> <p>Select an option:</p> <ul style="list-style-type: none"> • Delete—Deletes files. • Download—Downloads files. |
| Database Files | <p>Lists the database files located in the <code>/var/db</code> directory on the device.</p> <p>Select an option:</p> <ul style="list-style-type: none"> • Delete—Deletes files. • Download—Downloads files. |

SEE ALSO

[Maintain Reboot Schedule](#) | 315

Maintain Reboot Schedule

You are here: **Device Administration** > **Operations** > **Reboot**.

You can schedule reboot or halt the system using options such as reboot Immediately, reboot in, reboot with the system time, or halt immediately.

NOTE: A halted system can only be accessed from the system console port.

To reboot or halt the system:

1. Complete the configuration according to the guidelines provided in [Table 91 on page 315](#).

Table 91: Reboot Schedule Maintenance Options

| Field | Action |
|---|--|
| Reboot Immediately | Select this option to reboot the device immediately. |
| Reboot in <i>number of minutes</i> | 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> | Select this option to reboot 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 NOTE: This option is not available in SRX4600 device. | Select this option to stop the device immediately. After the software has stopped, you can access the device through the console port only. |

Table 91: Reboot Schedule Maintenance Options (*Continued*)

| Field | Action |
|---|--|
| <p>Reboot From Media</p> <p>NOTE: This option is not available in SRX4600 device.</p> | <p>Choose the boot device from the Reboot From Media list:</p> <ul style="list-style-type: none"> • internal—Reboots from the internal media (default). • usb—Reboots from the USB storage device. |
| <p>Message</p> | <p>Type a message to be displayed to the user on the device before the reboot occurs.</p> |

2. Click **Schedule**.

Schedules a reboot based on the scheduled configuration.

3. The J-Web interface requests confirmation to perform the reboot or to halt.

Click **OK** to confirm to reboot or alt the system or click **Cancel** to return to the Reboot page.

NOTE:

- 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.
- 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.

RELATED DOCUMENTATION

Maintain System Snapshots | 317

Maintain System Snapshots

You are here: **Device Administration** > **Operations** > **Snapshot**.

You can configure boot devices to replace primary boot device or to act as a backup boot device.

The snapshot process copies the current system software, along with the current and rescue configurations, to alternate media. Optionally, you can copy only the factory and rescue configurations.

To maintain the system snapshots, you create a snapshot of the running system software and save the snapshot to an alternate media.

1. Complete the configuration according to the guidelines provided in [Table 92 on page 317](#).
2. Click **Snapshot**.
Creates a boot device on an alternate media.
3. Click **OK** to perform the system snapshot to a media or click **Cancel** to return to the Snapshot page.

Table 92: Snapshot Maintenance Options

| Field | Function |
|--------------|---|
| 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>Select an option 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. |
| Partition | <p>Partitions the media. This process is usually necessary for boot devices that do not already have software installed on them.</p> <p>Select the check box.</p> |

Table 92: Snapshot Maintenance Options *(Continued)*

| Field | Function |
|---------|--|
| Factory | <p data-bbox="857 365 1414 464">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 data-bbox="857 495 1084 522">Select the check box.</p> <p data-bbox="857 554 1398 653">NOTE: After a boot device is created with the default factory configuration, it can operate only in an internal media slot.</p> |

RELATED DOCUMENTATION

[Upload Software Packages | 319](#)

[Install Software Packages | 320](#)

[Rollback Software Package Version | 321](#)

Software Management

IN THIS CHAPTER

- Upload Software Packages | 319
- Install Software Packages | 320
- Rollback Software Package Version | 321

Upload Software Packages

You are here: **Device Administration** > **Software Management** > **Upload Package**.

You can upload a software package file to the device for installation.

To upload software packages:

1. Complete the configuration according to the guidelines provided in [Table 93 on page 319](#).

Table 93: Upload Package Maintenance Options

| Field | Action |
|--------------------|---|
| File to Upload | Enter the location of the software package on the local system or click Choose File to navigate to the location. |
| Reboot If Required | Select the check box to automatically reboot when the upgrade is complete. |
| Do not save backup | Select the check box so that backup copy of the current Junos OS package is not saved. |

Table 93: Upload Package Maintenance Options *(Continued)*

| Field | Action |
|---|--|
| Format and re-partition the media before installation NOTE: This option is not available for SRX4600 devices. | Select the check box to format the internal media with dual-root partitioning. |

2. Click **Upload and Install Package**.

The software is activated after the device has rebooted.

RELATED DOCUMENTATION

[Install Software Packages | 320](#)

[Rollback Software Package Version | 321](#)

Install Software Packages

You are here: **Device Administration** > **Software Management** > **Install Package**.

You can install a software package from a remote server.

To install software packages:

1. Complete the configuration according to the guidelines provided in [Table 94 on page 320](#).

Table 94: Install Package Maintenance Options

| Field | Action |
|------------------|--|
| Package Location | Enter the full address of the software package location on the FTP or HTTP server. For example, use one of the following formats: <i>ftp://hostname/pathname/package-name</i> <i>http://hostname/pathname/package-name</i> |

Table 94: Install Package Maintenance Options (*Continued*)

| Field | Action |
|---|--|
| User | Enter the username to use on a remote server. |
| Password | Enter the password to use on a remote server. |
| Reboot If Required | Select the check box to automatically reboot when the upgrade is complete. |
| Do not save backup | Select the check box so that backup copy of the current Junos OS package is not saved. |
| Format and re-partition the media before installation | Select the check box to format the internal media with dual-root partitioning. |

2. Click **Fetch and Install Package**.

The software is activated after the device reboots.

RELATED DOCUMENTATION

[Rollback Software Package Version | 321](#)

Rollback Software Package Version

You are here: **Device Administration** > **Software Management** > **Rollback**.

You can rollback to the previously installed version of the device software.

To rollback software package version:

1. Click **Rollback** to rollback to the previous version of the software.

NOTE: You cannot stop the process once the rollback operation is requested.

2. Reboot the device when the rollback process is complete and for the new software to take effect. To reboot, perform the steps in "[Maintain Reboot Schedule](#)" on page 315 .

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

RELATED DOCUMENTATION

[Upload Software Packages](#) | 319

[Install Software Packages](#) | 320

Configuration Management

IN THIS CHAPTER

- [Manage Upload Configuration Files | 323](#)
- [Manage Configuration History | 324](#)
- [Manage Rescue Configuration | 328](#)

Manage Upload Configuration Files

You are here: **Device Administration** > **Configuration Management** > **Upload**.

You can compare two configuration files, download a configuration file to your local system, or roll back the configuration to any of the previous versions stored on the device.

To manage upload configuration files:

1. 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.

2. Click **Upload and Commit** to upload and commit the configuration.

The device checks the configuration for the correct syntax before committing it.

NOTE: The file configuration replaces the existing configuration and continues the upload and commit process. If any errors occur when the file is loading or committing, J-Web displays the error and restores the previous configuration.

RELATED DOCUMENTATION

[Manage Configuration History | 324](#)

Manage Configuration History

You are here: **Device Administration** > **Configuration Management** > **History**.

You can view configuration history and database information about users editing the configuration database.

To manage configuration history:

1. Complete the configuration according to the guidelines provided in [Table 95 on page 324](#) .

Table 95: History Maintenance Options

| Field | Function |
|-----------|--|
| Number | Indicates the version of the configuration file. To view a configuration, click the version number . |
| Date/Time | Indicates the date and time the configuration was committed. |
| User | Indicates the name of the user who committed the configuration. |

Table 95: History Maintenance Options (*Continued*)

| Field | Function |
|---------|--|
| 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. |

Table 95: History Maintenance Options (*Continued*)

| Field | Function |
|-------------|--|
| 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 Device Administration > Tools > CLI Editor option. • Imported upload [<i>filename</i>]—Configuration was uploaded with the Device Administration > Configuration Management > Upload option. • Modified via <i>quick-configuration</i>—Configuration was modified with the specified version of the J-Web user interface. • Rolled back via <i>user-interface</i>—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 95: History Maintenance Options (*Continued*)

| Field | Function |
|--------|---|
| Action | <p>Indicates action to perform with the configuration file.</p> <p>Select any one of the following available options:</p> <ul style="list-style-type: none"> Download—Downloads a configuration file to your local system. <p>Select the options on your Web browser to save the configuration file to a target directory on your local system.</p> <p>The file is saved as an ASCII file.</p> Rollback—Rolls back the configuration to any of the previous versions stored on the device. The History page displays the results of the rollback operation. <p>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.</p> |

2. To compare configurations files:

- a. Select any two configuration files you want to compare.
- b. Click **Compare**.

The History page 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.

RELATED DOCUMENTATION

[Manage Rescue Configuration | 328](#)

[Manage Upload Configuration Files | 323](#)

Manage Rescue Configuration

You are here: **Device Administration** > **Configuration Management** > **Rescue**.

If you inadvertently commit a configuration that denies management access, the only recourse may be to connect the console. Alternatively, you can rescue configuration that allows the management access to the device.

To load and commit the rescue configuration, press and immediately release the **Config** button on the chassis.

You can set or delete the rescue configuration.

To set or delete rescue configuration:

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 return to the Rescue page.
- **Delete rescue configuration**—Deletes the current rescue configuration. Click **OK** to confirm or **Cancel** to return to the Rescue page.

RELATED DOCUMENTATION

[Manage Your Licenses | 287](#)

[Manage Device Certificates](#)

Alarm Management

IN THIS CHAPTER

- [Monitor Chassis Alarm | 329](#)
- [Monitor System Alarm | 335](#)

Monitor Chassis Alarm

IN THIS SECTION

- [About Chassis Alarm Page | 329](#)
- [Create Chassis Alarm Definition | 329](#)
- [Edit Chassis Alarm Definition | 334](#)

About Chassis Alarm Page

You are here: **Device Administration** > **Alarm Management** > **Chassis Alarm**.

You can create a chassis alarm definition by selecting various options such as DS1, Ethernet, and integrated service, and so on.

Create Chassis Alarm Definition

To create Chassis Alarm Definition:

1. Enter the information specified in [Table 96 on page 330](#) to create Chassis Alarm Definition.

Table 96: Chassis Alarm Definition Options

| Chassis Component | Alarm Configuration Option |
|---------------------|---|
| DS1 | <p>Alarm indicator signal (ais)</p> <p>Yellow alarm (ylw)</p> <p>Select an alarm condition from the list for DS1:</p> <ul style="list-style-type: none"> • Ignore • Red • Yellow • None |
| Ethernet | <p>Link is down (link-down)</p> <p>Select an alarm condition from the list for Ethernet:</p> <ul style="list-style-type: none"> • Ignore • Red • Yellow • None |
| Integrated Services | <p>Hardware or software failure (failure)</p> <p>Select an alarm condition from the list for Integrated Services:</p> <ul style="list-style-type: none"> • Ignore • Red • Yellow • None |

Table 96: Chassis Alarm Definition Options (Continued)

| Chassis Component | Alarm Configuration Option |
|---|---|
| Management Ethernet | <p>Link is down (link-down)</p> <p>Select an alarm condition from the list for Management Ethernet:</p> <ul style="list-style-type: none"> • Ignore • Red • Yellow • None |
| Optical Transport Network Optical channel Data Unit (OTN ODU) | <p>Backward defect indication (odu-bdi)</p> <p>Payload type mismatch (odu-ptim)</p> <p>Trail trace identifier mismatch (odu-ttim)</p> <p>Select an alarm condition from the list for OTN ODU:</p> <ul style="list-style-type: none"> • Ignore • Red • Yellow • None |

Table 96: Chassis Alarm Definition Options (Continued)

| Chassis Component | Alarm Configuration Option |
|--|---|
| Optical Transport Network Optical channel Transport Unit (OTN OTU) | Loss of frame (oc-lof) Loss of multiframe (oc-lom) Loss of signal (oc-los) Backward defect indication (oc-bdi) Forward error correction excessive FEC errors (out-fec-excessive-errs) Incoming alignment error (out-iae) Trail trace identifier mismatch (out-ttim) Wavelength-Lock (Wavelength Lock) Select a alarm condition from the list for OTN OTU: <ul style="list-style-type: none"> • Ignore • Red • Yellow • None |
| Serial | Clear-to-send (CTS) signal absent (cts-absent) Data carrier detect (DCD) signal absent (dcd-absent) Data set ready (DSR) signal absent (dsr absent) Loss of receive clock (loss-of-rx-clock) Loss of transmit clock (loss-of-tx-clock) Select an alarm condition from the list for Serial: <ul style="list-style-type: none"> • Ignore • Red • Yellow • None |

Table 96: Chassis Alarm Definition Options (*Continued*)

| Chassis Component | Alarm Configuration Option |
|-------------------|---|
| Services | <p>Services module hardware down (hw-down)</p> <p>Services link down (linkdown)</p> <p>Services module held in reset (pic-hold-reset)</p> <p>Services module reset (pic-reset)</p> <p>Receive errors (rx-errors)</p> <p>Services module software down (sw-down)</p> <p>Transmit errors (tx-errors)</p> <p>Select an alarm condition from the list for Services:</p> <ul style="list-style-type: none"> • Ignore • Red • Yellow • None |

Table 96: Chassis Alarm Definition Options (Continued)

| Chassis Component | Alarm Configuration Option |
|-------------------|--|
| DS3 | Alarm indication signal (ais) Excessive number of zeros (exz) Far-end receive failure (ferf) Idle alarm (idle) Line code violation (lcv) Loss of frame (lof) Loss of signal (los) Phase-locked loop out of lock (pll) Yellow alarm (ylw) Select an alarm condition from the list for DS3: <ul style="list-style-type: none"> • Ignore • Red • Yellow • None |

2. Click **OK** to create Chassis Alarm Definition.

The Chassis Alarm Definition page appears.

3. Click **Cancel** to cancel your entries and returns to the Chassis Alarm Definition page.

Edit Chassis Alarm Definition

To edit Chassis Alarm Definition:

1. Click the pencil icon available on the upper-right corner of the Chassis Alarm Definition page.

See [Table 96 on page 330](#) for the options available for editing the Chassis Alarm Definition page.

2. Click **OK**.

RELATED DOCUMENTATION

| [Monitor System Alarm](#) | 335

Monitor System Alarm

IN THIS SECTION

- [About System Alarm Page | 335](#)
- [Create System Alarm Configuration | 335](#)
- [Edit System Alarm Configuration | 339](#)

About System Alarm Page

You are here: **Device Administration** > **Alarm Management** > **System Alarm**.

You can enable system login alarm login classes. The configured Login Classes will display system alarms while logging in.

Create System Alarm Configuration

To create System Alarm Configuration:

1. Enter the information specified in [Table 97 on page 335](#) to create System Alarm Configuration.

Table 97: RPM Information Troubleshooting Options

| Field | Function |
|--------------------------------|--|
| 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. |

Table 97: RPM Information Troubleshooting Options (*Continued*)

| Field | Function |
|------------------------|--|
| Probe Type | <p>Type of RPM probe configured for the specified test. Following are valid probe types:</p> <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 | <p>Explicitly configured source address that is included in the probe packet headers.</p> <p>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.</p> |
| 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 97: RPM Information Troubleshooting Options *(Continued)*

| Field | Function |
|------------------------------------|--|
| 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. |

Table 97: RPM Information Troubleshooting Options (*Continued*)

| Field | Function |
|--------------------------------------|--|
| 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. |
| 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. |

2. Click **OK** to create System Alarm Configuration.
System Alarm Configuration page appears.

3. Click **Cancel** to cancel your entries and returns to the System Alarm Configuration page.

Edit System Alarm Configuration

To edit System Alarm Configuration:

1. Click the pencil icon available on the upper-right corner of the System Alarm Configuration page.
See [Table 97 on page 335](#) for the options available for editing the System Alarm Configuration page.
2. Click **OK**.

SEE ALSO

| [Monitor Chassis Alarm | 329](#)

RPM

IN THIS CHAPTER

- Setup RPM | 340
- View RPM | 349

Setup RPM

IN THIS SECTION

- Problem | 340
- Solution | 340

Problem

Description

You are here: **Device Administration** > **RPM** > **Setup RPM**.

You can configure RPM parameters to monitor real-time performance through the J-Web interface. You can specify an RPM owner, request information related to probe, hardware timestamp, generates Traps, and specify a probe server.

Solution

To configure RPM parameters:

1. Enter the information specified in [Table 98 on page 341](#) to troubleshoot the issue.
2. 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 98: RPM Setup Troubleshooting Options

| Field | Function |
|--------------------------------|---|
| Probe Owners | |
| Identification | |
| Owner Name | <p>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).</p> <p>Type the name of the RPM owner.</p> |
| Performance Probe Tests | |
| Identification | |
| Test name | <p>Specifies a unique name to identify the RPM test.</p> <p>Type the name of the RPM test.</p> |
| Target (Address or URL) | <p>Specifies an IP address or a URL of a probe target.</p> <p>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://.</p> |
| Source Address | <p>Specifies an IP address to be used as the probe source address.</p> <p>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.</p> |

Table 98: RPM Setup Troubleshooting Options (*Continued*)

| Field | Function |
|----------------------------|---|
| Routing Instance | <p>Specifies a routing instance over which the probe is sent.</p> <p>Type the routing instance name. The routing instance applies only to probes of type <code>icmp</code> and <code>icmp-timestamp</code>. The default routing instance is <code>inet.0</code>.</p> |
| History Size | <p>Specifies the number of probe results saved in the probe history.</p> <p>Type a number between 0 and 255. The default history size is 50 probes.</p> |
| Request Information | |
| Probe Type | <p>Specifies the type of probe to send as part of the test.</p> <p>Select the desired probe type from the list:</p> <ul style="list-style-type: none"> • <code>http-get</code> • <code>http-get-metadata</code> • <code>icmp-ping</code> • <code>icmp-ping-timestamp</code> • <code>tcp-ping</code> • <code>udp-ping</code> |
| Interval | <p>Specifies the wait time (in seconds) between each probe transmission.</p> <p>Type a number between 1 and 255 (seconds).</p> |
| Test Interval | <p>Specifies the wait time (in seconds) between tests.</p> <p>Type a number between 0 and 86400 (seconds).</p> |

Table 98: RPM Setup Troubleshooting Options (*Continued*)

| Field | Function |
|---------------------------|---|
| Probe Count | <p>Specifies the total number of probes to be sent for each test.</p> <p>Type a number between 1 and 15.</p> |
| Moving Average Size | <p>Specifies the number of samples used for a moving average.</p> <p>Type a number between 0 and 225.</p> |
| Destination Port | <p>Specifies the TCP or UDP port to which probes are sent.</p> <p>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.</p> <p>Type the number 7—a standard TCP or UDP port number—or a port number from 49152 through 65535.</p> |
| DSCP Bits | <p>Specifies the Differentiated Services code point (DSCP) bits. This value must be a valid 6-bit pattern. The default is 000000.</p> <p>Type a valid 6-bit pattern.</p> |
| Data Size | <p>Specifies the size of the data portion of the ICMP probes.</p> <p>Type a size (in bytes) between 0 and 65507.</p> |
| Data Fill | <p>Specifies the contents of the data portion of the ICMP probes.</p> <p>Type a hexadecimal value between 1 and 800h to use as the contents of the ICMP probe data.</p> |
| Hardware Timestamp | |

Table 98: RPM Setup Troubleshooting Options (*Continued*)

| Field | Function |
|---------------------------------|--|
| One Way Hardware Timestamp | <p>Specifies the hardware timestamps for one-way measurements.</p> <p>To enable one-way timestamping, select the check box.</p> |
| Hardware Timestamp | <p>Specifies timestamping of RPM probe messages. You can timestamp the following RPM probes to improve the measurement of latency or jitter:</p> <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 <p>To enable timestamping, select the check box.</p> |
| Destination Interface | <p>Specifies the name of an output interface for probes.</p> <p>Select the interface from the list.</p> |
| Maximum Probe Thresholds | |
| Successive Lost Probes | <p>Specifies the total number of probes that must be lost successively to trigger a probe failure and generate a system log message.</p> <p>Type a number between 0 and 15.</p> |
| Lost Probes | <p>Specifies the total number of probes that must be lost to trigger a probe failure and generate a system log message.</p> <p>Type a number between 0 and 15.</p> |

Table 98: RPM Setup Troubleshooting Options (*Continued*)

| Field | Function |
|--------------------|--|
| Round Trip Time | <p>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.</p> <p>Type a number between 0 and 60,000,000 (microseconds).</p> |
| Jitter | <p>Specifies the total jitter (in microseconds) for a test that triggers a probe failure and generates a system log message.</p> <p>Type a number between 0 and 60,000,000 (microseconds).</p> |
| Standard Deviation | <p>Specifies the maximum allowable standard deviation (in microseconds) for a test, which, if exceeded, triggers a probe failure and generates a system log message.</p> <p>Type a number between 0 and 60,000,000 (microseconds).</p> |
| Egress Time | <p>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.</p> <p>Type a number between 0 and 60,000,000 (microseconds).</p> |
| Ingress Time | <p>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.</p> <p>Type a number between 0 and 60,000,000 (microseconds)</p> |
| Jitter Egress Time | <p>Specifies the total outbound-time jitter (in microseconds) for a test that triggers a probe failure and generates a system log message.</p> <p>Type a number between 0 and 60,000,000 (microseconds)</p> |

Table 98: RPM Setup Troubleshooting Options (*Continued*)

| Field | Function |
|------------------------------------|--|
| Jitter Ingress Time | <p>Specifies the total inbound-time jitter (in microseconds) for a test that triggers a probe failure and generates a system log message.</p> <p>Type a number between 0 and 60,000,000 (microseconds).</p> |
| Egress Standard Deviation | <p>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.</p> <p>Type a number between 0 and 60,000,000 (microseconds).</p> |
| Ingress Standard Deviation | <p>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.</p> <p>Type a number between 0 and 60,000,000 (microseconds).</p> |
| Traps | |
| Egress Jitter Exceeded | <p>Generates SNMP traps when the threshold for jitter in outbound time is exceeded.</p> <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 | <p>Generates SNMP traps when the threshold for standard deviation in outbound times is exceeded.</p> <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 98: RPM Setup Troubleshooting Options (*Continued*)

| Field | Function |
|-------------------------------------|---|
| Egress Time Exceeded | <p>Generates SNMP traps when the threshold for maximum outbound time is exceeded.</p> <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 | <p>Generates SNMP traps when the threshold for jitter in inbound time is exceeded.</p> <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 | <p>Generates SNMP traps when the threshold for standard deviation in inbound times is exceeded.</p> <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 | <p>Generates traps when the threshold for maximum inbound time is exceeded.</p> <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 | <p>Generates traps when the threshold for jitter in round-trip time is exceeded.</p> <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 98: RPM Setup Troubleshooting Options (*Continued*)

| Field | Function |
|--|---|
| Probe Failure | <p>Generates traps when the threshold for the number of successive lost probes is reached.</p> <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 | <p>Generates traps when the threshold for maximum round-trip time is exceeded.</p> <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 | <p>Generates traps when the threshold for standard deviation in round-trip times is exceeded.</p> <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 | <p>Generates traps when a test is completed.</p> <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 Failure | <p>Generates traps when the threshold for the total number of lost probes is reached.</p> <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 | |

Table 98: RPM Setup Troubleshooting Options (*Continued*)

| Field | Function |
|-------------------------------------|--|
| 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. |

RELATED DOCUMENTATION

[View RPM | 349](#)

View RPM

IN THIS SECTION

- [Problem | 350](#)
- [Solution | 350](#)

Problem

Description

You are here: **Device Administration > RPM > View RPM.**

You can configure the RPM probes, to view the RPM statistics and to ensure that the device is configured to receive and transmit TCP and UDP RPM probes on correct ports.

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. Enter the information specified in [Table 99 on page 350](#).

Table 99: RPM Information Troubleshooting Options

| Field | Function |
|--------------------------------|--|
| 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. |

Table 99: RPM Information Troubleshooting Options (*Continued*)

| Field | Function |
|------------------------|--|
| Probe Type | <p>Type of RPM probe configured for the specified test. Following are valid probe types:</p> <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 | <p>Explicitly configured source address that is included in the probe packet headers.</p> <p>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.</p> |
| 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 99: RPM Information Troubleshooting Options (*Continued*)

| Field | Function |
|------------------------------------|--|
| 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. |

Table 99: RPM Information Troubleshooting Options (*Continued*)

| Field | Function |
|--------------------------------------|--|
| 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. |
| 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. |

RELATED DOCUMENTATION

| [Setup RPM | 340](#)

Tools

IN THIS CHAPTER

- [Troubleshoot Ping Host | 355](#)
- [Troubleshoot Ping MPLS | 359](#)
- [Troubleshoot Traceroute | 365](#)
- [Control Plane Packet Capture | 368](#)
- [About the Data Plane Packet Capture Page | 375](#)
- [Access CLI | 379](#)
- [View CLI Configuration | 381](#)
- [Edit CLI Configuration | 382](#)
- [Point and Click CLI | 383](#)

Troubleshoot Ping Host

IN THIS SECTION

- [About Ping Host Page | 355](#)

About Ping Host Page

You are here: **Device Administration** > **Tools** > **Ping Host**.

The ping diagnostic tool sends a series of ICMP "echo request" packets to the specified remote host.

The receipt of such packets will usually result in the remote host replying with an ICMP "echo response." Note that some hosts are configured not to respond to ICMP "echo requests," so a lack of responses does not necessarily represent a connectivity problem. Also, some firewalls block the ICMP packet types that ping uses, so you may find that you are not able to ping outside your local network.

You can ping a host to verify that the host can be reached over the network or not.

To use the ping host tool:

1. Enter the information specified in [Table 100 on page 356](#) to troubleshoot the issue.

The Remote Host field is the only required field.

2. Click the expand icon next to Advanced options.

3. Click **Start**.

The results of the ping operation are displayed in [Table 101 on page 358](#) . 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
```

4. Click **OK** to stop the ping operation before it is complete.

Table 100: Ping Host Troubleshooting Options

| Field | Action |
|-------------------------|--|
| Remote Host | Type the hostname or IP address of the host to ping. |
| Advanced Options | |
| Don't Resolve Addresses | <ul style="list-style-type: none"> • To suppress the display of the hop hostnames along t the path, select the check box. • To display the hop hostnames along the path, clear the check box. |
| Interface | 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 | From the list, select the number of ping requests to send. |
| Don't Fragment | <ul style="list-style-type: none"> • To set the don't fragment (DF) bit in the IP header of the ping request packet, select the check box. • To clear the DF bit in the IP header of the ping request packet, clear the check box. |

Table 100: Ping Host Troubleshooting Options (Continued)

| Field | Action |
|------------------|--|
| Record Route | <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 | From the list, select the decimal value of the ToS in the IP header of the ping request packet. |
| Routing Instance | From the list, select the routing instance name for the ping attempt. |
| Interval | From the list, select the interval in seconds, between the transmission of each ping request. |
| Packet Size | 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 | Type the source IP address of the ping request packet. |
| Time-to-Live | From the list, select the TTL hop count for the ping request packet. |
| Bypass Routing | <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. <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> |

Table 101: Ping Host Results and Output Summary

| Field | Function |
|--|---|
| <i>bytes bytes from ip-address</i> | <ul style="list-style-type: none"> • <i>bytes</i>—Size of ping response packet, which is equal to the value you entered in the Packet Size box, plus 8. • <i>ip-address</i>—IP address of destination host that sent the ping response packet. |
| <i>icmp_seq=0</i> <i>icmp_seq=number</i> | <i>time</i> —Sequence Number field of the ping response packet. You can use this value to match the ping response to the corresponding ping request. |
| <i>ttl=number</i> | <i>number</i> —TTL hop-count value of the ping response packet. |
| <i>time=time</i> | <i>time</i> —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 packets transmitted</i> | <i>number</i> —Number of ping requests (probes) sent to host. |
| <i>number packets received</i> | <i>number</i> —Number of ping responses received from host. |
| <i>percentage packet loss</i> | <i>percentage</i> —Number of ping responses divided by the number of ping requests, specified as a percentage. |
| <i>round-trip min/avg/max/ stddev = min-time/ avg-time/ max-time/ std-dev ms</i> | <ul style="list-style-type: none"> • <i>min-time</i>—Minimum round-trip time (see <i>time=time</i> field in this table). • <i>avg-time</i>—Average round-trip time. • <i>max-time</i>—Maximum round-trip time. • <i>std-dev</i>—Standard deviation of the round-trip times. |

Table 101: Ping Host Results and Output Summary (*Continued*)

| Field | Function |
|-------------------------------------|--|
| 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> |

RELATED DOCUMENTATION

[Troubleshoot Ping MPLS | 359](#)

[Troubleshoot Traceroute | 365](#)

[Control Plane Packet Capture | 368](#)

Troubleshoot Ping MPLS

IN THIS SECTION

- [About Ping MPLS Page | 360](#)

About Ping MPLS Page

You are here: **Device Administration** > **Tools** > **Ping MPLS**.

You can send variations of ICMP "echo request" packets to the specified MPLS endpoint.

To use the ping MPLS tool:

1. Click the expand icon next to the ping MPLS option you want to use.
2. Enter information specified in [Table 102 on page 360](#) to troubleshoot the issue.
3. Click **Start**.

The results of the ping operation are displayed in [Table 103 on page 363](#).

4. Click **OK** to stop the ping operation before it is complete.

Table 102: Ping MPLS Troubleshooting Options

| Field | Action |
|-------------------------------|--|
| Ping RSVP-signaled LSP | |
| LSP Name | Type the name of the LSP to ping. |
| Source Address | Type the source IP address of the ping request packet—a valid address configured on a J Series device interface. |
| Count | From the list, select the number of ping requests to send. The default is 5 requests. |
| Detailed Output | Select the check box to display detailed output rather than brief ping output. |
| Ping LDP-signaled LSP | |
| FEC Prefix | Type the forwarding equivalence class (FEC) prefix and length of the LSP to ping. |
| Source Address | Type the source IP address of the ping request packet—a valid address configured on a J Series device interface. |
| Count | From the list, select the number of ping requests to send. The default is 5 requests. |

Table 102: Ping MPLS Troubleshooting Options (Continued)

| Field | Action |
|---|---|
| Detailed Output | Select the check box to display detailed output rather than brief ping output. |
| Ping LSP to Layer 3 VPN prefix | |
| Layer 3 VPN Name | Type the name of the VPN to ping. |
| Count | From the list, select the number of ping requests to send. The default is 5 requests. |
| Detailed Output | Select the check box to display detailed output rather than brief ping output. |
| VPN Prefix | Type the IP address prefix and length of the VPN to ping. |
| Source Address | Type the source IP address of the ping request packet—a valid address configured on a J Series device interface. |
| Ping LSP for a Layer 2 VPN connection by interface | |
| Interface | 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. (See the interface naming conventions in the Junos OS Interfaces Configuration Guide for Security Devices .) |
| Source Address | Type the source IP address of the ping request packet—a valid address configured on a J series device interface. |
| Count | From the list, select the number of ping requests to send. The default is 5 requests. |
| Detailed Output | Select the check box to display detailed output rather than brief ping output. |
| Ping LSP for a Layer 2 VPN connection by instance | |
| Layer 2VPN Name | Type the name of the Layer 2 VPN to ping. |

Table 102: Ping MPLS Troubleshooting Options (Continued)

| Field | Action |
|------------------------|--|
| Remote Site Identifier | Type the remote site identifier of the Layer 2 VPN to ping. |
| Source Address | Type the source IP address of the ping request packet—a valid address configured on a J Series device interface. |
| Local Site Identifier | Type the local site identifier of the Layer 2 VPN to ping. |
| Count | From the list, select the number of ping requests to send. The default is 5 requests. |
| Detailed Output | Select the check box to display detailed output rather than brief ping output. |

Ping LSP to a Layer 2 circuit remote site by interface

| | |
|-----------------|---|
| Interface | 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 | Type the source IP address of the ping request packet—a valid address configured on a J Series device interface. |
| Count | From the list, select the number of ping requests to send. The default is 5 requests. |
| Detailed Output | Select the check box to display detailed output rather than brief ping output. |

Ping LSP to a Layer 2 circuit remote site by VCI

| | |
|--------------------|--|
| Remote Neighbor | Type the IP address of the remote neighbor (PE router) within the virtual circuit to ping. |
| Circuit Identifier | Type the virtual circuit identifier for the Layer 2 circuit. |
| Source Address | Type the source IP address of the ping request packet—a valid address configured on a J Series device interface. |

Table 102: Ping MPLS Troubleshooting Options (Continued)

| Field | Action |
|-----------------------------|--|
| Count | From the list, select the number of ping requests to send. |
| Detailed Output | Select the check box to display detailed output rather than brief ping output. |
| Ping endpoint of LSP | |
| VPN Prefix | Type either the LDP FEC prefix and length or the RSVP LSP endpoint address for the LSP to ping. |
| Source Address | Type the source IP address of the ping request packet—a valid address configured on a J Series device interface. |
| Count | From the list, select the number of ping requests to send. |
| Detailed Output | Select the check box to display detailed output rather than brief ping output. |

Table 103: Ping MPLS Results and Output Summary

| Field | Function |
|--|---|
| 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. |
| <i>number</i> packets transmitted | <i>number</i> —Number of ping requests (probes) sent to a host. |
| <i>number</i> packets received | <i>number</i> —Number of ping responses received from a host. |

Table 103: Ping MPLS Results and Output Summary (*Continued*)

| Field | Function |
|-------------------------------------|--|
| <i>percentage packet loss</i> | <i>percentage</i> —Number of ping responses divided by the number of ping requests, specified as a percentage. |
| 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. |

RELATED DOCUMENTATION

[Troubleshoot Traceroute | 365](#)

[Control Plane Packet Capture | 368](#)

Troubleshoot Traceroute

IN THIS SECTION

- [About Traceroute Page | 365](#)

About Traceroute Page

You are here: **Device Administration** > **Tools** > **Traceroute**.

The traceroute diagnostic tool uses a series of packets crafted to elicit an ICMP "time exceeded" messages from intermediate points in the network between your device and the specified host.

The time-to-live for a packet is decremented each time the packet is routed, so traceroute generally receives at least one "time exceeded" response from each waypoint. Traceroute starts with a packet with a time-to-live value of one, and increments the time to live for subsequent packets, thereby constructing a rudimentary map of the path between hosts.

Use this page to display a list of routers between the device and a specified destination host.

To use the traceroute tool:

1. Click the expand icon next to Advanced options.
2. Enter information in the Traceroute page as described in [Table 104 on page 366](#).

The Remote Host field is the only required field.

3. Click **Start**.

The results of the traceroute operation are displayed in [Table 105 on page 367](#). 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.

4. Click **OK** to stop the traceroute operation before it is complete.

Table 104: Ping Traceroute Troubleshooting Options

| Field | Action |
|-------------------------|---|
| Remote Host | Type the hostname or IP address of the destination host of the traceroute. |
| Advanced Options | |
| Don't Resolve Addresses | <ul style="list-style-type: none"> To suppress the display of the hop hostnames along the path, select the check box. To display the hop hostnames along the path, clear the check box. |
| Interface | 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 | From the list, select the time-to-live (TTL) hop count for the traceroute request packet. |
| Type-of-Service | From the list, select the decimal value of the type-of-service (ToS) value to include in the IP header of the traceroute request packet. |
| Resolve AS Numbers | <ul style="list-style-type: none"> To display the autonomous system (AS) number of each intermediate hop between the device and the destination host, select the check box. To suppress the display of the AS number of each intermediate hop between the device and the destination host, clear the check box. |
| Routing Instance | From the list, select the routing instance name for the ping attempt. |
| Gateway | Type the gateway IP address to route through. |
| Source Address | Type the source IP address of the outgoing traceroute packets. |

Table 104: Ping Traceroute Troubleshooting Options (*Continued*)

| Field | Action |
|----------------|---|
| Bypass Routing | <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. <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> |

Table 105: Ping Traceroute Results and Output Summary

| Field | Function |
|---|--|
| Ping Traceroute Results and Output Summary | |
| <i>hop-number</i> | Number of the hop (router) along the path. |
| <i>host</i> | <p>Hostname, if available, or IP address of the router.</p> <p>To suppress the display of the hostname, select the Don't Resolve Addresses check box.</p> |
| <i>ip-address</i> | IP address of the router. |
| <i>as-number</i> | AS number of the router. |
| <i>time1</i> | Round-trip time between the sending of the first traceroute packet and the receiving of the corresponding Time Exceeded packet from that particular router. |
| <i>time2</i> | Round-trip time between the sending of the second traceroute packet and the receiving of the corresponding Time Exceeded packet from that particular router. |
| <i>time3</i> | 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 105: Ping Traceroute Results and Output Summary *(Continued)*

| Field | Function |
|--|--|
| 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> |

RELATED DOCUMENTATION

[Control Plane Packet Capture | 368](#)

Control Plane Packet Capture

IN THIS SECTION

- [About the Control Plane Packet Capture Page | 368](#)

About the Control Plane Packet Capture Page

You are here: **Device Administration** > **Tools** > **Control Plane Packet Capture**.

You can quickly capture and analyze router control traffic on a device.

The packet capture diagnostic tool allows inspection of control traffic (not transient traffic). The summary of each decoded packet is displayed as it is captured. Captured packets are written to a PCAP file which can be downloaded.

NOTE: Starting in Junos OS Release 19.3R1, J-Web supports RE3 line cards for SRX5000 line of devices.

To use J-Web Control Plane Packet Capture:

1. Enter the information specified in [Table 106 on page 369](#) to troubleshoot the issue.
2. Save the captured packets to a file or specify other advanced options by clicking the expand icon next to Advanced options.
3. Click **Start**.

The captured packet headers are decoded and displayed in the Packet Capture display as specified in [Table 107 on page 374](#).

4. 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 106: Packet Capture Troubleshooting Options

| Field | Description |
|-----------|--|
| Interface | <p>Specifies the interface on which the packets are captured.</p> <p>From the list, select an interface—for example, ge-0/0/0.</p> <p>If you select default, packets on the Ethernet management port 0 are captured.</p> |

Table 106: Packet Capture Troubleshooting Options (*Continued*)

| Field | Description |
|--------------|---|
| 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. <p>From the list, select Detail.</p> |
| 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> <p>From the list, select the number of packets to be captured—for example, 10.</p> |
| 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 106: Packet Capture Troubleshooting Options (*Continued*)

| Field | Description |
|-------------------------|--|
| Protocols | <p>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.</p> <p>From the list, select a protocol—for example:</p> <ol style="list-style-type: none"> 1. Select a protocol from the list. 2. Click Add. |
| Ports | <p>Matches the packet headers containing the specified source or destination TCP or UDP port number or port name.</p> <p>Select a direction and a port. For example:</p> <ol style="list-style-type: none"> 1. From the Direction list, select src. 2. In the Port box, type 23. 3. Click Add. |
| Advanced Options | |
| Absolute TCP Sequence | <p>Displays the absolute TCP sequence numbers for the packet headers.</p> <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 | <p>Displays the link-layer packet headers.</p> <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. |

Table 106: Packet Capture Troubleshooting Options (*Continued*)

| Field | Description |
|-----------------------|--|
| 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 | <p>Displays packet headers, except link-layer headers, in hexadecimal format.</p> <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 | <p>Displays packet headers in hexadecimal and ASCII formats.</p> <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. |

Table 106: Packet Capture Troubleshooting Options (*Continued*)

| Field | Description |
|-------------------------|---|
| 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> <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.</p> |
| Packet Size | <p>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.</p> <p>Type the number of bytes you want to capture for each packet header—for example, 256.</p> |
| Don't Resolve Addresses | <p>Specifies that IP addresses are not to be resolved into hostnames in the packet headers displayed.</p> <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 | <p>Suppresses the display of packet header timestamps.</p> <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. |

Table 106: Packet Capture Troubleshooting Options (*Continued*)

| Field | Description |
|---------------------------|--|
| 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. |

Table 107: Packet Capture Results and Output Summary

| Field | Function |
|----------------|--|
| 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> |
| Source Address | <p>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.</p> <p>NOTE: When a string is defined for the port, the packet capture output displays the string instead of the port number.</p> |

Table 107: Packet Capture Results and Output Summary (Continued)

| Field | Function |
|---------------------|---|
| Destination Address | <p>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.</p> <p>NOTE: When a string is defined for the port, the packet capture output displays the string instead of the port number.</p> |
| Protocol | <p>Displays the protocol for the packet.</p> <p>In the sample output, TCP indicates the Layer 4 protocol.</p> |
| Data Size | Displays the size of the packet (in bytes). |

Change History Table

Feature support is determined by the platform and release you are using. Use [Feature Explorer](#) to determine if a feature is supported on your platform.

| Release | Description |
|---------|---|
| 19.3R1 | Starting in Junos OS Release 19.3R1, J-Web supports RE3 line cards for SRX5000 line of devices. |

RELATED DOCUMENTATION

| [Troubleshoot Traceroute](#) | [365](#)

About the Data Plane Packet Capture Page

You are here: [Device Administration](#) > [Tools](#) > [Data Plane Packet Capture](#).

NOTE: This menu is supported for only SRX4600 devices and SRX5000 line of devices.

Starting in Junos OS 23.1R1 Release, you can quickly capture and analyze router data plane traffic on a device.

The packet capture diagnostic tool allows inspection of data plane traffic. The summary of each decoded packet is displayed as it is captured. Captured packets are written to a PCAP file which can be downloaded.

Capture the packet information from the operational mode without committing the configurations and with a minimal impact to the production system. You can define the packet filter to trace the traffic type based on your requirement.

To capture the data plane packet details:

1. Complete the configuration according to the guidelines provided in [Table 108 on page 376](#).

NOTE: To capture the packet information, you must provide at least one filter option from either Basic Filter or Source & Destination Filter.

2. Click **Start Packet Capture**.

The packet capturing starts, and the Data Plane Packet Capture page becomes read-only. You can navigate to other pages while the packet capture process is in progress.

3. Click **Stop Packet Capture**.

The packet capturing stops and the PCAP file is automatically downloaded to your system from the /var/log/ folder. To view the packet capture file in the J-Web UI, navigate to **Device Administration > Operations > Files** and then click **Log files**.

NOTE:

- You can only request one packet capture at a time, and you must stop each request before starting another.
- When a count limit is reached, the capture stops. Click **Stop Packet Capture** to download the PCAP file.

Table 108: Fields on the Data Plane Packet Capture Page

| Field | Description |
|---------------------|-------------|
| Basic Filter | |

Table 108: Fields on the Data Plane Packet Capture Page (*Continued*)

| Field | Description |
|--|---|
| Protocol | Select a protocol from the list to associate with the packet capture filter. You can search for a protocol name or a protocol number in the list. Range: 0 (HOPOPT) through 255 (Reserved). |
| Multitenancy type | Select one of the multitenancy type to filter the interface: Default, Tenant, or Logical System. |
| Logical interface | Select a logical interface from the list for the selected root logical system. |
| Tenant | Select a tenant name from the list. |
| Tenant logical interface | Select a logical interface from the list for the selected tenant. |
| Logical system | Select a logical system name from the list. |
| Logical system interface | Select a logical interface from the list for the selected logical system. |
| Source & Destination Filter | |
| Bidirectional | With this option enabled by default, J-Web collects bidirectional information such as traffic from source port to destination port and vice-versa. NOTE: To capture the packet information, you must provide at least one filter option from Source & Destination Filter. |
| Source port | Enter source port number (for example, 0). Port number: 0 through 65535. |

Table 108: Fields on the Data Plane Packet Capture Page (*Continued*)

| Field | Description |
|---------------------------|--|
| Source prefix | Enter source IPv4 or IPv6 address prefix to filter the packets. |
| Destination port | Enter destination port number (for example, 0). Port number: 0 through 65535. |
| Destination prefix | Enter destination IPv4 or IPv6 address prefix to filter the packets. |
| Additional Options | |
| Packet capture file name | Enter a packet capture file name. You can view the PCAP file using the Wireshark. Default file name is packet-capture . |
| Maximum file size | Select the maximum size of the packet capture file. Range: 1 through 1024. Default is 5 MB. |
| Maximum capture size | Select the maximum packet capture length. The packet truncates if the capture length is more than the specified length. Range: 68 through 10000. Default is 1514. |
| Packet limit | Select the packet capture limit value. The packet capture ends when the packets count limit is reached. Range: 10 through 1000000. Default is 100. |

RELATED DOCUMENTATION

[Access CLI | 379](#)

[Control Plane Packet Capture | 368](#)

Access CLI

IN THIS SECTION

- [About CLI Terminal Page | 379](#)

About CLI Terminal Page

IN THIS SECTION

- [CLI Terminal Requirements | 379](#)
- [CLI Overview | 380](#)

You are here: **Device Administration** > **Tools** > **CLI Terminal**.

The Junos CLI provides a set of commands for monitoring and configuring a routing platform. Use this page to access Junos OS CLI through J-Web interface.

This topic includes the following sections:

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.
- **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](#).

RELATED DOCUMENTATION

| [View CLI Configuration](#) | 381

View CLI Configuration

IN THIS SECTION

- [About CLI Viewer Page](#) | 381

About CLI Viewer Page

You are here: **Device Administration** > **Tools** > **CLI Viewer**.

You can view 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.

- Uncommitted configuration changes will also be listed.

To save, commit, or cancel the current configuration:

1. Click one:

- **OK**—Saves the configuration and returns to the CLI Viewer page.
- **Commit Options > Commit**—Commits the configuration and returns to the CLI Viewer page.
- **Cancel**—Cancels your entries and returns to the CLI Viewer page.

RELATED DOCUMENTATION

| [Edit CLI Configuration](#) | 382

Edit CLI Configuration

IN THIS SECTION

- [About CLI Editor Page](#) | 382

About CLI Editor Page

You are here: **Device Administration > Tools > CLI Editor**.

You can configure all routing platform services that you can configure from the Junos CLI prompt.

To edit the CLI configuration:

1. 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.
2. 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.

3. Click one:

- **OK**—Saves the configuration and returns to the CLI Editor page.
- **Commit Options>Commit**—Commits the configuration and returns to the CLI Editor page.
- **Cancel**—Cancels your entries and returns to the CLI Editor 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*.

RELATED DOCUMENTATION

| [Point and Click CLI | 383](#)

Point and Click CLI

IN THIS SECTION

- [About Point and Click CLI Page | 383](#)

About Point and Click CLI Page

You are here: **Device Administration > Tools > Point and Click CLI.**

You can edit configuration on a series of pages of clickable options.

1. To edit the configuration on a series of pages of clickable options that step you through the hierarchy, enter the information specified in [Table 109 on page 384](#) . [Table 110 on page 385](#) 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 109: Point and Click Configuration Details

| Field | Description |
|---------------|---|
| Configuration | <p>Specifies that you can edit the selected configuration on a series of pages of clickable options that step you through the hierarchy.</p> <p>Click an option:</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. |

Table 110: J-Web Configuration Editor Page Details

| Field | Function |
|---------------------------|--|
| 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"> • Configure—Configures the feature. • Edit—Edits the feature. • Delete—Deletes the feature. |
| Accounting options | <p>Specifies that you can configure accounting options such as log data about basic system operations and services on the device. The option available is:</p> <ul style="list-style-type: none"> • Configure—Configures the feature. |
| Applications | <p>Specifies that you can edit or delete applications functions of the Junos OS and their properties on the device. The options available are:</p> <ul style="list-style-type: none"> • Edit—Edits the feature • Delete—Deletes the feature. |
| Chassis | <p>Specifies that you can configure alarms and other chassis properties on the device. The option available is:</p> <ul style="list-style-type: none"> • Configure—Configures the feature. • Edit—Edits the feature. • Delete—Deletes the feature. |
| Class of service | <p>Specifies that you can edit or delete the Class-of-Service feature. The options available are:</p> <ul style="list-style-type: none"> • Edit—Edits the feature • Delete—Deletes the feature. |

Table 110: J-Web Configuration Editor Page Details (*Continued*)

| Field | Function |
|----------------------------|--|
| Ethernet switching options | <p>Specifies that you can configure Ethernet switching options on the device. The option available is:</p> <ul style="list-style-type: none"> • Configure—Configures the feature. |
| Event options | <p>Specifies that you can configure diagnostic event policies and actions associated with each policy. The option available is:</p> <ul style="list-style-type: none"> • Configure—Configures the feature. |
| Firewall | <p>Specifies that you can configure stateless firewall filters—also known as ACLs—on the device. The option available is:</p> <ul style="list-style-type: none"> • Configure—Configures the feature. |
| Forwarding options | <p>Specifies that you can configure forwarding option protocols, including flow monitoring, accounting properties, and packet capture. The option available is:</p> <ul style="list-style-type: none"> • Configure—Configures the feature. |
| Interfaces | <p>Specifies that you can edit or delete interfaces on the device. The options available are:</p> <ul style="list-style-type: none"> • Edit—Edits the feature. • Delete—Deletes the feature. |
| Multicast snooping options | <p>Specifies that you can configure multicast snooping options. The option available is:</p> <ul style="list-style-type: none"> • Configure—Configures the feature. |

Table 110: J-Web Configuration Editor Page Details (*Continued*)

| Field | Function |
|--------------------------|---|
| Poe | <p>Specifies that you can edit or delete Power over Ethernet options on the device. The options available are:</p> <ul style="list-style-type: none"> • Edit—Edits the feature. • Delete—Deletes the feature. |
| Policy options | <p>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:</p> <ul style="list-style-type: none"> • Configure—Configures the feature. |
| Protocols | <p>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:</p> <ul style="list-style-type: none"> • Edit—Edits the feature. • Delete—Deletes the feature. |
| Routing instances | <p>Specifies that you can configure a hierarchy to configure routing instances. The options available re:</p> <ul style="list-style-type: none"> • Configure—Configures the feature. |
| Routing options | <p>Specifies that you can edit or delete protocol-independent routing properties. The options available are:</p> <ul style="list-style-type: none"> • Edit—Edits the feature. • Delete—Deletes the feature. |
| Schedulers | <p>Specifies that you can determine the day and time when security policies are in effect. The option available is:</p> <ul style="list-style-type: none"> • Configure—Configures the feature. |

Table 110: J-Web Configuration Editor Page Details (*Continued*)

| Field | Function |
|-----------------|--|
| 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. |
| 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. • Edit—Edits the feature. • Delete—Deletes the feature. |
| 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. |
| 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. |

Table 110: J-Web Configuration Editor Page Details (*Continued*)

| Field | Function |
|-----------------------|---|
| 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. |
| 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. |
| 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. |
| Access profile | |
| Access profile name | Enter the access profile name. |
| Advanced | |
| Add new entry | Click Add new entry to add a new identifier. |

RELATED DOCUMENTATION

| [Edit CLI Configuration](#) | 382

Reset Configuration

IN THIS CHAPTER

- [Reset Configuration and Rerun Setup Wizard | 390](#)

Reset Configuration and Rerun Setup Wizard

You are here: [Device Administration](#) > [Reset Configuration](#)

NOTE: This menu is only available if you have selected Standalone mode when configuring device factory default settings using the J-Web Setup Wizard.

This page allows you to reset the device configuration and rerun the J-Web Setup Wizard. For details on using the setup wizard to perform initial configuration on a device with a factory default configuration, see ["Access the J-Web User Interface" on page 3](#).

On the **Reset Configuration** dialog page:

1. Click **Reset** to proceed.
The **Reconfigure Setup Wizard** warning dialogue appears.
2. Click **Proceed to Launch** to reset the configuration and rerun the Setup Wizard.
For details on using the Setup Wizard, see ["The J-Web Setup Wizard" on page 8](#).

RELATED DOCUMENTATION

| [Access the J-Web User Interface | 3](#)



Network

- Connectivity—Interfaces | 393
- Connectivity—VLAN | 406
- Connectivity—Link Aggregation | 413
- Connectivity—Wireless LAN | 422
- DHCP Client | 432
- DHCP Server | 436
- Firewall Filters—IPv4 | 446
- Firewall Filters—IPv6 | 464
- Firewall Filters—Assign to Interfaces | 480
- NAT Policies | 482
- NAT Pools | 491
- Destination NAT | 502
- Static NAT | 508
- NAT Proxy ARP/ND | 516
- Static Routing | 523
- RIP Routing | 527
- OSPF Routing | 536
- BGP Routing | 549
- Routing Instances | 565
- Routing—Policies | 570

[Routing—Forwarding Mode | 587](#)

[CoS—Value Aliases | 589](#)

[CoS—Forwarding Classes | 593](#)

[CoS Classifiers | 597](#)

[CoS—Rewrite Rules | 602](#)

[CoS—Schedulers | 607](#)

[CoS—Scheduler Maps | 612](#)

[CoS—Drop Profile | 616](#)

[CoS—Virtual Channel Groups | 620](#)

[CoS—Assign To Interface | 624](#)

[Application QoS | 630](#)

[IPsec VPN | 640](#)

[Dynamic VPN | 702](#)

[Compliance | 710](#)

Connectivity—Interfaces

IN THIS CHAPTER

- [About the Interfaces Page | 393](#)
- [Add a Logical Interface | 397](#)
- [Edit an Interface | 404](#)
- [Delete a Logical Interface | 405](#)

About the Interfaces Page

IN THIS SECTION

- [Tasks You Can Perform | 393](#)
- [Field Descriptions | 394](#)

You are here: **Network** > **Connectivity** > **Interfaces**.

Use this page to view or configure the logical interfaces to switch to L2 or L3 mode. You can view the interfaces in the ways of interface type, interface state, or zone association.

NOTE: Starting in Junos OS Release 23.4R1, J-Web supports SRX1600 and SRX2300 Firewalls.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a logical interface. See ["Add a Logical Interface" on page 397](#) .

- Edit a logical interface. See ["Edit an Interface" on page 404](#) .
- Delete a logical interface. See ["Delete a Logical Interface" on page 405](#) .

Field Descriptions

[Table 111 on page 394](#) describes the fields to view interface configuration on the Interfaces page.

NOTE:

- J-Web supports IOC4 line cards for SRX5000 line of devices. You can also view the sub-ports details configured on any or all ports of the SRX5K-IOC4-MRATE line card.
- J-Web supports Wi-Fi Mini-PIM for SRX320, SRX340, SRX345, and SRX550M devices. The physical interface for the Wi-Fi Mini-PIM uses the name wl-x/0/0, where x identifies the slot on the services gateway where the Mini-PIM is installed.

You can also configure the wl-x/0/0 interface when adding a zone at **Security Policies & Objects > Zones/Screens**.

Table 111: View Interface Configuration Details on the Interfaces Page

| Field | Action |
|--------------|--|
| Filter by | <p>Select an option from the list to view the interfaces configuration details. The available options are:</p> <ul style="list-style-type: none"> • Interface Type—Select an option to display the list of interfaces available on the device. • Interface State—Select an option to display the interfaces state of the device. The options are: <ul style="list-style-type: none"> • Admin Up • Link Up • Admin Up & Link Down • Admin Down • Zone Association—Select an option to display the list of available security zones. |
| Clear Filter | Clears the filter options that you have selected and displays all the interfaces. |

Table 111: View Interface Configuration Details on the Interfaces Page (Continued)

| Field | Action |
|-------------------|---|
| Expand All | Expands the tree under the list of interfaces. |
| Global Options | <p>To configure global setting for the interface ports:</p> <ol style="list-style-type: none"> 1. Click Global Options. The Global Options window appears. 2. Enter the following details: <ul style="list-style-type: none"> • MAC table size—Enter the size of MAC address forwarding table. • MAC limit—Enter the maximum number of MAC addresses learned per interface. The range is 1 through 65,535. • Action—Select an option from the list for the action taken when MAC limit is reached. The options available are: <ul style="list-style-type: none"> • drop • drop-and-log • log • none • shutdown |
| Disable Interface | Disables the selected interface. |
| Enable Interface | Enables the selected disabled interface. |

[Table 112 on page 396](#) describes the fields on the Interfaces page.

Table 112: Fields on the Interfaces Page

| Field | Description |
|-----------------------|--|
| Interface | <p>Displays the interface name.</p> <p>Logical interfaces configured under this interface appear in a collapsible list under the physical interface.</p> |
| 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 | <p>Displays the configured IP addresses.</p> <p>Multiple IP addresses configured on one logical interface are displayed in a collapsible list under the logical interface.</p> |
| VLAN ID | <p>Displays the VLAN ID.</p> <p>NOTE: VLAN ID is mandatory if the interface unit is higher than zero.</p> |
| Zone | Displays the security zone with which this interface is associated. |
| Logical System/Tenant | Display the statistics information for the specified logical system or tenant. |
| Speed | Displays the Interface speed (For example, 10 Mbps, 100 Mbps, 1 Gbps, 25 Gbps, or Auto). |
| Description | Displays the interface description. |

RELATED DOCUMENTATION

| [Add a Logical Interface](#) | 397

Add a Logical Interface

You are here: **Network** > **Connectivity** > **Interfaces**.

To add a logical interface:

1. Select an interface and click **+** available on the upper-right corner of the Interfaces page.
The Add Interface page appears.
2. Complete the configuration according to the guidelines provided in [Table 113 on page 397](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.
If you click OK, a new logical interface with the provided configuration is created.

[Table 113 on page 397](#) provides guidelines on using the fields on the Add Interface page.

Table 113: Fields on the Add Interface Page

| Field | Description |
|--------------------|--|
| General | |
| Unit | Enter the logical unit number. |
| Description | Enter the description for the interface. |
| Vlan Id | Enter the VLAN ID |
| Multi Tenancy Type | Select an option from the list: <ul style="list-style-type: none"> • None • Logical System • Tenant |
| Logical System | Select a logical system from the list. NOTE: This option is available when you select the multitenancy type as logical system. |

Table 113: Fields on the Add Interface Page (Continued)

| Field | Description |
|---------------------------------|--|
| Tenant | Select a tenant from the list. NOTE: This option is available when you select the multitenancy type as tenant. |
| Zone | Select a zone form the list. |
| Protocol (family) | |
| IPv4 Address | |
| IPv4 Address/DHCP configuration | Select the check box to enable this option. |
| Enable DHCP | Select this option to enable Dynamic Host Configuration Protocol (DHCP). |
| Enable address configuration | Select this option to add IPv4 address. To add IPv4 address: 1. Click + . 2. Enter the following details: <ul style="list-style-type: none"> • IPv4 Address—Enter an IPv4 address. • Web Auth—Click Configure and enable the options, Enable Http, Enable Https, and Redirect to Https. Then, click OK to save changes. • ARP—Click Edit. In the ARP Address page, click + and enter the IPv4 Address, MAC Address, and select Publish. Click OK to save the changes. |
| IPv6 Address | |

Table 113: Fields on the Add Interface Page (Continued)

| Field | Description |
|----------------------------------|---|
| IPv6 Address/DHCP configuration | Select the check box to enable this option. NOTE: Not available for IRB interface |
| Enable DHCP | Select this option to enable DHCP. |
| Enable address configuration | Select this option to add IPv6 address. To add IPv6 address: <ol style="list-style-type: none">1. Click +.2. Enter an IPv6 address. |
| Ethernet Switching | |
| Ethernet Switching configuration | Select the check box to enable this option. NOTE: Not available for IRB interface |
| Interface Mode | Select an option from the list: <ul style="list-style-type: none"> • access—Configures a logical interface to accept untagged packets. • trunk—Configures a single logical interface to accept packets tagged with any VLAN ID. |
| Recovery Timeout | Enter a period of time in seconds that the interface remains in a disabled state due to a port error prior to automatic recovery. |
| VLAN Member | Select a VLAN member from the list. |
| VoIP VLAN | Select a VLAN name from the list to be sent from the authenticating server to the IP phone. |
| Configure Vlan(s) | Select a VLAN from the Available column and move it to Selected column using the right arrow. |

Table 113: Fields on the Add Interface Page (Continued)

| Field | Description |
|---------------------------|--|
| All Vlans | Select this option to select any available VLANs. |
| General- ge | |
| Description | Enter a description for the interface. |
| MTU (Bytes) | Enter the MTU in bytes. |
| Speed | Select the speed from the list: 10 Mbps, 100 Mbps, 1 Gbps, or None. |
| Link Mode | Select the link mode from the list: Half Duplex, Full Duplex, and None. |
| Loopback | Select this option if you want the interface to loop back. |
| Flow Control | Select this option to enable flow control, which regulates the flow of packets from the router to the remote side of the connection. |
| Enable Auto Negotiation | Select this option to enable autonegotiation. |
| Enable Per Unit Scheduler | Select this option to enable the association of scheduler maps with logical interfaces. |
| Enable Vlan Tagging | Select this option to enable the reception and transmission of 802.1Q VLAN-tagged frames on the interface. |
| Source MAC Filter | |
| Add | Click + and enter the MAC address to assign it to the interface. |
| Delete | Select a MAC address and click X. |

Table 113: Fields on the Add Interface Page (Continued)

| Field | Description |
|--------------------|--|
| MAC Limit | Enter a value for MAC addresses to be associated with a VLAN. Range: 1 through 131071. |
| Packet Action | Select an option from the list: <ul style="list-style-type: none"> • drop—Drop packets with new source MAC addresses, and do not learn the new source MAC addresses. • drop-and-log—Drop packets with new source MAC addresses, and generate an alarm, an SNMP trap, or a system log entry • log—Hold packets with new source MAC addresses, and generate an alarm, an SNMP trap, or a system log entry. • none—Forward packets with new source MAC addresses and learn the new source MAC address. • shutdown—Disable the specified interface, and generate an alarm, an SNMP trap, or a system log entry. |
| General- It | |
| Unit | Enter a logical unit number. |
| Encapsulation | Select an option from the list: <ul style="list-style-type: none"> • Ethernet • Ethernet-VPLS |
| Peer Unit | Enter a peer unit number. |

Table 113: Fields on the Add Interface Page (*Continued*)

| Field | Description |
|----------------------|--|
| Multi Tenancy Type | Select an option from the list: <ul style="list-style-type: none"> • None • Logical System • Tenant |
| Logical System | Select a logical system from the list. NOTE: This option is available when you select the multitenancy type as logical system. |
| Tenant | Select a tenant from the list. NOTE: This option is available when you select the multitenancy type as tenant. |
| IP Address | Click Add and enter an IP address. Select an IP address and click Delete to delete the selected IP address. |
| st0 | |
| Tunnel Interface st0 | Enter the logical unit number. |
| Zone | Select a zone from the list. |
| Description | Enter the description for the interface. |
| Unnumbered | Select this option to fetch interface from which an unnumbered interface borrows an IPv4 address. |
| Numbered | Select this option to fetch interface from which a numbered interface borrows an IPv4 or IPv6 address. |
| IPv4 Address | Enter an IPv4 address. |

Table 113: Fields on the Add Interface Page (Continued)

| Field | Description |
|----------------------------|--|
| IPv4 Subnet Mask | Enter a subnet mask for the IPv4 address. |
| IPv6 Address | Enter an IPv4 address. |
| IPv6 Subnet Mask | Enter a subnet mask for the IPv6 address. |
| Multipoint | |
| St Interface Configuration | Select the check box to enable this option. |
| Automatic | Select this option to automatically fetch next hop tunnel address. |
| Manual | Click + to add next hop tunnel address and VPN name. Select an existing next hop address and click X to delete it. |
| Routing Protocols | |
| Enable Routing Protocols | Select an option: <ul style="list-style-type: none"> • all—Select this option to enable all protocols routing on the routing device. • OSPF—Select this option to enable OSPF routing on the routing device. • BGP—Select this option to enable BGP routing on the routing device. • RIP—Select this option to enable RIP routing on the routing device. |

RELATED DOCUMENTATION

[Edit an Interface | 404](#)
[Delete a Logical Interface | 405](#)

Edit an Interface

You are here: **Network** > **Connectivity** > **Interfaces**.

To edit an interface:

1. Select an existing interface that you want to edit on the Interfaces page.
2. Click the pencil icon available on the upper-right corner of the page.

The interface options appear with editable fields. For more information on the options, see ["Add a Logical Interface" on page 397](#) .

3. Click **OK**.

Starting in Junos OS Junos OS 22.3R1 release, you can enable the interface with flexible VLAN tagging along with native VLAN ID or VLAN tagging for interfaces. To do this:

NOTE: Supported interfaces are GE, XE, AE, WL, and RETH.

1. Select an existing interface on the Interfaces page.
2. Click the pencil icon available on the upper right side of the page.
3. In the VLAN tagging type field, select one of the following options:
 - None—No action.
 - VLAN tagging—Receive and forward single-tag frames, dual-tag frames, or a mixture of single-tag and dual-tag frames.
 - Flexible VLAN tagging—Simultaneously supports transmission of 802.1Q VLAN single-tag and dual-tag frames on logical interfaces on the same Ethernet port.

NOTE: Selected interfaces are deleted when you edit:

- None to VLAN tagging or Flexible VLAN tagging
- VLAN tagging or Flexible VLAN tagging to None

4. Click up or down arrow in the Native VLAN ID field to specify the VLAN identifier to associate with untagged packets received on the physical interface.

Range: 1 through 4094

NOTE: This option is available only if you choose Flexible VLAN tagging type.

5. Click **OK**.

RELATED DOCUMENTATION

[Delete a Logical Interface | 405](#)

Delete a Logical Interface

You are here: **Network > Connectivity > Interfaces**.

To delete a logical interface:

1. Select a logical interface that you want to delete from the Interfaces page.
2. Click the delete icon available on the upper-right corner of the page.
A confirmation window appears.
3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

[Add a Logical Interface | 397](#)

[Edit an Interface | 404](#)

Connectivity—VLAN

IN THIS CHAPTER

- [About the VLAN Page | 406](#)
- [Add a VLAN | 408](#)
- [Edit a VLAN | 410](#)
- [Delete a VLAN | 411](#)
- [Assign an Interface to VLAN | 411](#)

About the VLAN Page

IN THIS SECTION

- [Tasks You Can Perform | 406](#)
- [Field Descriptions | 407](#)

You are here: **Network** > **Connectivity** > **VLAN**.

Use this page to view, add, and remove VLAN configuration details.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a VLAN. See ["Add a VLAN" on page 408](#) .
- Edit a VLAN. See ["Edit a VLAN" on page 410](#) .
- Delete a VLAN. See ["Delete a VLAN" on page 411](#) .

- Assign Interface. See ["Assign an Interface to VLAN" on page 411](#) .
- Show or hide columns in the VLAN table. To do this, use the Show Hide Columns icon in the upper-right corner of the page and select the options you want to show or deselect to hide options on the page.
- Advanced search for a VLAN. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

For an advanced search:

1. Enter the search string in the text box.

Based on your input, a list of items from the filter context menu appears.

2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.

3. Press Enter to display the search results in the grid.

Field Descriptions

[Table 114 on page 407](#) describes the fields on the VLAN page.

Table 114: VLAN Configuration Page

| Field | Function |
|--------------------|--|
| 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. |

Table 114: VLAN Configuration Page (*Continued*)

| Field | Function |
|-------------|--|
| Description | Displays a brief description for the VLAN. |

RELATED DOCUMENTATION

[Add a VLAN | 408](#)

Add a VLAN

You are here: **Network > Connectivity > VLAN.**

To add a VLAN:

1. Click **+** available on the upper-right corner of the VLAN page.
The Add VLAN page appears.
2. Complete the configuration according to the guidelines provided in [Table 115 on page 408](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

[Table 115 on page 408](#) provides guidelines on using the fields on the Add VLAN page.

Table 115: Fields on the Add VLAN Page

| Field | Description |
|---------------------|---|
| VLAN Details | |
| VLAN Name | Enter a unique name for the VLAN. NOTE: The VLAN text field is disabled when vlan-tagging is not enabled. |

Table 115: Fields on the Add VLAN Page (Continued)

| Field | Description |
|--|---|
| VLAN ID Type | Select a type of VLAN ID. The available options are: <ul style="list-style-type: none"> • Single • Range |
| VLAN ID | Enter a unique identification number for the VLAN from 1 through 4094. If no value is specified, the default is 1. |
| Description | Enter a brief description for the VLAN. |
| Advanced Settings (optional) | |
| L2 Interfaces | Enter 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 | To apply an input firewall filter to an interface, select the firewall filter from the list. |
| Output Filter | To apply an output firewall filter to an interface, select the firewall filter from the list. |
| IPv4 Address | |
| NOTE: This option is available only when you select VLAN ID type as Single. | |
| IPv4 Address | Enter the IPv4 address of the VLAN. |

Table 115: Fields on the Add VLAN Page (*Continued*)

| Field | Description |
|--|---|
| Subnet | <p>Enter the range of logical addresses within the address space that is assigned to an organization. For example, 255.255.255.0.</p> <p>You can also specify the address prefix.</p> |
| IP Address | <p>Enter the IP address of the VLAN.</p> <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. • Delete—Select the IPv4 address or addresses that you do not want associated with the VLAN. |
| <p>IPv6 Address</p> <p>NOTE: This option is available only when you select VLAN ID type as Single.</p> | |
| IPv6 Address | Enter the IPv6 address of the VLAN. |
| Prefix | Select the destination prefix of the VLAN. |

RELATED DOCUMENTATION

[Edit a VLAN](#) | 410

Edit a VLAN

You are here: **Network** > **Connectivity** > **VLAN**.

To edit a VLAN:

1. Select an existing VLAN that you want to edit on the VLAN page.
2. Click the pencil icon available on the upper-right corner of the page.

The Edit VLAN page appears with editable fields. For more information on the options, see ["Add a VLAN" on page 408](#).

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

| [Delete a VLAN | 411](#)

Delete a VLAN

You are here: **Network** > **Connectivity** > **VLAN**.

To delete a VLAN:

1. Select one or more VLANs that you want to delete on the VLAN page.
2. Click the delete icon available on the upper-right corner of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

| [Assign an Interface to VLAN | 411](#)

Assign an Interface to VLAN

You are here: **Network** > **Connectivity** > **VLAN**.

To assign an interface to VLAN:

1. Select a VLAN.
2. Click **Assign Interface** on the upper-right corner of the VLAN page.
The Assign Interfaces page appears.
3. Complete the configuration according to the guidelines provided in [Table 116 on page 412](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 116: Fields on the Assign Interfaces Page

| Field | Description |
|-----------------|---|
| 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 | Select the interfaces in the Available column and use the right arrow to move them to the Selected column. |
| VoIP Interfaces | Select the VoIP interfaces in the Available column and use the right arrow to move them to the Selected column. |

RELATED DOCUMENTATION

| [Add a VLAN](#) | 408

Connectivity—Link Aggregation

IN THIS CHAPTER

- [About the Link Aggregation Page | 413](#)
- [Link Aggregation Global Settings | 415](#)
- [Add a Logical Interface to Link Aggregation | 416](#)
- [Add a Link Aggregation | 417](#)
- [Edit an Aggregated Interface | 419](#)
- [Delete Link Aggregation | 420](#)
- [Search for Text in the Link Aggregation Table | 420](#)

About the Link Aggregation Page

IN THIS SECTION

- [Tasks You Can Perform | 413](#)
- [Field Descriptions | 414](#)

You are here: **Network > Connectivity > Link Aggregation.**

Use this page to view, add, and remove link aggregation configuration details.

Tasks You Can Perform

You can perform the following tasks from this page:

- Global Settings. See ["Link Aggregation Global Settings" on page 415](#) .
- Add Logical Interface. See ["Add a Logical Interface to Link Aggregation" on page 416](#) .

- Enable/Disable LACP link-protection. To do this, select a link aggregation and click **Enable/Disable** available at the upper-right corner of the Link Aggregation table.
- Add Link Aggregation. See ["Add a Link Aggregation" on page 417](#) .
- Edit Link Aggregation. See ["Edit an Aggregated Interface" on page 419](#) .
- Delete Link Aggregation. See ["Delete Link Aggregation" on page 420](#) .
- Search for text in a link aggregation table. See ["Search for Text in the Link Aggregation Table" on page 420](#) .
- Show or hide columns in the Link Aggregation table. To do this, use the Show Hide Columns icon in the upper-right corner of the page and select the options you want to show or deselect to hide options on the page.

Field Descriptions

[Table 117 on page 414](#) describes the fields on the Link Aggregation page.

Table 117: Fields on the Link Aggregation Page

| Field | Description |
|-------------------|---|
| 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. |
| 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 Type | Displays whether the interface is enabled with VLAN-tagging, Flexible VLAN Tagging, or Flexible VLAN Tagging along with native VLAN ID. |

Table 117: Fields on the Link Aggregation Page (Continued)

| Field | Description |
|------------------|---|
| Enabled/Disabled | Displays whether the LACP link-protection is enabled or disabled. |
| Description | Provides a description of the LAG. |

RELATED DOCUMENTATION

| [Link Aggregation Global Settings](#) | 415

Link Aggregation Global Settings

You are here: **Network** > **Connectivity** > **Link Aggregation**.

To add link aggregation global settings:

Complete the configuration according to the guidelines provided in [Table 118 on page 415](#) .

Table 118: Fields on the Link Aggregation Global Settings page

| Field | Action |
|--|--|
| General | |
| Device count | Enter the device count. By default, J-Web displays the device count as the same number of created aggregated Ethernet interfaces. Range: 1 through 128. |
| Link Aggregation Control Protocol (LACP) | |
| NOTE: This option is not available for SRX5000 line of devices. | |
| System priority | Click the arrow button to select the priority level that you want to associate with the LAG. |

Table 118: Fields on the Link Aggregation Global Settings page (Continued)

| Field | Action |
|----------------------|--|
| Link protection mode | Select one of the following options: <ul style="list-style-type: none"> • Revertive—Enable to switch to a better priority link (if one is available). • Non-revertive—Disable the ability to switch to a better priority link (if one is available) once a link is established as active and collection distribution is enabled. |

RELATED DOCUMENTATION

| [Add a Logical Interface to Link Aggregation | 416](#)

Add a Logical Interface to Link Aggregation

You are here: **Network** > **Connectivity** > **Link Aggregation**.

To add an interface to link aggregation:

1. Select an aggregated interface.
2. Click **Add Logical Interface** on the upper-right corner of the Link Aggregation page.
The Add Logical Interface page appears.
3. Complete the configuration according to the guidelines provided in [Table 119 on page 416](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 119: Fields on the Add Logical Interface Page

| Field | Action |
|------------------------|-------------------------------------|
| General | |
| AE interface name | Displays aggregated interface name. |
| Logical interface unit | Enter the logical interface unit. |

Table 119: Fields on the Add Logical Interface Page (Continued)

| Field | Action |
|---------------------|---|
| Description | Enter the description. |
| VLAN ID | Enter the VLAN ID. VLAN ID is mandatory. |
| IPv4 Address | |
| IPv4 Address | Click + and enter a valid IPv4 address. |
| Subnet Mask | Enter a valid subnet mask for IPv4 address. |
| IPv6 Address | |
| IPv6 Address | Click + and enter a valid IPv6 address. |
| Subnet Mask | Enter a valid subnet mask for IPv6 address. |

RELATED DOCUMENTATION

| [Add a Link Aggregation](#) | 417

Add a Link Aggregation

You are here: **Network > Connectivity > Link Aggregation.**

To add a link aggregation:

1. Click + on the upper-right corner of the Link Aggregation page.
The Create Link Aggregation page appears.
2. Complete the configuration according to the guidelines provided in [Table 120 on page 418](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 120: Fields on the Create Link Aggregation Page

| Field | Action |
|---|---|
| General | |
| Name | <p>Enter the aggregated interface name. The name should be in aeX format. Where X is a number.</p> <p>NOTE: If an aggregated interface already exists, then the field is displayed as read-only.</p> |
| Description | Enter a description for the LAG. |
| Interfaces | <p>Select the interface available for aggregation and move to Selected column using right arrow.</p> <p>NOTE: Only interfaces that are configured with the same speed can be selected together for a LAG.</p> |
| VLAN tagging type | <p>Select one of the following VLAN tagging type:</p> <ul style="list-style-type: none"> • None • VLAN Tagging—Receive and forward single-tag frames, dual-tag frames, or a mixture of single-tag and dual-tag frames. • Flexible VLAN Tagging—Simultaneously supports transmission of 802.1Q VLAN single-tag and dual-tag frames on logical interfaces on the same Ethernet port. <p>NOTE: When you edit from None to VLAN tagging or Flexible VLAN tagging or vice versa, all the logical interfaces of the selected interface are deleted.</p> |
| Native VLAN ID | <p>VLAN identifier to associate with untagged packets received on the physical interface.</p> <p>Range: 0 through 4094.</p> |
| Link Aggregation Control Protocol (LACP) | |

Table 120: Fields on the Create Link Aggregation Page (*Continued*)

| Field | Action |
|----------------------|---|
| LACP mode | <p>Select a mode in which Link Aggregation Control Protocol packets are exchanged between the interfaces. The modes are:</p> <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. |
| Periodic | <p>Select a periodic transmissions of link aggregation control PDUs occur at different transmission rate. The options available are:</p> <ul style="list-style-type: none"> • Fast—Transmit link aggregation control PDUs every second. • Slow—Transmit link aggregation control PDUs every 30 seconds. |
| System priority | Click the arrow button to select the priority level that you want to associate with the LAG. |
| Link protection | <p>Enable or disable the option to protect the link.</p> <p>NOTE: You can configure only two member links for an aggregated Ethernet interface, that is, one active and one standby.</p> |
| Link protection mode | <p>Select one of the following options:</p> <ul style="list-style-type: none"> • Revertive—Enable to switch to a better priority link (if one is available). • Non-revertive—Disable the ability to switch to a better priority link (if one is available) once a link is established as active and collection distribution is enabled. |

RELATED DOCUMENTATION

[Edit an Aggregated Interface](#) | 419

Edit an Aggregated Interface

You are here: **Network** > **Connectivity** > **Link Aggregation**.

To edit an aggregated interface:

1. Select an existing aggregated interface that you want to edit on the Aggregated Interface page.
2. Click the pencil icon available on the upper-right corner of the page.

The edit Aggregated Interface page appears with editable fields. For more information on the options, see ["Add a Link Aggregation" on page 417](#) .

3. Click **OK** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

| [Delete Link Aggregation](#) | 420

Delete Link Aggregation

You are here: **Network** > **Connectivity** > **Link Aggregation**.

To delete link aggregation:

1. Select one or more aggregated interfaces that you want to delete on the Link Aggregation page.
2. Click the delete icon available on the upper-right corner of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

| [About the Link Aggregation Page](#) | 413

Search for Text in the Link Aggregation Table

You are here: **Network** > **Connectivity** > **Link Aggregation**.

You can use the search icon in the upper-right corner of the Link Aggregation page to search for text containing letters and special characters on that page.

To search for text:

1. Click the search icon and enter partial text or full text of the keyword in the search bar.

The search results are displayed.

2. Click **X** next to a search keyword or click **Clear All** to clear the search results.

RELATED DOCUMENTATION

| [About the Link Aggregation Page](#) | 413

Connectivity—Wireless LAN

IN THIS CHAPTER

- [About the Settings Page | 422](#)
- [Create an Access Point | 424](#)
- [Edit an Access Point | 425](#)
- [Delete an Access Point | 426](#)
- [Create an Access Point Radio Setting | 426](#)
- [Edit an Access Point Radio Setting | 430](#)
- [Delete an Access Point Radio Settings | 430](#)

About the Settings Page

IN THIS SECTION

- [Tasks You Can Perform | 423](#)
- [Field Descriptions | 423](#)

You are here: **Network** > **Connectivity** > **Wireless LAN** > **Settings**.

Use this page to configure wireless LAN settings.

NOTE: Starting in Junos OS Release 20.1R1, J-Web supports SRX380 devices. You can configure the SRX380 device supported wireless LAN settings.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create an access point. See ["Create an Access Point" on page 424](#) .
- Edit an access point. See ["Edit an Access Point" on page 425](#) .
- Delete an access point. See ["Delete an Access Point" on page 426](#) .
- Create access point radio settings. See ["Create an Access Point Radio Setting" on page 426](#) .
- Edit access point radio settings. See ["Edit an Access Point Radio Setting" on page 430](#) .
- Delete access point radio settings. See ["Delete an Access Point Radio Settings" on page 430](#) .

Field Descriptions

[Table 121 on page 423](#) describes the fields on the Settings page.

Table 121: Fields on the Settings Page

| Field | Description |
|-------------------|--|
| Access Point Name | Displays the access point name. |
| Description | Displays the description for the access point. |
| WL Interface | Displays the wireless LAN interface name. |
| Location | Displays the location of the access point. |
| MAC Address | Displays the MAC address. |
| Country | Displays the country of the access point. |

Change History Table

Feature support is determined by the platform and release you are using. Use [Feature Explorer](#) to determine if a feature is supported on your platform.

| Release | Description |
|---------|--|
| 20.1R1 | Starting in Junos OS Release 20.1R1, J-Web supports SRX380 devices. You can configure the SRX380 device supported wireless LAN settings. |

RELATED DOCUMENTATION

| [Create an Access Point](#) | 424

Create an Access Point

You are here: **Network** > **Connectivity** > **Wireless LAN** > **Settings**.

To create an access point:

1. Click **+** on the upper-right corner of the Settings page.
The Create Access Point Configuration page appears.
2. Complete the configuration according to the guidelines provided in [Table 122 on page 424](#).
3. Click **OK** to save the changes.
An access point is created.

If you want to discard your changes, click **Cancel**.

Table 122: : Fields on the Create Access Point Configuration Page

| Field | Action |
|-----------------------|--|
| Basic Settings | |
| Name | Enter a unique name for the access point. |
| Description | Enter the description for the access point. |
| Interface | Select a wireless LAN interface from the list. |

Table 122: : Fields on the Create Access Point Configuration Page (*Continued*)

| Field | Action |
|-----------------------------|---|
| Location | Enter the location of the access point. |
| MAC Address | Enter the MAC address. |
| Access Point Options | |
| Country | Select a country of the access point from the list. |

RELATED DOCUMENTATION

[About the Settings Page | 422](#)

[Edit an Access Point | 425](#)

[Delete an Access Point | 426](#)

[Create an Access Point Radio Setting | 426](#)

Edit an Access Point

You are here: **Network** > **Connectivity** > **Wireless LAN** > **Settings**.

To edit an access point:

1. Select an existing access point that you want to edit on the Settings page.
2. Click the pencil icon on the upper-right corner of the page.

The Edit Access Point Configuration page appears with editable fields. For more information on the options, see "[Create an Access Point](#)" on page 424 .

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[About the Settings Page | 422](#)

[Delete an Access Point | 426](#)

Delete an Access Point

You are here: **Network** > **Connectivity** > **Wireless LAN** > **Settings**.

To delete an access point:

1. Select an existing access point that you want to delete on the Settings page.
2. Click the delete icon on the upper-right corner of the page.
3. Click **Yes** to delete the access point or click **No** to retain the access point.

RELATED DOCUMENTATION

[About the Settings Page | 422](#)

[Create an Access Point | 424](#)

[Edit an Access Point | 425](#)

Create an Access Point Radio Setting

You are here: **Network** > **Connectivity** > **Wireless LAN** > **Settings**.

To create an access point radio setting:

1. Click **+** on the upper-right corner of the Radio Settings table.
The Create Access Point Radio Settings page appears.
2. Complete the configuration according to the guidelines provided in [Table 123 on page 426](#).
3. Click **OK** to save the changes.

The access point radio settings are created.

If you want to discard your changes, click **Cancel**.

Table 123: Fields on the Create Access Point Radio Settings Page

| Field | Action |
|--------------|------------------------------------|
| Radio | |
| Radio Type | Select a radio type from the list. |

Table 123: Fields on the Create Access Point Radio Settings Page (Continued)

| Field | Action |
|-------------|-----------------------------------|
| Radio State | Select the radio state to enable. |

Table 123: Fields on the Create Access Point Radio Settings Page (*Continued*)

| Field | Action |
|-----------------------|--|
| Virtual Access Points | <p>To add a virtual access point:</p> <ol style="list-style-type: none"> Click Add. The Create VAP Configuration page appears. Enter the following details: <ul style="list-style-type: none"> <i>Basic Settings:</i> <ul style="list-style-type: none"> VAP ID—Enter a value using up or down arrows. Description—Enter a description for the virtual access points. SSID—Enter a unique name to broadcast from access points. VLAN ID—Enter a VLAN identifier (VID) using up or down arrows. Download Limit (Kbps)—Enter a value using up or down arrows. Upload Limit (Kbps)—Enter a value using up or down arrows. Broadcast SSID—Select No to disable. Maximum Stations—Enter a value using up or down arrows. Station Isolation—Select the check box to enable. <i>Security:</i> <ul style="list-style-type: none"> Security—Select an option from the list. If you have selected WPA Personal, enter the following details: <ul style="list-style-type: none"> WPA Version—Select an option from the list. Cipher Suites—Select an option from the list. WPA Shared Key—Enter a value for the key. Key Type—Select an option from the list. If you have selected WPA Enterprise, enter the following details: |

Table 123: Fields on the Create Access Point Radio Settings Page (*Continued*)

| Field | Action |
|-------------------------------------|--|
| | <ul style="list-style-type: none"> • WPA Version—Select an option from the list. • Cipher Suites—Select an option from the list. • Radius Server IP—Enter IP address for the radio server. • Radius Port—Enter a value using up or down arrows. • Radius Key—Enter a value for the key. <p><i>Station MAC Filter:</i></p> <ul style="list-style-type: none"> • Allowed List MAC Address—Enter a MAC address that you want to allow and click Add to add the address in the MAC addresses list. Select the MAC address click Delete to remove it. • Deny List MAC Address—Enter a MAC address that you want to block and click Add to add the address in the MAC addresses list. Select the MAC address click Delete to remove it. <p>3. Click OK to save VAP configuration.</p> <p>Select the virtual access point and click Edit or Delete icons to edit or remove it.</p> |
| Radio Settings—Radio Options | |
| Mode | Select a radio mode option from the list. |
| Channel Number | Select a channel number for radio from the list. |
| Channel Bandwidth | Select a channel bandwidth for radio from the list. |
| Transmit Power | Enter a value for radio transmit power using up or down arrows. |

RELATED DOCUMENTATION

[About the Settings Page | 422](#)

[Edit an Access Point Radio Setting | 430](#)

[Delete an Access Point Radio Settings | 430](#)

Edit an Access Point Radio Setting

You are here: **Network** > **Connectivity** > **Wireless LAN** > **Settings**.

To edit an access point radio settings:

1. Select an existing access point radio setting that you want to edit on the Settings page.
2. Click the edit icon on the upper-right corner of the Radio Settings table.
The Edit Access Point Radio Settings page appears with editable fields. For more information on the options, see "[Create an Access Point Radio Setting](#)" on page 426 .
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[About the Settings Page | 422](#)

[Delete an Access Point Radio Settings | 430](#)

Delete an Access Point Radio Settings

You are here: **Network** > **Connectivity** > **Wireless LAN** > **Settings**.

To delete an access point radio settings:

1. Select an existing access point radio setting that you want to delete on the Settings page.
2. Click the delete icon available on the upper-right corner of the Radio Settings table.
3. Click **Yes** to delete the access point radio settings or click **No** to retain the access point radio settings.

RELATED DOCUMENTATION

[About the Settings Page | 422](#)

[Create an Access Point Radio Setting | 426](#)

[Edit an Access Point Radio Setting | 430](#)

DHCP Client

IN THIS CHAPTER

- [About the DHCP Client Page | 432](#)
- [Add DHCP Client Information | 433](#)
- [Delete DHCP Client Information | 435](#)

About the DHCP Client Page

IN THIS SECTION

- [Tasks You Can Perform | 432](#)
- [Field Descriptions | 432](#)

You are here: **Network** > **DHCP** > **DHCP Client**.

Use this page to view, add, and remove link aggregation configuration details.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create DHCP client information. See ["Add DHCP Client Information" on page 433](#) .
- Delete DHCP client information. See ["Delete DHCP Client Information" on page 435](#) .

Field Descriptions

[Table 124 on page 433](#) describes the fields on the DHCP Client page.

Table 124: Fields on the DHCP Client Page

| Field | Description |
|------------------------|--|
| Interface Name | Displays the interface name. |
| DHCP Client Identifier | Displays the name of the client used by the DHCP server to index its database of address bindings. |
| Server | Displays the DHCP server address. |
| Lease Time | Displays the time in seconds, to negotiate and exchange DHCP messages. |
| Add | Adds a new DHCP client configuration. |
| Delete | Deletes the selected DHCP client configuration. |

RELATED DOCUMENTATION

| [Add DHCP Client Information](#) | 433

Add DHCP Client Information

You are here: **Network > DHCP > DHCP Client.**

To add DHCP Client information:

1. Click **Add** on the DHCP Client page.
The DHCP Client Information page appears.
2. Complete the configuration according to the guidelines provided in [Table 125 on page 434](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 125: Fields on the DHCP Client Information Page

| Field | Action |
|--------------------------------|---|
| DHCP Client Information | |
| Interface | Enter the name of the interface on which to configure the DHCP client. |
| Client Identifier | <p>Specifies the name of the client used by the DHCP server to index its database of address bindings.</p> <p>Select an option from the list:</p> <ul style="list-style-type: none"> • ASCII— ASCII client. • Hexadecimal—Hexadecimal client. |
| Lease Time | <p>Enter a value from 60 through 2,147,483,647.</p> <p>Specifies the time in seconds, to negotiate and exchange DHCP messages.</p> |
| Retransmission Attempt | <p>Enter a value from 0 through 6. The default value is 4.</p> <p>Specifies the number of attempts the router is allowed to retransmit a DHCP packet fallback.</p> |
| DHCP Server Address | <p>Enter the IPv4 address of the DHCP server.</p> <p>Specifies the preferred DHCP server that the DHCP clients contact with DHCP queries.</p> |
| Vendor Class ID | <p>Enter the vendor class ID numbers.</p> <p>Specifies the vendor class identity number for the DHCP client.</p> |
| Update Server | Select the check box to enable the propagation of TCP/IP settings on the specified interface (if it is acting as a DHCP client) to the DHCP server that is configured on the router. |

RELATED DOCUMENTATION

[Delete DHCP Client Information | 435](#)

Delete DHCP Client Information

You are here: **Network** > **DHCP** > **DHCP Client**.

To delete a DHCP Client Information:

1. Select a DHCP Client that you want to delete on the DHCP Client page.
2. Click **Delete** available on the DHCP Client page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the DHCP Client Page | 432](#)

[Add DHCP Client Information | 433](#)

DHCP Server

IN THIS CHAPTER

- [About the DHCP Server Page | 436](#)
- [Add a DHCP Pool | 438](#)
- [Edit a DHCP Pool | 442](#)
- [Delete a DHCP Pool | 443](#)
- [DHCP Groups Global Settings | 443](#)
- [Add a DHCP Group | 444](#)
- [Edit a DHCP Group | 444](#)
- [Delete a DHCP Group | 445](#)

About the DHCP Server Page

IN THIS SECTION

- [Tasks You Can Perform | 436](#)
- [Field Descriptions | 437](#)

You are here: **Network** > **DHCP** > **DHCP Server**.

Use this page to view, add, and remove DHCP server configuration details.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a DHCP Pool. See ["Add a DHCP Pool" on page 438](#) .

- Edit a DHCP Pool. See ["Edit a DHCP Pool" on page 442](#) .
- Delete a DHCP Pool. See ["Delete a DHCP Pool" on page 443](#) .
- Configure DHCP group global settings. See ["DHCP Groups Global Settings" on page 443](#) .
- Add a DHCP group. See ["Add a DHCP Group" on page 444](#) .
- Edit a DHCP group. See ["Edit a DHCP Group" on page 444](#) .
- Delete a DHCP group. See ["Delete a DHCP Group" on page 445](#) .

Field Descriptions

[Table 126 on page 437](#) describes the fields on the DHCP Server page.

Table 126: Fields on the DHCP Server Page

| Field | Description |
|--------------------|---|
| Routing Instance | Displays the name of the routing instance selected for DHCP server. |
| DHCP Pools | |
| Pool Name | Displays the name of the source pool. |
| Network Addresses | Displays the IP address in the pool. |
| Routing Instance | Displays the name of the routing instance selected. |
| DHCP Groups | |
| Global Settings | Specifies the global settings of DHCP server. |
| Group name | Specifies the source name of the group. |
| Interfaces | Displays name of the interfaces selected. |
| Routing Instance | Displays the name of the routing instance selected. |

Table 126: Fields on the DHCP Server Page *(Continued)*

| Field | Description |
|--------------------------------------|---|
| DHCP Address range for pool | |
| Address Range Name | Specify the name of the address assignment pool. |
| Address Range (Low) | Specifies the lowest address in the IP address pool range. |
| Address Range (High) | Specifies the highest address in the IP address pool range. |
| DHCP Static Bindings for pool | |
| Host Name | Specifies the name of the client for the static binding. |
| MAC Address | Specifies the client MAC address. |
| Fixed IP Address | Specifies the IP address to reserve for the client. |

RELATED DOCUMENTATION

| [Add a DHCP Pool](#) | 438

Add a DHCP Pool

You are here: **Network** > **DHCP** > **DHCP Server**.

To add a DHCP Pool:

1. Click **+** on the upper-right corner of the DHCP Pools table.
The Add DHCP Pool page appears.
2. Complete the configuration according to the guidelines provided in [Table 127 on page 439](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

[Table 127 on page 439](#) describes the Add DHCP Pool Page.

Table 127: Fields on the Add DHCP Pool Page.

| Field | Action |
|--|---|
| General | |
| Pool Name | Enter a name for DHCP pool. |
| Routing Instance | Select a routing instance from the list. |
| Network Addresses | Enter the following details: <ul style="list-style-type: none"> • IP Address—Enter an IP address. • Subnet Mask—Enter a subnet mask for the IP address. |
| DHCP Pool Attributes | |
| Click DHCP Attributes to add DHCP pool attributes. After configuring the attributes, click OK to save the changes. | |
| Pool Name | Displays the DHCP pool name. |
| Domain Name | Enter the domain name to be assigned to the address pool. |
| Server Identifier | Enter the name of the server identifier to assign to the DHCP client in the address pool. |
| Netbios Node Type | Select a NetBIOS node type from the list. This is equivalent to DHCP option 46. |
| Next Server | Enter the IP address of the next DHCP server that the clients need to contact. |
| Propagate Settings | Select an interface from the list. Specifies the name of the interface on the router through which the resolved DHCP queries are propagated to the DHCP pool. |
| TFTP Server | Enter the IP address of the TFTP server. |

Table 127: Fields on the Add DHCP Pool Page. (Continued)

| Field | Action |
|---------------------------|---|
| Maximum Lease Time (Secs) | <p>Enter a from value 60 through 1,209,600.</p> <p>Specifies the maximum length of time in seconds, a client can hold a lease. (Dynamic BOOTP lease lengths can exceed this maximum time.)</p> |
| Boot File | Enter the path and filename of the initial boot file to be used by the client. |
| Boot Server | Enter the IP address or hostname of the TFTP server that provides the initial boot file to the client. |
| Grace Period (Secs) | <p>Enter a number of seconds the lease is retained.</p> <p>range is 0 through 4,294,967,295. By default, 0 is no grace period.</p> |
| DNS Name Servers | <p>Specifies the DNS name to assign to the DHCP client in the address pool.</p> <p>Click any one of the following:</p> <ul style="list-style-type: none"> • +—Adds the DNS name in the address pool. • Click the pencil icon to edit a selected DNS name in the address pool. • X—Deletes the DNS name in the address pool. |
| WINS Servers | <p>Specifies the WINS servers to assign to the DHCP client in the address pool.</p> <p>Click any one of the following:</p> <ul style="list-style-type: none"> • +—Adds WINS servers to the address pool. • Click the pencil icon to edit a selected WINS server in the address pool. • X—Deletes the WINS servers in the address pool. |

Table 127: Fields on the Add DHCP Pool Page. (Continued)

| Field | Action |
|-----------------|---|
| Gateway Routers | <p>Specifies the gateway router to assign client in the address pool.</p> <p>Click any one of the following:</p> <ul style="list-style-type: none"> • +—Adds the gateway router to the address pool. • Click the pencil icon to edit a selected gateway router in the address pool. • X—Deletes the gateway router in the address pool. |
| Options | <p>Click + to add DHCP option.</p> <p>Enter the following details:</p> <ul style="list-style-type: none"> • Code—Type a number. • Type—Select a type from the list that corresponds to the code. • Value—Type a valid option value based on the type. <p>You can select the DHCP option and click the pencil icon to edit or click X to delete the DHCP options.</p> |
| Option-82 | <p>Device inserts DHCP option 82 (also known as the DHCP relay agent information option) information.</p> <p>Enter the following details:</p> <ul style="list-style-type: none"> • Circuit Identifier—Enter circuit ID to identify the circuit (interface or VLAN) on the switching device on which the request was received. • Ranges—Enter a value for the circuit ID. • Remote Identifier—Enter remote ID to identify the remote host. • Ranges—Enter a value for the remote ID. |

Address Range

Click **+** to add address range. After configuring the attributes, click **OK** to save the changes.

Selected an address range and click the pencil icon to edit it or click **X** to delete it.

Table 127: Fields on the Add DHCP Pool Page. (Continued)

| Field | Action |
|-------|--|
| Name | Enter the address range name. |
| Low | Enter an IP address that is part of the subnet specified in Address Pool subnet. |
| High | 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. |

Static Bindings

Click **+** to add DHCP static bindings. After configuring the attributes, click **OK** to save the changes.

Selected a DHCP static binding and click the pencil icon to edit it or click **X** to delete it.

| | |
|------------------|---|
| Host Name | Enter the hostname to assign the DHCP client to the MAC address. |
| Mac Address | Enter the MAC address of the DHCP client. |
| Fixed IP Address | Enter the fixed address to assign the DHCP client to the MAC address. |

RELATED DOCUMENTATION

[Edit a DHCP Pool](#) | 442

Edit a DHCP Pool

You are here: **Network** > **DHCP** > **DHCP Server**.

To edit a DHCP Pool:

1. Select an existing DHCP Pool that you want to edit on the DHCP Server page.
2. Click the pencil icon available on the upper-right corner of the DHCP Pools table.

The Edit DHCP Pool page appears. You can edit the network addresses. For more information on the options, see "[Add a DHCP Pool](#)" on page 438 .

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[Delete a DHCP Pool | 443](#)

Delete a DHCP Pool

You are here: **Network** > **DHCP** > **DHCP Server**.

To delete a DHCP Pool:

1. Select a DHCP Pool that you want to delete on the DHCP Server page.
2. Click the delete icon available on the upper-right corner of the DHCP Pools table.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[DHCP Groups Global Settings | 443](#)

DHCP Groups Global Settings

You are here: **Network** > **DHCP** > **DHCP Server**.

To configure DHCP groups global settings:

1. Click **Global Settings** available on the upper-right corner of the DHCP Groups table.
The DHCP Global Configuration page appears.
2. Select the options available in the Available column and move them to Selected column using the arrow to configure the order of the DHCP pool match.
3. Click **OK** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

[Add a DHCP Group | 444](#)

[Edit a DHCP Group | 444](#)

Add a DHCP Group

You are here: **Network** > **DHCP** > **DHCP Server**.

To add a DHCP Group:

1. Click **+** on the upper-right corner of the DHCP Groups table.
The Add DHCP Group page appears.
2. Complete the configuration according to the guidelines provided in [Table 128 on page 444](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

[Table 128 on page 444](#) describes the fields on the Add DHCP Group.

Table 128: Fields on the Add DHCP Group Page

| Field | Action |
|------------------|---|
| Group Name | Enter a name for the DHCP group. |
| Routing Instance | Select a routing instance from the list. |
| Interfaces | Select the interfaces available in the Available column and move them to Selected column using the right arrow. |

RELATED DOCUMENTATION

[Edit a DHCP Group | 444](#)

[Delete a DHCP Group | 445](#)

[DHCP Groups Global Settings | 443](#)

Edit a DHCP Group

You are here: **Network** > **DHCP** > **DHCP Server**.

To edit a DHCP group:

1. Select an existing DHCP group that you want to edit on the DHCP Server page.
2. Click the pencil icon available on the upper-right corner of the DHCP Groups table.

The Edit DHCP Group page appears with editable fields. For more information on the options, see ["Add a DHCP Group" on page 444](#).

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[DHCP Groups Global Settings | 443](#)

[Add a DHCP Group | 444](#)

[Delete a DHCP Group | 445](#)

Delete a DHCP Group

You are here: **Network > DHCP > DHCP Server**.

To delete a DHCP group:

1. Select a DHCP group that you want to delete on the DHCP Server page.
2. Click the delete icon available on the upper-right corner of the DHCP Groups table.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[DHCP Groups Global Settings | 443](#)

[Add a DHCP Group | 444](#)

[Edit a DHCP Group | 444](#)

Firewall Filters—IPv4

IN THIS CHAPTER

- [About the IPv4 Page | 446](#)
- [Add IPv4 Firewall Filters | 447](#)

About the IPv4 Page

IN THIS SECTION

- [Tasks You Can Perform | 446](#)
- [Field Descriptions | 446](#)

You are here: **Network** > **Firewall Filters** > **IPv4**.

Use this page to configure IPv4 firewall filters.

Tasks You Can Perform

You can perform the following task from this page:

- Add an IPv4 firewall filter. See ["Add IPv4 Firewall Filters" on page 447](#) .

Field Descriptions

[Table 129 on page 447](#) describes the fields on the IPv4 page.

Table 129: Fields on the IPv4 Page

| Field | Description |
|----------------------------|--|
| IPv4 Filter Summary | |
| Filter Name | Displays the name of the filter and when expanded, lists the terms attached to the filter. |
| Add New IPv4 Filter | |
| Filter Name | Searches for existing filters by filter name. |
| Term Name | Searches for existing terms by term name. |
| Location | Specifies the position of the new filter. |

RELATED DOCUMENTATION

[Add IPv4 Firewall Filters](#) | 447

Add IPv4 Firewall Filters

You are here: **Network** > **Firewall Filters** > **IPv4**.

To add an IPV4 firewall filter:

1. Complete the configuration according to the guidelines provided in [Table 130 on page 448](#) and [Table 131 on page 450](#).
2. Click **Add** available in the Add New IPv4 Filter section.
A new IPv4 Firewall Filter is created.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 130: Fields on the Add IPv4 Firewall Filter Page

| Field | Action |
|----------------------------|---|
| IPv4 Filter Summary | |
| Action column | <p>Select an option.</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. |
| 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. |
| Search | |
| IPv4 Filter Name | <p>Enter the existing 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. |

Table 130: Fields on the Add IPv4 Firewall Filter Page (Continued)

| Field | Action |
|----------------------------|--|
| IPv4 Term Name | <p>Enter the 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 . |
| Number of Items to Display | Enter the number of filters or terms to display on one page. Select the number of items to be displayed on one page. |

Add New IPv4 Filter

| | |
|-------------|---|
| Filter Name | <p>Enter the existing 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. |
| Term Name | <p>Enter the 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 . |

Table 130: Fields on the Add IPv4 Firewall Filter Page (*Continued*)

| Field | Action |
|----------|---|
| Location | Positions the new filter in one of the following locations: <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. |
| Add | Adds a new filter name. Opens the term summary page for this filter allowing you to add new terms to this filter. |

Add New IPv4 Term

| | |
|----------|--|
| Location | Positions the new term in one of the following locations: <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. |
| Add | Opens the Filter Term page allowing you to define the match conditions and the action for this term. |

Table 131: Fields on the Match Criteria for IPv4 Firewall Filter

| Field | Action |
|--------------|--------|
| Match Source | |

Table 131: Fields on the Match Criteria for IPv4 Firewall Filter *(Continued)*

| Field | Action |
|--------------------|---|
| Source Address | <p>Enter 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. <p>Enter an IP source address and prefix length and select an option.</p> |
| Source Prefix List | <p>Enter 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>Select an option:</p> <ul style="list-style-type: none"> • Add—To include a predefined source prefix list in the match condition, type the prefix list name. • Except—To exclude the prefix list from the match condition and then select Add—To include the prefix list in the match condition. • Delete—To remove a prefix list from the match condition. |

Table 131: Fields on the Match Criteria for IPv4 Firewall Filter (*Continued*)

| Field | Action |
|--------------------------|---|
| Source Port | <p>Enter 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. <p>Select the port from the port name list; enter the port name, number, or range and then select an option.</p> |
| Match Destination | |
| Destination Address | <p>Enter 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. <p>Enter an IP destination address and prefix length and select an option.</p> |

Table 131: Fields on the Match Criteria for IPv4 Firewall Filter *(Continued)*

| Field | Action |
|-------------------------|--|
| Destination Prefix List | <p>Enter 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>Select an option:</p> <ul style="list-style-type: none"> • Add—To include a predefined destination prefix list, enter the prefix list name. • Except—To exclude the prefix list from the match condition and then select Add—To include the prefix list in the match condition. • Delete—To remove a prefix list from the match condition. |
| Destination Port | <p>Enter 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. <p>Select the port from the port name list; enter the port name, number, or range; and then select an option.</p> |

Match Source or Destination

Table 131: Fields on the Match Criteria for IPv4 Firewall Filter *(Continued)*

| Field | Action |
|-------------|--|
| Address | <p>Enter 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. <p>Enter an IP destination address and prefix length and select an option.</p> |
| Prefix List | <p>Enter 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>Select an option:</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. |

Table 131: Fields on the Match Criteria for IPv4 Firewall Filter *(Continued)*

| Field | Action |
|------------------------|---|
| Port | <p>Enter 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. <p>Select the port from the port name list; enter the port name, number, or range; and then select an option.</p> |
| Match Interface | |
| Interface | <p>Enter 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. <p>Select a name from the interface name list or Enter the interface name and select an option.</p> |

Table 131: Fields on the Match Criteria for IPv4 Firewall Filter *(Continued)*

| Field | Action |
|---------------------------------|--|
| Interface Set | <p>Enter 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. <p>Enter the interface set name and select an option.</p> |
| Interface Group | <p>Enter 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. <p>Enter the name of the group and select an option.</p> |
| Match Packet and Network | |
| First Fragment | <p>Select the check box.</p> <p>Matches the first fragment of a fragmented packet.</p> |
| Is Fragment | <p>Select the check box.</p> <p>Matches trailing fragments (all but the first fragment) of a fragmented packet.</p> |
| Fragment Flags | <p>Enter fragmentation flags to be included in the match condition.</p> <p>Enter a text or numeric string defining the flag.</p> |

Table 131: Fields on the Match Criteria for IPv4 Firewall Filter (*Continued*)

| Field | Action |
|-----------------|---|
| TCP Established | <p>Select the check box.</p> <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> |
| TCP Initial | <p>Select the check box.</p> <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> |
| TCP Flags | <p>Enter 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> |
| Protocol | <p>Enter 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. <p>Select a protocol name from the list or enter a protocol name or number and then select an option.</p> |

Table 131: Fields on the Match Criteria for IPv4 Firewall Filter (*Continued*)

| Field | Action |
|-----------------|---|
| ICMP Type | <p>Select a packet type from the list or enter a packet type name or number and then select an option.</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. <ul style="list-style-type: none"> Add—To include the packet type in the match condition. • Delete—To remove an ICMP packet type from the match condition. |
| ICMP Code | <p>Select a packet code from the list or enter the packet code as text or a number and select an option.</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 <ul style="list-style-type: none"> Add—To include the packet type in the match condition. • Delete—To remove an ICMP packet type from the match condition. |
| Fragment Offset | <p>Enter a fragment offset number or range and then select an option.</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. |

Table 131: Fields on the Match Criteria for IPv4 Firewall Filter *(Continued)*

| Field | Action |
|------------|--|
| Precedence | <p>Enter IP precedence 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. |
| DSCP | <p>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.</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. |
| TTL | <p>Enter an IPv4 TTL value by entering a number from 1 through 255 and select an option.</p> <p>NOTE: This option is not available in SRX5600 device.</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. |

Table 131: Fields on the Match Criteria for IPv4 Firewall Filter (*Continued*)

| Field | Action |
|------------------|--|
| Packet Length | <p>Specify a packet length, enter a value or range.</p> <p>Select an option.</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. |
| Forwarding Class | <p>Specify a forwarding class by selecting a forwarding class from the list or entering a forwarding class, and then select an option.</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. |
| IP Options | <p>Enter option by selecting an IP option from the list or entering a text or numeric string identifying the option, and then select an option.</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. |

Table 131: Fields on the Match Criteria for IPv4 Firewall Filter (Continued)

| Field | Action |
|---------------|---|
| IPsec ESP SPI | <p>Enter an ESP SPI value by entering a binary, hexadecimal, or decimal SPI value or range, and then select an option.</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. |
| Action | |
| Nothing | <p>Select Nothing.</p> <p>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.</p> |
| Accept | <p>Select Accept.</p> <p>Accepts a packet that meets the match conditions of the term.</p> |
| Discard | <p>Select Discard.</p> <p>Discards a packet that meets the match conditions of the term. Names a discard collector for packets.</p> |
| Reject | <p>Select Reject and then select a message type from the reason list.</p> <p>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.</p> <p>NOTE: To log and sample rejected packets, specify log and sample action modifiers in conjunction with this action.</p> |

Table 131: Fields on the Match Criteria for IPv4 Firewall Filter (Continued)

| Field | Action |
|-------------------------|--|
| Next Term | <p>Select Next Term.</p> <p>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.</p> |
| Routing Instance | <p>Accepts a packet that meets the match conditions, and forwards it to the specified routing instance.</p> <p>Select Routing Instance and enter the routing instance name in the box next to Routing Instance.</p> |
| Action Modifiers | |
| Forwarding Class | <p>Classifies the packet as a specific forwarding class.</p> <p>Select Forwarding Class from the list.</p> |
| Count | <p>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.</p> <p>Select Count and enter a 24-character string containing letters, numbers, or hyphens to specify a counter name.</p> |
| Virtual Channel | <p>Enter a string identifying the virtual channel.</p> <p>NOTE: This option is not available in SRX345 of devices.</p> |
| Prefix Action | <p>Enter the prefix action.</p> <p>NOTE: This option is not available in SRX4100 and SRX345 devices.</p> |
| Log | <p>Select Log.</p> <p>Logs the packet header information in the routing engine.</p> |

Table 131: Fields on the Match Criteria for IPv4 Firewall Filter (Continued)

| Field | Action |
|---------------|--|
| Syslog | <p>Select Syslog.</p> <p>Records packet information in the system log.</p> |
| Port Mirror | <p>Select Port Mirror.</p> <p>Port mirrors the packet.</p> <p>NOTE: This option is not available in SRX5600 and SRX345 devices.</p> |
| Loss Priority | <p>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.</p> <p>Select the range of priority from the list.</p> |

RELATED DOCUMENTATION

| [About the IPv4 Page](#) | 446

Firewall Filters—IPv6

IN THIS CHAPTER

- [About the IPv6 Page | 464](#)
- [Add IPv6 Firewall Filters | 465](#)

About the IPv6 Page

IN THIS SECTION

- [Tasks You Can Perform | 464](#)
- [Field Descriptions | 464](#)

You are here: **Network** > **Firewall Filters** > **IPv6**.

Use this page to configure IPv6 firewall filter.

Tasks You Can Perform

You can perform the following task from this page:

- Add an IPv6 Firewall Filters. See ["Add IPv6 Firewall Filters" on page 465](#) .

Field Descriptions

[Table 132 on page 465](#) describes the fields on IPv6 page.

Table 132: Fields on the IPv6 Page

| Field | Description |
|----------------------------|--|
| IPv6 Filter Summary | |
| Filter Name | Displays the name of the filter and when expanded, lists the terms attached to the filter. |
| Add New IPv6 Filter | |
| Filter Name | Searches for existing filters by filter name. |
| Term Name | Searches for existing terms by term name. |
| Location | Specifies the position of the new filter. |

RELATED DOCUMENTATION

| [Add IPv6 Firewall Filters](#) | 465

Add IPv6 Firewall Filters

You are here: **Network** > **Firewall Filters** > **IPv6**.

To add an IPv6 firewall filter:

1. Complete the configuration according to the guidelines provided in [Table 133 on page 466](#) and [Table 134 on page 469](#).
2. Click **Add** available in the Add New IPv6 Filter section.
A new IPv6 Firewall Filter is created.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

[Table 133 on page 466](#) describes the fields on the Add IPv6 page.

Table 133: Fields on the Add IPv6 Firewall Filter Page

| Field | Action |
|----------------------------|--|
| IPv6 Filter Summary | |
| Action column | <p>Select an option:</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 X from the same row. |
| Filter Name | <p>Enter 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. |
| Search | |

Table 133: Fields on the Add IPv6 Firewall Filter Page (*Continued*)

| Field | Action |
|----------------------------|---|
| 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. |
| 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. |
| Number of Items to Display | <p>Specifies the number of filters or terms to display on one page. Selects the number of items to be displayed on one page.</p> |
| Add New IPv6 Filter | |

Table 133: Fields on the Add IPv6 Firewall Filter Page (*Continued*)

| Field | Action |
|-------------|---|
| Filter Name | <p>Enter 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>Select an option:</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. |
| Term Name | <p>Searches for existing terms by term name.</p> <p>Select an option:</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. |
| Location | <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. |

Table 133: Fields on the Add IPv6 Firewall Filter Page (*Continued*)

| Field | Action |
|--------------------------|--|
| Add | <p>Click Add.</p> <p>Opens the Filter Term page allowing you to define the match conditions and the action for this term.</p> |
| Add New IPv6 Term | |
| Location | <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. |
| Add | <p>Click Add.</p> <p>Opens the Filter Term page allowing you to define the match conditions and the action for this term.</p> |

Table 134: Fields on the Match Criteria for IPv6 Firewall Filter

| Field | Action |
|---------------------|--------|
| Match Source | |

Table 134: Fields on the Match Criteria for IPv6 Firewall Filter *(Continued)*

| Field | 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>Enter an IP source address and prefix length, and select an option:</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. |
| 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>Select an option:</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. |
| 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>Select the port from the port name list; enter the port name, number, or range and then select an option:</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. |
| Match Destination | |

Table 134: Fields on the Match Criteria for IPv6 Firewall Filter (*Continued*)

| Field | 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>Enter an IP destination address and prefix length and select an option:</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. |
| 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>Select an option:</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. |
| 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>Select the port from the port name list; enter the port name, number, or range; and then select an option:</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. |

Match Source or Destination

Table 134: Fields on the Match Criteria for IPv6 Firewall Filter *(Continued)*

| Field | 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>Enter an IP destination address and prefix length and select an option:</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. |
| 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>Select an option:</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. |

Table 134: Fields on the Match Criteria for IPv6 Firewall Filter *(Continued)*

| Field | 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>Select the port from the port name list; enter the port name, number, or range; and then select an option:</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. |
| 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>Select a name from the interface name list or Enter the interface name and select an option:</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. |
| 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>Enter the interface set name and select an option:</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. |

Table 134: Fields on the Match Criteria for IPv6 Firewall Filter *(Continued)*

| Field | 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>Enter the name of the group and select an option:</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. |
| 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> <p>Select the check box.</p> |
| 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> <p>Select the check box.</p> |
| 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> <p>Enter a text or numeric string defining the flag.</p> |

Table 134: Fields on the Match Criteria for IPv6 Firewall Filter *(Continued)*

| Field | Action |
|-------------|---|
| 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> <p>Select a protocol name from the list or enter a protocol name or number and then select an option:</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. |
| 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>Select a packet type from the list or enter a packet type name or number and then select an option:</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. |

Table 134: Fields on the Match Criteria for IPv6 Firewall Filter *(Continued)*

| Field | Action |
|---------------|--|
| 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>Select a packet code from the list or enter the packet code as text or a number and select an option:</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. |
| 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. |
| 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>Specify a packet length, enter a value or range.</p> <p>Select an option:</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. |

Table 134: Fields on the Match Criteria for IPv6 Firewall Filter (Continued)

| Field | Action |
|------------------|--|
| 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>Specify a forwarding class by selecting a forwarding class from the list or entering a forwarding class, and then select an option:</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. |
| Action | |
| Nothing | <p>Select Nothing.</p> <p>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.</p> |
| Accept | <p>Select Accept.</p> <p>Accepts a packet that meets the match conditions of the term.</p> |
| Discard | <p>Select Discard.</p> <p>Discards a packet that meets the match conditions of the term. Names a discard collector for packets.</p> |
| Reject | <p>Select Reject and then select a message type from the reason list.</p> <p>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.</p> <p>NOTE: To log and sample rejected packets, specify log and sample action modifiers in conjunction with this action.</p> |

Table 134: Fields on the Match Criteria for IPv6 Firewall Filter (Continued)

| Field | Action |
|-------------------------|--|
| Next Term | <p>Select Next Term.</p> <p>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.</p> |
| Routing Instance | <p>Accepts a packet that meets the match conditions, and forwards it to the specified routing instance.</p> <p>Select Routing Instance and enter the routing instance name in the box next to Routing Instance.</p> |
| Action Modifiers | |
| Forwarding Class | <p>Classifies the packet as a specific forwarding class.</p> <p>Select Forwarding Class from the list.</p> |
| Count | <p>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.</p> <p>Select Count and enter a 24-character string containing letters, numbers, or hyphens to specify a counter name.</p> |
| Log | <p>Select Log.</p> <p>Logs the packet header information in the routing engine.</p> |
| Syslog | <p>Select Syslog.</p> <p>Records packet information in the system log.</p> |
| Loss Priority | <p>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.</p> <p>Select the range of priority from the list.</p> |

RELATED DOCUMENTATION

| [About the IPv6 Page](#) | 464

Firewall Filters—Assign to Interfaces

IN THIS CHAPTER

- [About the Assign to Interfaces Page | 480](#)

About the Assign to Interfaces Page

IN THIS SECTION

- [Field Descriptions | 480](#)

You are here: You are here: **Network** > **Firewall Filters** > **Assign To Interfaces**.

Use this page to configure interface for firewall filters.

Field Descriptions

[Table 135 on page 481](#) describes the fields on the Assign Interfaces page.

Table 135: Fields on the Assign Interfaces Page

| Field | Description |
|-------------------------|---|
| 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"> • Input firewall filter: <ul style="list-style-type: none"> • IPv4 Input Filter—Enter the name of IPv4 filter applied to received packets. • IPv6 Input Filter—Enter the name of IPv6 filter applied to received packets. • Output firewall filter: <ul style="list-style-type: none"> • IPv4 Output Filter—Enter the name of IPv4 filter applied to transmitted packets. • IPv6 Output Filter—Enter the name of IPv6 filter applied to transmitted packets. <p>Click OK to save the changes.</p> |
| 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. |

RELATED DOCUMENTATION

[Add IPv4 Firewall Filters | 447](#)

[Add IPv6 Firewall Filters | 465](#)

NAT Policies

IN THIS CHAPTER

- [About the NAT Policies Page | 482](#)
- [Create a Source NAT | 484](#)
- [Edit a Source NAT | 490](#)
- [Delete a Source NAT | 490](#)

About the NAT Policies Page

IN THIS SECTION

- [Tasks You Can Perform | 483](#)
- [Field Descriptions | 483](#)

You are here: **Network** > **NAT** > **Policies**.

Network Address Translation (NAT) is a form of network masquerading where you can hide devices between the zones or interfaces. A trust zone is a segment of the network where security measures are applied. It is usually assigned to the internal LAN. An untrust zone is the Internet. NAT modifies the IP addresses of the packets moving between the trust and untrust zones.

Whenever a packet arrives at the NAT device, the device performs a translation on the packet's IP address by rewriting it with an IP address that was specified for external use. After translation, the packet appears to have originated from the gateway rather than from the original device within the network. This helps you hide internal IP addresses from the other networks and keep your network secure.

Use this page to configure source, destination, and static NAT.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a source NAT. See ["Create a Source NAT" on page 484](#) .
- Edit a source NAT. See ["Edit a Source NAT" on page 490](#) .
- Delete a source NAT. See ["Delete a Source NAT" on page 490](#) .
- View destination NAT rules. For more information on destination NAT, see ["About the Destination Page" on page 502](#) .
- View static NAT rules. For more information on static NAT, see ["About the Static Page" on page 508](#) .

Field Descriptions

[Table 136 on page 483](#) describes the fields on the NAT Policies Page.

Table 136: Fields on the NAT Policies Page.

| Field | Description |
|--------------------|--|
| Seq | Displays the sequence number of rules in a context. Drag and drop the policies within the same context to reorder your NAT policy among the existing policies. |
| Hits | Displays the number of hits the rule has encountered. |
| Rule Name | Displays the rule name. |
| NAT Type | Displays whether the NAT is source, destination, or static. |
| Source Ingress | Displays the source ingress type. For example: zone, interface, or routing instance. |
| Source Address | Displays the match source address of the NAT policy. |
| Source Port | Displays the match source port of the NAT policy. |
| Destination Egress | Displays the match destination egress type. For example: zone, interface, or routing instance. |

Table 136: Fields on the NAT Policies Page. (Continued)

| Field | Description |
|---------------------|---|
| Destination Address | Displays the match destination address of the NAT policy. |
| Destination Port | Displays the match destination port of the NAT policy. |
| Applications | Displays the match application for the NAT policy. |
| Protocol | Displays the match IP protocol for the NAT policy. |
| Actions | Displays the action of the NAT policy. |
| Description | Displays the description for the NAT policy. |

Create a Source NAT

You are here: **Network > NAT > Policies.**

To create a source NAT:

1. Click **Create > Source NAT** on the upper right-side of the Policies page.
The inline creation fields will appear.
2. Complete the configuration according to the guidelines provided in [Table 137 on page 484](#).
3. Click the tick icon on the right-side of the row once done with the configuration.

Table 137: Fields on the Policies Page—Create Source NAT

| Field | Description |
|---------------------|--------------------------------------|
| Rule Name > Name | Enter a unique source NAT rule name. |

Source Ingress

Table 137: Fields on the Policies Page—Create Source NAT (Continued)

| Field | Description |
|-----------------------|--|
| Select Sources | |
| Source ingress type | <p>Select an option from the list for ingress traffic that originates from inside the network:</p> <ul style="list-style-type: none"> • Zone • Interface • Routing Instance |
| Zone | <p>Select the source zones in the Available column and use the right arrow to move them to the Selected column.</p> <p>NOTE: This option is available only if you select source ingress type as Zone.</p> |
| Interface | <p>Select the source interfaces in the Available column and use the right arrow to move them to the Selected column.</p> <p>NOTE: This option is available only if you select source ingress type as Interface.</p> |
| Routing instance | <p>Select the source routing instances in the Available column and use the right arrow to move them to the Selected column.</p> <p>NOTE: This option is available only if you select source ingress type as Routing Instance.</p> |
| Addresses | <p>Select the source addresses in the Available column and use the right arrow to move them to the Selected column.</p> <p>To create a new address:</p> <ol style="list-style-type: none"> 1. Click +. <ul style="list-style-type: none"> The Create Address page appears. 2. Enter the following details: <ul style="list-style-type: none"> • Name—Optional. Enter a unique name for source address. • Description—Enter the description for source address. • Host IP—Enter IPv4 or IPv6 host address. |

Table 137: Fields on the Policies Page—Create Source NAT (Continued)

| Field | Description |
|---------------------------|---|
| Ports/Port range | <p>Click + to enter port number or port range (for example, 1-5) with minimum and maximum values for source.</p> <p>Range: 0 through 65535.</p> <p>To edit a port number or port range, select it and click the pencil icon.</p> <p>To delete a port number or port range, select it and click the delete icon.</p> |
| Destination Egress | |
| Select Destination | |
| Destination egress type | <p>Select an option from the list for outgoing traffic that originates from inside of the device network:</p> <ul style="list-style-type: none"> • Zone • Interface • Routing Instance |
| Zone | <p>Select the destination zones in the Available column and use the right arrow to move them to the Selected column.</p> <p>NOTE: This option is available only if you select destination egress type as Zone.</p> |
| Interface | <p>Select the destination interfaces in the Available column and use the right arrow to move them to the Selected column.</p> <p>NOTE: This option is available only if you select destination egress type as Interface.</p> |
| Routing instance | <p>Select the destination routing instances in the Available column and use the right arrow to move them to the Selected column.</p> <p>NOTE: This option is available only if you select destination egress type as Routing Instance.</p> |

Table 137: Fields on the Policies Page—Create Source NAT (Continued)

| Field | Description |
|----------------------------|---|
| Addresses | <p>Select the destination addresses in the Available column and use the right arrow to move them to the Selected column.</p> <p>To create a new address:</p> <ol style="list-style-type: none"> Click +. <ul style="list-style-type: none"> The Create Address page appears. Enter the following details: <ul style="list-style-type: none"> Name—Optional. Enter a unique name for destination address. Description—Enter the description for destination address. Host IP—Enter IPv4 or IPv6 host address. |
| Ports/Port range | <p>Click + to enter port number or port range (for example, 1-5) with minimum and maximum values for destination.</p> <p>Range: 0 through 65535.</p> <p>To edit a port number or port range, select it and click the pencil icon.</p> <p>To delete a port number or port range, select it and click the delete icon.</p> |
| Applications | |
| Select Applications | |
| Applications | <p>Select an application option:</p> <ul style="list-style-type: none"> Any—Any applications you want to associate with the NAT policy. Specific—Select the applications in the Available column and use the right arrow to move them to the Selected column. None—No applications selected to associate with the NAT policy. |
| Protocols | |
| Select Protocols | |

Table 137: Fields on the Policies Page—Create Source NAT (Continued)

| Field | Description |
|------------------|---|
| Protocols | Select the protocols in the Available column and use the right arrow to move them to the Selected column. |
| Add Protocol | Click + and enter a protocol number to associate with the NAT policy. Range is 0 through 255. |
| Actions | |
| Actions | |
| Translation type | Select an option: <ul style="list-style-type: none"> • None—No translation is performed for the incoming traffic. • Interface—Performs interface-based translations on the source traffic. • Pool—Performs pool-based translations on the source traffic. |
| Source pool | Select a source pool from the list. Click Add New to create a new source NAT pool. For more information on field options, see " Create a Source NAT Pool " on page 494 . |
| Persistent | Enable this option for mapping all requests from the same internal transport address to the same reflexive transport address. |

Table 137: Fields on the Policies Page—Create Source NAT (Continued)

| Field | Description |
|------------------------|--|
| Persistent NAT type | <p>Select an option from the list:</p> <ul style="list-style-type: none"> • any-remote-host—All requests from a specific internal IP address and port are mapped to the same reflexive transport address. Any external host can send a packet to the internal host by sending the packet to the reflexive transport address. • target-host—All requests from a specific internal IP address and port are mapped to the same reflexive transport address. An external host can send a packet to an internal host by sending the packet to the reflexive transport address. The internal host must have previously sent a packet to the external hosts IP address. • target-host-port—All requests from a specific internal IP address and port are mapped to the same reflexive transport address. An external host can send a packet to an internal host by sending the packet to the reflexive transport address. The internal host must have previously sent a packet to the external hosts IP address and port. |
| Inactivity timeout | <p>Enter the amount of time that the persistent NAT binding remains in the sites memory when all the sessions of the binding entry have ended.</p> <p>Range is 60 through 7200 seconds.</p> |
| Maximum session number | <p>Enter the maximum number of sessions with which a persistent NAT binding can be associated.</p> <p>Range is 8 through 65536</p> |
| Description | <p>Enter the description for the source NAT.</p> |

RELATED DOCUMENTATION

[Edit a Source NAT | 490](#)

[Delete a Source NAT | 490](#)

Edit a Source NAT

You are here: **Network** > **NAT** > **Policies**.

To edit a source NAT:

1. Double-click an existing source NAT that you want to edit on the Policies page.
2. Complete the configuration according to the guidelines provided in "[Create a Source NAT](#)" on page 484 .
3. Click the tick icon on the right-side of the row once done with the configuration.

RELATED DOCUMENTATION

| [Delete a Source NAT | 490](#)

Delete a Source NAT

You are here: **Network** > **NAT** > **Policies**.

To delete a source NAT:

1. Select one or more source NATs that you want to delete on the Policies page.
2. Click the delete icon available on the upper-right corner of the page.
A confirmation message window appears.
3. Click **Yes** to delete or click **No** to retain the source NAT.

RELATED DOCUMENTATION

| [Create a Source NAT | 484](#)

| [Edit a Source NAT | 490](#)

NAT Pools

IN THIS CHAPTER

- [About the NAT Pools Page | 491](#)
- [Global Options | 493](#)
- [Create a Source NAT Pool | 494](#)
- [Edit a Source NAT Pool | 498](#)
- [Delete a Source NAT Pool | 499](#)
- [Add a Destination NAT Pool | 499](#)
- [Edit a Destination NAT Pool | 501](#)
- [Delete a Destination NAT Pool | 501](#)

About the NAT Pools Page

IN THIS SECTION

- [Tasks You Can Perform | 492](#)
- [Field Descriptions | 492](#)

You are here: **Network** > **NAT** > **Pools**.

A NAT pool is a set of IP addresses that you can define and use for translation. NAT policies perform address translation by translating internal IP addresses to the addresses in these pools. Unlike static NAT, where there is a one-to-one mapping that includes destination IP address translation in one direction and source IP address translation in the reverse direction, with source NAT, you translate the original source IP address to an IP address in the address pool. With destination NAT, you translate the original destination address to an IP address in the address pool.

Use this page to configure source and destination NAT pools.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a global option. See ["Global Options" on page 493](#) .
- Create a source NAT pool. See ["Create a Source NAT Pool" on page 494](#) .
- Edit a source NAT pool. See ["Edit a Source NAT Pool" on page 498](#) .
- Delete a source NAT pool. See ["Delete a Source NAT Pool" on page 499](#) .
- Add a destination NAT pool. See ["Add a Destination NAT Pool" on page 499](#) .
- Edit a destination NAT pool. See ["Edit a Destination NAT Pool" on page 501](#) .
- Delete a destination NAT pool. See ["Delete a Destination NAT Pool" on page 501](#) .

Field Descriptions

[Table 138 on page 492](#) describes the fields on the NAT Pools Page.

Table 138: Fields on the NAT Pools Page.

| Field | Description |
|--------------|---|
| Pool Name | Displays the NAT pool name. |
| Pool Type | Displays whether the NAT pool is either source or destination. |
| Pool Address | Displays the NAT pool address. |
| Proxy ARP/ND | Displays the Address Resolution Protocol (ARP) proxy or Neighbor Discovery Protocol (NDP) proxy for the NAT pool. |
| Description | Displays the description for the NAT pool. |

Global Options

You are here: **Network** > **NAT** > **Pools**.

To add global options for a NAT pool:

1. Click the **Global Options** available on the upper-right corner of the page.
The Global Options page appears.
2. Complete the configuration according to the guidelines provided in [Table 139 on page 493](#).
3. Click **OK** to save the changes.

Table 139: Fields on the Global Options Page

| Field | Action |
|----------------------------|---|
| Persistent address | Enable this option to ensure that the same IP address is assigned from the source NAT pool to a specific host for multiple concurrent sessions. |
| Port randomization | Enable port randomization. The device performs NAT translation choosing the IP address by round robin, then chooses the port used for that IP address by randomization. |
| Interface port overloading | Enable this option to set the port range for NAT interface overload mapping. It also allows you to block a specific port from being used in interface overload mapping. |
| Overloading factor | Enter a value for the port overloading capacity for the source NAT interface. For example, if overloading factor is set to 2, and it is multiplied by a maximum port capacity of 63,486, the port overloading threshold is 126,972. If the configured setting exceeds the maximum port capacity of the interface, an error message is generated during the configuration commit. |

RELATED DOCUMENTATION

[About the NAT Pools Page | 491](#)

[Create a Source NAT Pool | 494](#)

[Add a Destination NAT Pool | 499](#)

Create a Source NAT Pool

You are here: **Network** > **NAT** > **Pools**.

To add a source NAT pool:

1. Click **Create** > **Source NAT Pool** on the upper-right corner of the Pools page.
The Create Source NAT Pool page appears.
2. Complete the configuration according to the guidelines provided in [Table 140 on page 494](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

[Table 140 on page 494](#) describes the fields on the Create Source NAT Pool page.

Table 140: Fields on the Create Source NAT Pool Page

| Field | Description |
|------------------|---|
| Name | Enter a unique string of alphanumeric characters, hyphens and underscores; maximum length 63-character. |
| Description | Enter a description for the source NAT pool. |
| Basic | |
| Routing instance | Select a routing instance from the list. |

Table 140: Fields on the Create Source NAT Pool Page (Continued)

| Field | Description |
|-------------------------|--|
| Pool addresses | <p>Select the source NAT pool addresses in the Available column and the use the right arrow to move them to the Selected column.</p> <p>To add a new pool address:</p> <ol style="list-style-type: none"> Click +. <p>The Add Pool Address page appears.</p> <ol style="list-style-type: none"> Enter the following details: <ul style="list-style-type: none"> Name—Enter a name for the pool address. Description—Enter a description for the pool address. Pool address type—Select either IP address or address range for the pool. IP address—Enter IPv4 or IPv6 address of the host. <p>NOTE: This option is available only when you select IP address as pool address type.</p> Start Address—Enter the starting range of IPv4 or IPv6 address for the source NAT pool. <p>NOTE: This option is available only when you select Address Range as pool address type.</p> End Address—Enter the ending range of IPv4 or IPv6 address for the source NAT pool. <p>NOTE: This option is available only when you select Address Range as pool address type.</p> |
| Advanced | |
| Port Translation | |

Table 140: Fields on the Create Source NAT Pool Page (Continued)

| Field | Description |
|--------------------|---|
| Port translation | <p>Select a port translation option from the list:</p> <ul style="list-style-type: none"> • No Translation • Translation with port range—Port range from low to high. Range is 1024 through 65535. • Translation with port overloading factor—Port overloading capacity for the source NAT interface. |
| Shared Address | <p>Enable this option to map many-to-one external IP addresses. This increases NAT resources and improves traffic.</p> <p>NOTE: This option is available only when you select No Translation.</p> |
| Host address base | <p>Enter IPv4 or IPv6 address used as the host address base.</p> <p>For example, if the host address base is 198.51.100.30 and the NAT pool uses the range 203.0.113.10 to 203.0.113.20, then 198.51.100.30 translates to 203.0.113.10, 198.51.100.31 translates to 203.0.113.11, and so on.</p> |
| Port range from | <p>Enter the lower limit of the port range.</p> <p>Range: 1024 through 65535.</p> <p>NOTE: This option is available only when you select Translation with port range.</p> |
| Port range to | <p>Enter the upper limit of the port range.</p> <p>Range: 1024 through 65535.</p> <p>NOTE: This option is available only when you select Translation with port range.</p> |
| Overloading factor | <p>Enter the port overloading factor value.</p> <p>Range: 2 through 32.</p> <p>NOTE: This option is available only when you select Translation with port overloading factor.</p> |

Table 140: Fields on the Create Source NAT Pool Page (Continued)

| Field | Description |
|--------------------------|---|
| Address pooling | Specifies that multiple internal IP addresses can be mapped to the same external IP address. Use this option only when the source NAT pool is configured with no port translation. |
| Paired | Select this option to use in source NAT pools with port translation for applications that require all sessions associated with one internal IP address to be translated to the same external IP address for multiple sessions. NOTE: This option is available only when you enable Address Pooling. |
| Non-paired | Select this option to use in source NAT pools without port translation for assigning IP addresses using a round-robin fashion. NOTE: This option is available only when you enable Address Pooling. |
| Overflow pool type | Specify a source pool to use when the current address pool is exhausted: <ul style="list-style-type: none"> • None—No support for overflow. • Interface—Allow the interface to support overflow. • Pool—Name of the source address pool. NOTE: This option is available only when you select No Translation. |
| Overflow pool | Select a source address pool from the list. |
| Utilization Alarm | |
| Upper threshold | Enter an upper threshold percentage for pool address utilization at which an SNMP trap is triggered. Range: 50 through 100. |

Table 140: Fields on the Create Source NAT Pool Page (*Continued*)

| Field | Description |
|-----------------|--|
| Lower threshold | <p>Enter a lower threshold percentage for pool address utilization at which an SNMP trap is triggered.</p> <p>Range: 40 through 100.</p> <p>NOTE: This option can be set only if you configure the upper threshold value.</p> |

RELATED DOCUMENTATION

[About the NAT Pools Page | 491](#)

[Edit a Source NAT Pool | 498](#)

[Delete a Source NAT Pool | 499](#)

Edit a Source NAT Pool

You are here: **Network** > **NAT** > **Pools**.

To edit a source NAT pool:

1. Select an existing source NAT pool that you want to edit on the Pools page.
2. Click the pencil icon available on the upper-right corner of the page.

The Edit Source NAT Pool page appears with editable fields. For more information on the options, see "[Create a Source NAT Pool](#)" on page 494 .

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[Delete a Source NAT Pool | 499](#)

Delete a Source NAT Pool

You are here: **Network** > **NAT** > **Pools**.

To delete source NAT pool(s):

1. Select one or more source NAT pools that you want to delete on the Pools page.
2. Click the delete icon available on the upper-right corner of the page.
A confirmation message window appears.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the NAT Pools Page | 491](#)

[Create a Source NAT Pool | 494](#)

[Edit a Source NAT Pool | 498](#)

Add a Destination NAT Pool

You are here: **Network** > **NAT** > **Pools**.

To add a destination NAT pool:

1. Click **Create** > **Destination NAT Pool** on the upper-right corner of the Pools page.
The Create Destination NAT Pool page appears.
2. Complete the configuration according to the guidelines provided in [Table 141 on page 499](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

[Table 141 on page 499](#) describes the fields on the Create Destination NAT Pool page.

Table 141: Fields on the Create Destination NAT Pool Page

| Field | Action |
|-------------|---|
| Name | Enter the destination pool name. |
| Description | Enter a description for the destination pool. |

Table 141: Fields on the Create Destination NAT Pool Page (*Continued*)

| Field | Action |
|-------------------|---|
| Routing instance | Select a routing instance from the list. |
| Pool address type | Select one of the following pool address type: <ul style="list-style-type: none"> • Address & Port—Translate destination IP address or addresses and port number(s) to a specific IP address and one port number. • Address Range—Translate a range of destination IP addresses to another range of IP addresses. This mapping is one-to-one. |
| Pool address | Enter IPv4 or IPv6 address for destination pool. NOTE: This option is available only when you select Address & Port as pool address type. |
| Pool port | Enter a destination port value. Range: 0 through 65535. NOTE: This option is available only when you select Address & Port as pool address type. |
| Start address | Enter starting address (IPv4 or IPv6) of the destination address range. NOTE: This option is available only when you select Address Range as pool address type. |
| End address | Enter ending address (IPv4 or IPv6) of the destination address range. NOTE: This option is available only when you select Address Range as pool address type. |

RELATED DOCUMENTATION

[Edit a Destination NAT Pool | 501](#)

[Delete a Destination NAT Pool | 501](#)

[About the NAT Pools Page | 491](#)

[Create a Source NAT Pool | 494](#)

Edit a Destination NAT Pool

You are here: **Network** > **NAT** > **Pools**.

To edit a destination NAT pool:

1. Select an existing destination NAT pool that you want to edit on the Pools page.
2. Click the pencil icon available on the upper-right corner of the page.

The Edit Destination NAT Pool page appears with editable fields. For more information on the options, see "[Add a Destination NAT Pool](#)" on page 499 .

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[Delete a Destination NAT Pool](#) | 501

[About the NAT Pools Page](#) | 491

Delete a Destination NAT Pool

You are here: **Network** > **NAT** > **Pools**.

To delete destination NAT pool(s):

1. Select one or more destination NAT pools that you want to delete on the Pools page.
2. Click the delete icon available on the upper-right corner of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[Add a Destination NAT Pool](#) | 499

[Edit a Destination NAT Pool](#) | 501

Destination NAT

IN THIS CHAPTER

- [About the Destination Page | 502](#)
- [Add a Destination Rule Set | 504](#)
- [Edit a Destination Rule Set | 507](#)
- [Delete a Destination Rule Set | 507](#)

About the Destination Page

IN THIS SECTION

- [Tasks You Can Perform | 502](#)
- [Field Descriptions | 503](#)

You are here: **Network > NAT > Destination.**

Use this page to add, edit, or delete destination NAT configurations.

Tasks You Can Perform

You can perform the following tasks from this page:

- [Add a Destination Rule Set. See "Add a Destination Rule Set" on page 504.](#)
- [Edit a Destination Rule Set. See "Edit a Destination Rule Set" on page 507.](#)
- [Delete a Destination Rule Set. See "Delete a Destination Rule Set" on page 507.](#)

Field Descriptions

Table 142 on page 503 describes the fields on the Destination Page.

Table 142: Fields on the Destination Page.

| Field | Description |
|-----------------------------------|--|
| Destination 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 destination 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 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. |

Table 142: Fields on the Destination Page. (Continued)

| Field | Description |
|------------------------|--|
| Match Destination Port | Displays the match destination port. |
| Action | Displays the action of the rule in the selected rule set. |
| Upper Threshold | Displays upper threshold at which an SNMP trap is triggered. |
| Lower Threshold | Displays lower threshold at which an SNMP trap is triggered. |
| Description | Displays a description of the rule in the selected destination NAT rule set. |

RELATED DOCUMENTATION

| [Add a Destination Rule Set](#) | 504

Add a Destination Rule Set

You are here: **Network** > **NAT** > **Destination**.

To add a destination Rule Set:

1. Click **+** on the upper-right corner of the Destination page.
The Add Rule Set page appears.
2. Complete the configuration according to the guidelines provided in [Table 143 on page 504](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

[Table 143 on page 504](#) describes the fields on the Add Rule Set page.

Table 143: Fields on the Add Rule Set page.

| Field | Action |
|---------------------|--------|
| Add Rule Set | |

Table 143: Fields on the Add Rule Set page. (Continued)

| Field | Action |
|----------------------|--|
| Rule Set Name | Enter the rule set name. |
| Rule Set Description | Enter a description for the rule set. |
| From | <p>Specifies the filter options. Select an option:</p> <ul style="list-style-type: none"> • Routing Instance • Zone • Interface <p>Select the routing instances/zones/interfaces in the Available column and the use the right arrow to move them to the Selected column.</p> |
| Add Rule | |
| Rule Name | Enter the rule name. |
| Rule Description | Enter a description for the rule. |
| Match | |
| Source Address | <p>Search and select the source addresses in the Available column and the use the right arrow to move them to the Selected column.</p> <p>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.</p> |
| Destination Address | Enter the destination IP address. |
| Port | Enter the destination port number. |
| IP Protocol | Enter the protocol name in the text box and click + to add the protocol to the IP Protocol column. |

Table 143: Fields on the Add Rule Set page. (Continued)

| Field | Action |
|-------------------------------------|--|
| Actions | Specifies the actions for the destination NAT pool. Select an option: <ul style="list-style-type: none"> No Destination NAT. Do Destination NAT With Pool. |
| Do Destination NAT With Pool | |
| Add New Pool | Select a pool from the list or click +. |
| Add Destination Pool | |
| Pool Name | Enter the destination pool name. |
| Pool Description | Enter a description for the destination pool. |
| Routing Instance | Specifies the routing instance available. Select an option. |
| Pool Addresses and Port | |
| Address/Port | Enter the destination pool address. |
| Port | Enter the destination pool port number. |
| Address Range | Enter the destination pool address range. |
| Upper Threshold | Enter upper threshold at which an SNMP trap is triggered. Session count hit alarm range: 1 through 4294967295 |
| Lower Threshold | Enter lower threshold at which an SNMP trap is triggered. Rule session count alarm range: 1 through 4294967295 |

RELATED DOCUMENTATION

[Edit a Destination Rule Set | 507](#)

Edit a Destination Rule Set

You are here: **Network** > **NAT** > **Destination**.

To edit a destination rule set:

1. Select an existing destination rule set that you want to edit on the Destination page.
2. Click the pencil icon available on the upper-right corner of the page.

The Edit Rule Set page appears with editable fields. For more information on the options, see "[Add a Destination Rule Set](#)" on page 504 .

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[Delete a Destination Rule Set | 507](#)

Delete a Destination Rule Set

You are here: **Network** > **NAT** > **Destination**.

To delete destination rule set(s):

1. Select one or more destination rule sets that you want to delete on Destination page.
2. Click the delete icon available on the upper-right corner of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[Add a Destination NAT Pool | 499](#)

Static NAT

IN THIS CHAPTER

- [About the Static Page | 508](#)
- [Add a Static Rule Set | 510](#)
- [Edit a Static Rule Set | 514](#)
- [Delete a Static Rule Set | 514](#)

About the Static Page

IN THIS SECTION

- [Tasks You Can Perform | 508](#)
- [Field Descriptions | 509](#)

You are here: **Network** > **NAT** > **Static**.

Use this page to configure static NAT.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a static rule set and rules to it. See ["Add a Static Rule Set" on page 510](#) .
- Edit a static rule set and its rules. See ["Edit a Static Rule Set" on page 514](#) .
- Delete a static rule set and its rules. See ["Delete a Static Rule Set" on page 514](#) .
- Move the rules in the rules table. To do this, select a rule which you want to move and select the following options according to your choice:

- Move Up—Enables you to move the rule up in the list.
- Move Down—Enables you to move the rule down in the list.
- Move to Top—Enables you to move the rule to top of the list
- Move to Bottom—Enables you to move the rule to the bottom of the list

Field Descriptions

[Table 144 on page 509](#) describes the fields on the Static page.

Table 144: Fields on the Static Page

| Field | Description |
|-----------------------------------|--|
| 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 options. |
| Name | Displays the name of the static NAT rule set. |
| From | Displays the name of the routing instance, zone, or 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 | |

Table 144: Fields on the Static Page (Continued)

| Field | Description |
|-----------------------|--|
| Rule Name | Displays the name of the routing instance, zone, or interface to which the packet flows. |
| Source Addresses | Displays the source address to match the rule. |
| Source Ports | Displays the source port number. |
| Destination Addresses | Displays the destination address to match the rule. |
| Destination Ports | Displays the destination port number. |
| Prefix | Displays the static IP address prefix. |
| Mapped Port | Displays the destination port or port range to allow static NAT to map ports. |
| Upper Threshold | Displays the upper threshold value of the at which an SNMP trap is triggered. |
| Lower Threshold | Displays the lower threshold value of the at which an SNMP trap is triggered. |
| Description | Displays the description of the rule in the selected static NAT rule set. |

RELATED DOCUMENTATION

[Add a Static Rule Set | 510](#)

[Edit a Static Rule Set | 514](#)

[Delete a Static Rule Set | 514](#)
Add a Static Rule Set

You are here: **Network** > **NAT** > **Static**.

To add a static rule set:

1. Click **+** on the upper-right corner of the Static page.
The Add Rule Set page appears.
2. Complete the configuration according to the guidelines provided in [Table 145 on page 511](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 145: Fields on the Add Static Rule Set Page

| Field | Action |
|----------------------|---|
| Rule Set Name | Enter a rule set name. |
| Rule Set Description | Enter a description for the rule set. |
| From | <p>Select a filter option from the list:</p> <ul style="list-style-type: none"> • Routing Instance • Zone • Interface <p>Select the routing instances, zones, or interfaces in the Available column and use the right arrow to move them to the Selected column.</p> |
| Rules | |
| Rules | Specifies the rules added to the selected static rule set. |

Table 145: Fields on the Add Static Rule Set Page (Continued)

| Field | Action |
|-------|--|
| Add | <p>To add a rule to the selected static rule set:</p> <ol style="list-style-type: none"> Click + available at the upper right of the Rules table. The Add Rule page appears. Enter the following details: <ul style="list-style-type: none"> Rule Name—Enter a rule name. Rule Description—Enter a description for the rule. Match—Displays the match destination address. <ul style="list-style-type: none"> Source Address—Select an IPv4 or IPv6 address from the list or enter the address and click + to add it. Select an existing IPv4 or IPv6 address and click X to delete it. Source Port—Enter a port number or port range from low to high and click + to add it. Port Range: 0 through 65535. Select an existing port and click X to delete it. Destination Address—Select IPv4 or IPv6 and then select an address from the list. Destination Port—Select one of the following options: <ul style="list-style-type: none"> Any—Selects available port. Port—Enter a port number. Port Range—Enter a port range from low to high. Then—Enter the following details: <ul style="list-style-type: none"> Host Address—Enter the static prefix address. <p>NOTE: You can select Translate to ipv4 address if you have selected IPv6 in the destination address.</p> |

Table 145: Fields on the Add Static Rule Set Page (*Continued*)

| Field | Action |
|--------|---|
| | <ul style="list-style-type: none"> • Mapped Port—Select one of the following options: <ul style="list-style-type: none"> • Any—Selects available port. • Port—Enter a port number. • Port Range—Enter a port range from low to high. • Routing Instance—Select a routing instance from the list. • Upper Threshold—Enter an upper threshold value at which an SNMP trap is triggered. Range: 1 through 4294967295. • Lower Threshold—Enter a lower threshold value at which an SNMP trap is triggered. Range: 1 through 4294967295. <p>NOTE: This option can be set only if you configure the upper threshold value.</p> <p>3. Click OK to save the changes. If you want to discard your changes, click Cancel.</p> |
| Edit | <p>Select an existing rule and click the edit icon at the upper-right corner of the Rules table.</p> <p>The Edit Interface page appears with editable fields.</p> |
| Delete | <p>Select an interface and click the delete icon at the upper-right corner of the Rules table.</p> <p>A confirmation window appears. Click Yes to delete the selected interface or click No to discard.</p> |

RELATED DOCUMENTATION

[About the Static Page | 508](#)

[Edit a Static Rule Set | 514](#)

[Delete a Static Rule Set | 514](#)

Edit a Static Rule Set

You are here: **Network** > **NAT** > **Static**.

To edit a static rule set and its rules:

1. Select an existing static rule set that you want to edit on the Static page.
2. Click the pencil icon available on the upper-right corner of the Static page.

The Edit Static Rule Set page appears with editable fields. For more information on the options, see ["Add a Static Rule Set" on page 510](#).

NOTE: Alternatively, you can select the rule directly and click the pencil icon available on the upper-right corner of the Rules table to edit a rule for the selected rule set.

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[About the Static Page | 508](#)

[Add a Static Rule Set | 510](#)

[Delete a Static Rule Set | 514](#)

Delete a Static Rule Set

You are here: **Network** > **NAT** > **Static**.

To delete a static rule set and its rules:

1. Select one or more static rules sets that you want to delete on the Static page.
2. Click the delete icon available on the upper-right corner of the page.

A confirmation window appears.

NOTE: Alternatively, you can select the rule directly and click the delete (X) icon available on the upper-right corner of the Rules table to delete a rule for the selected rule set.

3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the Static Page | 508](#)

[Add a Static Rule Set | 510](#)

[Edit a Static Rule Set | 514](#)

NAT Proxy ARP/ND

IN THIS CHAPTER

- [About the Proxy ARP/ND Page | 516](#)
- [Add a Proxy ARP | 517](#)
- [Edit a Proxy ARP | 519](#)
- [Delete a Proxy ARP | 519](#)
- [Add a Proxy ND | 520](#)
- [Edit a Proxy ND | 521](#)
- [Delete a Proxy ND | 521](#)

About the Proxy ARP/ND Page

IN THIS SECTION

- [Tasks You Can Perform | 516](#)
- [Field Descriptions | 517](#)

You are here: **Network** > **NAT** > **Proxy ARP/ND**.

You can add, edit, and delete proxy ARP or proxy ND configurations.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a proxy ARP. See ["Add a Proxy ARP" on page 517](#) .
- Edit a proxy ARP. See ["Edit a Proxy ARP" on page 519](#) .

- Delete a proxy ARP. See ["Delete a Proxy ARP" on page 519](#) .
- Create a proxy ND. See ["Add a Proxy ND" on page 520](#) .
- Edit a proxy ND. See ["Edit a Proxy ND" on page 521](#) .
- Delete a proxy ND. See ["Delete a Proxy ND" on page 521](#) .
- Launch NAT wizard. To do this, click **Launch Wizard** option at the upper-right corner of the page. The NAT wizard leads you through the basic required steps to configure NAT for the SRX Series security device.

Field Descriptions

[Table 146 on page 517](#) describes the fields on the Proxy ARP/ND Configuration page.

Table 146: Fields on the Proxy ARP/ND Configuration Page

| Field | Description |
|-----------|------------------------------------|
| Interface | Displays the interface type. |
| Address | Displays the IPv4 or IPv6 address. |

RELATED DOCUMENTATION

[Add a Proxy ARP | 517](#)

[Edit a Proxy ARP | 519](#)

[Delete a Proxy ARP | 519](#)

[Add a Proxy ND | 520](#)

[Edit a Proxy ND | 521](#)

[Delete a Proxy ND | 521](#)

Add a Proxy ARP

You are here: **Network** > **NAT** > **Proxy ARP/ND**.

To add a proxy ARP:

1. Click **+** on the upper-right corner of the proxy ARP/ND page.
Select the Proxy ARP page. The Add Proxy ARP page appears.
2. Complete the configuration according to the guidelines provided in [Table 147 on page 518](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 147: Fields on the Add Proxy ARP Page

| Field | Action |
|--------------------|--|
| Interface | Enter the interface type. Select an option: <ul style="list-style-type: none"> • ge-0/0/0.0 • ge-0/0/2.0 • lo0.0 • vlan0.0 |
| Addresses | Displays the proxy ARP IP address. Click Delete to deleted the proxy ARP address. |
| IPv4 Address/Range | Enter the source IP address range and the end IP address that the device can be assigned to. Click + to add to the addresses. |

RELATED DOCUMENTATION

[About the Proxy ARP/ND Page | 516](#)

[Edit a Proxy ARP | 519](#)

[Delete a Proxy ARP | 519](#)

[Add a Proxy ND | 520](#)

[Edit a Proxy ND | 521](#)

[Delete a Proxy ND | 521](#)

Edit a Proxy ARP

You are here: **Network** > **NAT** > **Proxy ARP/ND**.

To edit a proxy ARP:

1. Select an existing proxy ARP that you want to edit on the Proxy ARP/ND page.
2. Click the pencil icon available on the upper-right corner of the page.

The Edit Proxy ARP page appears with editable fields. For more information on the options, see "[Add a Proxy ARP](#)" on page 517 .

3. Click **OK** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

[About the Proxy ARP/ND Page | 516](#)

[Add a Proxy ARP | 517](#)

[Delete a Proxy ARP | 519](#)

[Add a Proxy ND | 520](#)

[Edit a Proxy ND | 521](#)

[Delete a Proxy ND | 521](#)

Delete a Proxy ARP

You are here: **Network** > **NAT** > **Proxy ARP/ND**.

To delete proxy ARP(s):

1. Select one or more proxy ARPs that you want to delete on the Proxy ARP page.
2. Click the delete icon available on the upper-right corner of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the Proxy ARP/ND Page | 516](#)

[Add a Proxy ARP | 517](#)

[Edit a Proxy ARP | 519](#)

[Add a Proxy ND | 520](#)

[Edit a Proxy ND | 521](#)

[Delete a Proxy ND | 521](#)

Add a Proxy ND

You are here: **Network** > **NAT** > **Proxy ARP/ND**.

To add a proxy ND:

1. Click **+** on the upper-right corner of the proxy ARP/ND page.
The Add Proxy ND page appears.
2. Complete the configuration according to the guidelines provided in [Table 148 on page 520](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 148: Fields on the Add Proxy ND Page

| Field | Action |
|--------------------|---|
| Interface | Enter the interface type. Select an option: <ul style="list-style-type: none"> • ge-0/0/0.0 • ge-0/0/1.0 • ge-0/0/3.0 • lo0.0 |
| Addresses | Displays the proxy ND IP address. Click Delete to deleted the proxy ND address. |
| IPv6 Address/Range | Enter the source IPv6 address range and the end IPv6 address that the device can be assigned to. Click + to add to the addresses. |

RELATED DOCUMENTATION

[About the Proxy ARP/ND Page | 516](#)

[Add a Proxy ARP | 517](#)

[Edit a Proxy ARP | 519](#)

[Delete a Proxy ARP | 519](#)

[Edit a Proxy ND | 521](#)

[Delete a Proxy ND | 521](#)

Edit a Proxy ND

You are here: **Network** > **NAT** > **Proxy ARP/ND**.

To edit a proxy ND:

1. Select an existing proxy ND that you want to edit on the Proxy ARP/ND page.
2. Click the pencil icon available on the upper-right corner of the page.

The Edit Proxy ND page appears with editable fields. For more information on the options, see "[Add a Proxy ND](#)" on page 520 .

3. Click **OK** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

[About the Proxy ARP/ND Page | 516](#)

[Add a Proxy ARP | 517](#)

[Edit a Proxy ARP | 519](#)

[Delete a Proxy ARP | 519](#)

[Add a Proxy ND | 520](#)

[Delete a Proxy ND | 521](#)

Delete a Proxy ND

You are here: **Network** > **NAT** > **Proxy ARP/ND**.

To delete proxy ND(s):

1. Select one or more proxy NDs that you want to delete on the Proxy ND page.
2. Click the delete icon available on the upper-right corner of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the Proxy ARP/ND Page | 516](#)

[Add a Proxy ARP | 517](#)

[Edit a Proxy ARP | 519](#)

[Delete a Proxy ARP | 519](#)

[Add a Proxy ND | 520](#)

[Edit a Proxy ND | 521](#)

Static Routing

IN THIS CHAPTER

- [About the Static Routing Page | 523](#)
- [Add a Static Route | 524](#)
- [Edit a Static Route | 526](#)
- [Delete a Static Route | 526](#)

About the Static Routing Page

IN THIS SECTION

- [Tasks You Can Perform | 523](#)
- [Field Descriptions | 524](#)

You are here: **Network** > **Routing** > **Static Routing**.

Use this page to view, add, and remove link aggregation configuration details.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a static route. See ["Add a Static Route" on page 524](#) .
- Edit a static route. See ["Edit a Static Route" on page 526](#) .
- Delete a static route. See ["Delete a Static Route" on page 526](#) .

Field Descriptions

Table 149 on page 524 describes the fields on the Static Routing page.

Table 149: Fields on the Static Routing Page

| Field | Description |
|------------------|--|
| Route | Displays the static route selected. |
| Next-hop | Displays the selected next-hop address. |
| Routing Instance | Displays the routing instance selected for this route. |

RELATED DOCUMENTATION

| [Add a Static Route | 524](#)

Add a Static Route

You are here: **Network > Routing > Static Routing.**

To add a static route:

1. Click **+** on the upper-right corner of the Static Routing page.
The Add Static Route page appears.
2. Complete the configuration according to the guidelines provided in [Table 150 on page 525](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.
If you click **OK**, a new static route is added with the provided configuration.

Table 150: Fields on the Add Static Route Page

| Field | Description |
|------------------|--|
| Routing Instance | <p>Select the routing instance from the list.</p> <p>The selected destination routing instance that points to the routing table containing the tunnel destination address.</p> <p>NOTE: If you log in as a tenant user, routing instance is not displayed as tenant context supports only one routing instance.</p> |
| IPv4 | Click the IPv4 button. |
| IP address | Enter the static route IPv4 address. |
| Subnet mask | Enter the subnet mask. For example, 24 bits represents the 255.255.255.0 address. |
| IPv6 | Click the IPv6 button. |
| IPv6 address | Enter the static route IPv6 address. |
| Prefix | Enter the prefix for IPv6 address. |
| Next-hop | <p>Displays the next-hop address created.</p> <p>Click any one of the following</p> <ul style="list-style-type: none"> • +—To add the next-hop, enter the following details and click OK: <ul style="list-style-type: none"> • IP Address/IPv6 Address—Enter the IPv4 or IPv6 address based on the selected static route address type. • Interface Name—Select an interface from the list. • Delete—Select one or more next-hop addresses and click X. Then, click Yes to delete it. |

RELATED DOCUMENTATION

[Edit a Static Route | 526](#)

Edit a Static Route

You are here: **Network** > **Routing** > **Static Routing**.

To edit a static route:

1. Select the existing static route that you want to edit on the Static Routing page.
2. Click the pencil icon available on the upper-right corner of the Static Routing page.

The Edit Static Route page appears with editable fields. For more information on the options, see ["Add a Static Route" on page 524](#).

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

| [Delete a Static Route | 526](#)

Delete a Static Route

You are here: **Network** > **Routing** > **Static Routing**.

To delete a static route:

1. Select the existing static route that you want to delete on the Static Routing page.
2. Click the delete icon available on the upper-right corner of the Static Routing page.

A confirmation window appears.

3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

| [About the Static Routing Page | 523](#)

RIP Routing

IN THIS CHAPTER

- [About the RIP Page | 527](#)
- [Add a RIP Instance | 529](#)
- [Edit a RIP Instance | 531](#)
- [Delete a RIP Instance | 531](#)
- [Edit RIP Global Settings | 531](#)
- [Delete RIP Global Settings | 535](#)

About the RIP Page

IN THIS SECTION

- [Tasks You Can Perform | 527](#)
- [Field Descriptions | 528](#)

You are here: **Network > Routing > RIP.**

Use this page to configure RIP.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a RIP instance. See "[Add a RIP Instance](#)" on page 529 .
- Edit a RIP instance. See "[Edit a RIP Instance](#)" on page 531 .
- Delete a RIP instance. See "[Delete a RIP Instance](#)" on page 531 .

- Edit RIP global settings. See ["Edit RIP Global Settings" on page 531](#) .
- Delete RIP global settings. See ["Delete RIP Global Settings" on page 535](#) .

Field Descriptions

[Table 151 on page 528](#) describes the fields on the RIP page.

Table 151: Fields on the RIP Page

| Field | Description |
|----------------------------|--|
| Routing Instance | Select a routing instance from the list. |
| RIP Instances | |
| RIP Instances | Displays the RIP instance selected. |
| Neighbors | Displays the neighbors selected. |
| Routing Instance | Displays the routing instance. |
| Export Policies | Displays the export policies selected. |
| 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. |
| RIP Global Settings | |
| Name | Displays the name of the RIP. |
| Value | Displays the values for RIP. |

RELATED DOCUMENTATION

| [Add a RIP Instance](#) | 529

Add a RIP Instance

You are here: **Network** > **Routing** > **RIP**.

To add a RIP instance:

1. Click **+** on the upper-right corner of the RIP page.
The Add page appears.
2. Complete the configuration according to the guidelines provided in [Table 152 on page 529](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.
If you click **OK**, a new RIP instance is added with the provided configuration.

Table 152: Fields on the Add Page

| Field | Action |
|-------------------|---|
| General | |
| Routing Instance | Select a routing instance from the list to display only the default routing instance or all routing instances. |
| RIP Instance Name | Enter the RIP instance name. |
| Preference | Enter the preference of the external routes learned by RIP as compared to those learned from other routing protocols. |
| Metric out | Enter the metric value to add to routes transmitted to the neighbor. |
| Update Interval | Enter the update time interval to periodically send out routes learned by RIP to neighbors. |
| Route Timeout | Enter the route timeout interval for RIP. |
| Policy | |

Table 152: Fields on the Add Page (Continued)

| Field | 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.</p> <p>Click one of the following options:</p> <ul style="list-style-type: none"> • +—Adds an import policy. • Move up arrow—Moves the selected policy up the list of policies. • Move down arrow—Moves the selected policy down the list of policies. • X—Removes an import policy. |
| Export Policy | <p>Specifies one or more policies to control which summary LSAs are flooded into an area.</p> <p>Click one of the following options:</p> <ul style="list-style-type: none"> • +—Adds an export policy. • Move up arrow—Moves the selected policy up the list of policies. • Move down arrow—Moves the selected policy down the list of policies. • X—Removes an export policy. |
| Neighbor | |
| Displays the RIP-enabled interfaces, its port, metric-in, and update interval. | |
| Associate | <p>Select interface(s) to associate with the RIP.</p> <p>Select the box next to the interface name to enable RIP on an interface.</p> <p>Click the edit icon to modify one or more selected interfaces settings.</p> <p>NOTE: Only logical interfaces for RIP are displayed.</p> |

RELATED DOCUMENTATION

[Edit a RIP Instance](#) | 531

Edit a RIP Instance

You are here: **Network** > **Routing** > **RIP**.

To edit a RIP instance:

1. Select the existing logical system profile that you want to edit on the RIP page.
2. Click the pencil icon available on the upper-right corner of the RIP page.

The Edit page appears with editable fields. For more information on the options, see "[Add a RIP Instance](#)" on page 529 .

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

| [Delete a RIP Instance](#) | 531

Delete a RIP Instance

You are here: **Network** > **Routing** > **RIP**.

To delete a RIP instance:

1. Select the existing logical system profile that you want to delete on the RIP page.
2. Click the delete icon available on the upper-right corner of the RIP page.

A confirmation window appears.

3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

| [Edit RIP Global Settings](#) | 531

Edit RIP Global Settings

You are here: **Network** > **Routing** > **RIP**.

To edit RIP global settings:

1. Click the pencil icon on the upper-right corner of the RIP Global Settings table.
The Edit RIP Global Settings page appears.
2. Complete the configuration according to the guidelines provided in [Table 153 on page 532](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 153: Fields on the Edit RIP Global Settings Page

| Field | Action |
|-----------------------|--|
| General | |
| Send | Select a RIP send options from the list: <ul style="list-style-type: none"> • Broadcast • Multicast • None • Version-1 |
| Receive | Select a RIP receive options from the list: <ul style="list-style-type: none"> • Both • None • Version-1 • Version-2 |
| Route timeout (sec) | Enter the route timeout interval value for RIP. |
| Update interval (sec) | Enter the update time interval value to periodically send out routes learned by RIP to neighbors. |
| Hold timeout (sec) | Enter the hold timeout interval period for which the expired route is retained in the routing table before being removed. |
| Metric in | Enter the metric-in value to add to incoming routes when advertising into RIP routes that were learned from other protocols. |

Table 153: Fields on the Edit RIP Global Settings Page (*Continued*)

| Field | Action |
|---------------------|---|
| RIB Group | Select a routing table group to install RIP routes into multiple routing tables. |
| Message size | Enter the number of route entries to be included in every RIP update message. |
| Check Zero | <p>Specifies whether the reserved fields in a RIP packet are set to zero.</p> <p>Select an option:</p> <ul style="list-style-type: none"> • True—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-zero the RIP version 1 and version 2 specifications. • False—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. |
| Graceful switchover | <p>Specifies graceful switch over for RIP.</p> <p>Enter the following:</p> <ul style="list-style-type: none"> • Disable—Select the check box to disable graceful switchover. • Restart time (sec)—Enter the time in seconds for the restart to complete. |
| Authentication | <p>Enter the following:</p> <ul style="list-style-type: none"> • Authentication Type—Select 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 • Authentication key—Enter the authentication key for MD5. |
| Policy | |

Table 153: Fields on the Edit RIP Global Settings Page (*Continued*)

| Field | Action |
|----------------------|---|
| Import Policy | <p>Specifies one or more policies to routes being imported into the local routing device from the neighbors.</p> <p>Click one of the following options:</p> <ul style="list-style-type: none"> • +—Adds an import policy. • Move up arrow—Moves the selected policy up the list of policies. • Move down arrow—Moves the selected policy down the list of policies. • X—Removes an import policy. |
| Trace Options | |
| File Name | Enter the filename to receive the output of the trace operation. |
| Number of Files | Enter the maximum number of trace files. |
| File Size | Enter the maximum size for each trace file. |
| World-readable | <p>Specifies whether or not the trace file can be read by any user or not.</p> <p>Select an option:</p> <ul style="list-style-type: none"> • True—Allows any user to read the file. • False—Restricts all users being able to read the file. |
| Flags | Select one or more flags from the Available Flags column and move it to the Configured Flags column using the arrow. |

RELATED DOCUMENTATION

[Delete RIP Global Settings](#) | 535

Delete RIP Global Settings

You are here: **Network** > **Routing** > **RIP**.

To delete RIP global settings:

1. Select an information that you want to delete on the RIP Global settings table.
2. Click the delete icon available on the upper-right corner of the RIP Global settings table.
A confirmation window appears.
3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

| [About the RIP Page](#) | 527

OSPF Routing

IN THIS CHAPTER

- [About the OSPF Page | 536](#)
- [Add an OSPF | 538](#)
- [Edit an OSPF | 547](#)
- [Delete an OSPF | 547](#)

About the OSPF Page

IN THIS SECTION

- [Tasks You Can Perform | 536](#)
- [Field Descriptions | 537](#)

You are here: **Network** > **Routing** > **OSPF**.

Use this page to configure OSPF routing.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add an OSPF. See ["Add an OSPF" on page 538](#) .
- Edit an OSPF. See ["Edit an OSPF" on page 547](#) .
- Delete OSPF. See ["Delete an OSPF" on page 547](#) .
- Advanced search for an OSPF. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you

hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

For an advanced search:

1. Enter the search string in the text box.

Based on your input, a list of items from the filter context menu appears.

2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.

3. Press Enter to display the search results in the grid.
- Show or hide columns in the OSPF table. To do this, click the Show Hide Columns icon in the upper-right corner of the OSPF table and select the options you want to view or deselect the options you want to hide on the page.

Field Descriptions

Table 154 on page 537 describes the fields on the OSPF page.

Table 154: Fields on the OSPF Page

| Field | Description |
|-------------------|---|
| Filter | Select an instance for OSPF from the list. |
| Area ID | Displays the area ID selected. |
| Area Type | Displays the area type selected. |
| Member Interfaces | Displays the member interface selected. |
| Version | Displays the version of the interface selected (OSPF for IPv4 and OSPFv3 for IPv6). |

Table 154: Fields on the OSPF Page (Continued)

| Field | Description |
|------------------|---|
| 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. |

RELATED DOCUMENTATION

[Add an OSPF](#) | 538

Add an OSPF

You are here: **Network** > **Routing** > **OSPF**.

To add an OSPF routing:

1. Click **+** on the upper-right corner of the OSPF page.
The Create OSPF page appears.
2. Complete the configuration according to the guidelines provided in [Table 155 on page 538](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.
If you click **OK**, a new OSPF routing is added with the provided configuration.

Table 155: Fields on the Add an OSPF Page

| Field | Action |
|-----------------------|--------|
| Basic Settings | |

Table 155: Fields on the Add an OSPF Page (Continued)

| Field | Action |
|------------------------|--|
| Routing Instance | <p>Select the routing instance from the list or create a new routing instance inline.</p> <p>NOTE: This option is not available for tenant users.</p> <p>To add a new routing instance inline:</p> <ol style="list-style-type: none"> Click Add. <p>The Create Routing Instance page appears.</p> <ol style="list-style-type: none"> Enter the following details: <ul style="list-style-type: none"> General Settings <ul style="list-style-type: none"> Name—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—Enter a description for the routing instance. We recommend that you enter a maximum of 255 characters. Instance Type—Select a type of routing instance from the 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—Select one or more interfaces to associate with the routing instance from the Available column and move it to the Selected column using arrow. <p>To search for specific interface, click the search icon and enter partial text or full text of the keyword in the search bar.</p> <ol style="list-style-type: none"> Click OK to save changes. |
| Routing Options | |
| Router ID | Enter the ID of the routing device. |

Table 155: Fields on the Add an OSPF Page *(Continued)*

| Field | Action |
|--|---|
| Traffic Engineering NOTE: This option is not available for OSPFv3. | Enable this option 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 155: Fields on the Add an OSPF Page (Continued)

| Field | Action |
|------------|---|
| Area Range | <p>Displays a range of IP addresses for the summary link state advertisements (LSAs) to be sent within an area.</p> <p>Select an option:</p> <ol style="list-style-type: none"> 1. To add an area range form: <ol style="list-style-type: none"> a. Click +. <p>The Create Area Range Form page appears.</p> b. Enter the following details: <ul style="list-style-type: none"> • Area Range—Enter the area range address. <p>NOTE: For OSPF, enter an IPv4 address and for OSPFv3 enter an IPv6 address.</p> • Subnet mask—Enter the subnet mask area address. <p>NOTE: This option is available only for IPv4 address.</p> • Override metric—Select a value to override the metric for the IP address range. <p>Range: 1025 through 65534.</p> c. Select Restrict Advertisements of this area range to specify that the routes contained within a summary must not be displayed. d. 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. e. Click OK. 2. To edit the selected are range: <ol style="list-style-type: none"> a. Select the existing area range. b. Click the pencil icon to edit the selected area range. <p>The Edit Area Range Form page appears with editable fields.</p> |

Table 155: Fields on the Add an OSPF Page (Continued)

| Field | Action |
|---|--|
| | <p>c. Click OK to save the changes.</p> <p>3. To delete an area range:</p> <p>a. Select the area range that you want to delete.</p> <p>b. Click the delete icon.</p> <p>A confirmation message appears.</p> <p>c. Click Yes to delete the selected area range.</p> |
| Version | <p>Select the version of the OSPF:</p> <ul style="list-style-type: none"> • ospf—Enables OSPF routing on the routing device. • ospf3—Enables OSPFv3 routing on the routing device. |
| <p>Area Type</p> <p>NOTE: This option is not applicable for area zero.</p> | <p>Specifies the type of OSPF area.</p> <p>Select an option from the list:</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). |
| <p>No Summaries (Totally Stubby area)</p> <p>NOTE: This option is applicable for non-zero area and it is not applicable for area zero.</p> | <p>Enable or disable the summaries.</p> <p>NOTE: This option can be configured when area-type is nssa or stub.</p> |
| <p>Virtual Link</p> <p>NOTE: This option is applicable for area zero and it is not applicable for non-zero area.</p> | <p>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.</p> |

Table 155: Fields on the Add an OSPF Page (*Continued*)

| Field | Action |
|--------------------------|---|
| Interface Details | |
| Select Interface | Select one or more interfaces to associate with the routing instance from the Available column and move it to the Selected column using arrow. |
| Interface type | <p>Specifies the interfaces to be associated with the OSPF configuration.</p> <p>Select an option from the list:</p> <ul style="list-style-type: none"> • None—No interface. • nbma—Non broadcast multiaccess (NBMA) interface. NOTE: This option is not available for OSPFv3. • 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. |
| Interface Metric | Type the metric that you want for measuring the interface. |
| Passive mode | <p>Enable this option for the passive mode.</p> <p>NOTE: You can enable this option only if Secondary option is disabled and vice-versa.</p> |
| Advanced | |

Table 155: Fields on the Add an OSPF Page (Continued)

| Field | Action |
|---------------------------------|---|
| Bidirectional Forward Detection | <p>Enable this option for the bidirectional forward detection (BFD) protocol version that you want to detect.</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 | <p>Select a number of one of the security associations 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 | <p>Enable this option. Creates a backup loop-free alternate path to the primary next hop for all destination routes that traverse the protected interface.</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 | <p>Enable this option. Creates an alternate loop-free path to the primary next hop for all destination routes that traverse a protected interface.</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> |

Table 155: Fields on the Add an OSPF Page (*Continued*)

| Field | Action |
|---|--|
| Secondary | <p>Enable this option. Specifies an interface to belong to another OSPF area.</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 NOTE: This option is not available for OSPFv3. | <p>Select an authentication key (password) from the list:</p> <ul style="list-style-type: none"> • None • md5 • simplepassword |
| MD5 Authentication Key NOTE: This option is not available for OSPFv3. | <p>Specifies an MD5 authentication key (password).</p> <p>Click + and enter the following details:</p> <ul style="list-style-type: none"> • MD5 ID—MD5 key identifier. Range: 0 through 255. • Key—One or more MD5 key strings. <p>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 (" ").</p> <ul style="list-style-type: none"> • Start Time—MD5 start time. <p>Then, click tick mark to save the changes.</p> |
| Simple Password NOTE: This option is not available for OSPFv3. | <p>Enter a simple authentication key (password).</p> |
| Advanced Settings | |
| Policy | |
| NOTE: This option is not available for tenant users. | |

Table 155: Fields on the Add an OSPF Page (*Continued*)

| Field | 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.</p> <p>Click one of the following options:</p> <ul style="list-style-type: none"> • +—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. • X—Removes the import policy. |
| Export Policy | <p>Specifies one or more policies to control which summary LSAs are flooded into an area.</p> <p>Click one of the following options:</p> <ul style="list-style-type: none"> • +—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. • X—Removes the import policy. |
| Trace Options | |
| File Name | Enter the name of the file to receive the output of the trace operation. |
| Number of files | Enter the maximum number of trace files. |
| File Size | Enter the maximum size for each trace file. |
| World Readable | <p>Enable this option to allow any user to read the file.</p> <p>Disable this option to prevent all users from reading the file.</p> |

Table 155: Fields on the Add an OSPF Page *(Continued)*

| Field | Action |
|--------------|---|
| Flags | <p>Specifies the trace operation to be performed.</p> <p>Select one or more flags in the Available column and move them to the Selected column using the right arrow.</p> |

RELATED DOCUMENTATION

| [Edit an OSPF](#) | 547

Edit an OSPF

You are here: **Network** > **Routing** > **OSPF**.

To edit an OSPF routing:

1. Select an existing OSPF routing that you want to edit on the OSPF page.
2. Click the pencil icon available on the upper-right corner of the OSPF page.

The Create OSPF page appears with editable fields. For more information on the options, see "[Add an OSPF](#)" on page 538 .

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

| [Delete an OSPF](#) | 547

Delete an OSPF

You are here: **Network** > **Routing** > **OSPF**.

To delete an OSPF routing:

1. Select an existing OSPF routing that you want to delete on the OSPF page.

2. Click the delete icon available on the upper-right corner of the OSPF page.
A confirmation window appears.
3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

| [About the OSPF Page](#) | 536

BGP Routing

IN THIS CHAPTER

- [About the BGP Page | 549](#)
- [Add a BGP Group | 553](#)
- [Edit a BGP Group | 558](#)
- [Delete a BGP Group | 559](#)
- [Edit Global Information | 559](#)

About the BGP Page

IN THIS SECTION

- [Tasks You Can Perform | 549](#)
- [Field Descriptions | 550](#)

You are here: **Network** > **Routing** > **BGP**.

Use this page to configure BGP routing.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a routing instance. See ["Add a BGP Group" on page 553](#) .
- Edit a routing instance. See ["Edit a BGP Group" on page 558](#) .
- Delete a routing instance. See ["Delete a BGP Group" on page 559](#) .

- Disable group information. To do this, select an existing group information and click **Disable**.
- Edit global information. See ["Edit Global Information" on page 559](#) .
- Disable global information. To do this, select an existing global information and click **Disable**.

Field Descriptions

[Table 156 on page 550](#) describes the fields on the BGP page.

Table 156: Fields on the BGP Page

| Field | Description |
|--|--|
| 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. | Select routing instances from the list. Example: default or all routing instances. |
| 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. NOTE: If you log in as a tenant user, Routing Instance, Import Policy, and Export Policy are not displayed. |

Table 156: Fields on the BGP Page (Continued)

| Field | Description |
|---------------|---|
| Export Policy | <p>Displays the export policy selected.</p> <p>NOTE: If you log in as a tenant user, Routing Instance, Import Policy, and Export Policy are not displayed.</p> |

Global Information

The global information values corresponding to 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.

| | |
|------|--|
| Edit | <p>Edits the Global settings which lists the following fields. See "Edit Global Information" on page 559 .</p> |
|------|--|

Table 156: Fields on the BGP Page *(Continued)*

| Field | Description |
|-------|--|
| Name | <p>Displays the following names:</p> <ul style="list-style-type: none"> • 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. • 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. 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. NOTE: If you log in as a tenant user, Export Policy is not displayed. |

RELATED DOCUMENTATION

[Add a BGP Group](#) | 553

Add a BGP Group

You are here: **Network** > **Routing** > **BGP**.

To add a BGP Group:

1. Click **+** on the upper-right corner of the BGP Group page.
The Add a Group page appears.
2. Complete the configuration according to the guidelines provided in [Table 157 on page 553](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 157: Fields on the Add a Group Page

| Field | Action |
|--|---|
| General | |
| 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. | Select a routing instance from the list. |
| Group Name | Enter a new group name. |
| 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 | Enter the degree of preference value for an external route. The route with the highest local preference value is preferred. |

Table 157: Fields on the Add a Group Page (Continued)

| Field | Action |
|---------------------------|--|
| Cluster Id | <p>Enter the IPv6 or IPv4 address to be used as the cluster identifier.</p> <p>The cluster identifier is used by the route reflector cluster in an internal BGP group.</p> |
| Description | Enter the text description for the global, group, or neighbor configuration. |
| Damping | Select the check box to enable route flap damping. |
| Advertise Inactive Routes | Select the check box to enable advertising of inactive routes. |
| Advertise Peer AS Routes | Select the check box to advertising of peer AS routes. |
| Neighbors | |

Table 157: Fields on the Add a Group Page (Continued)

| Field | Action |
|-------------------|--|
| Dynamic Neighbors | <p>Configures a dynamic neighbor (peer).</p> <p>Select one of the following options:</p> <ol style="list-style-type: none"> 1. To add a dynamic neighbor: <ol style="list-style-type: none"> a. Click +. <p>The Add Dynamic Neighbor window appears.</p> b. Select one of the following options in the Addresses field: <ul style="list-style-type: none"> • All • IPv4 • IPv6 c. Enter the following details if you select IPv4 in the Addresses field: <ul style="list-style-type: none"> • IP Address—Enter the IPv4 address for dynamic neighbor. • Subnet Mask—Enter the subnet mask for the IPv4 address. d. Enter the following details if you select IPv6 in the Addresses field: <ul style="list-style-type: none"> • IPv6 Address—Enter the IPv6 address for dynamic neighbor. • Prefix—Enter the prefix length using up and down arrows for the IPv6 address. e. Click OK to save changes. 2. To edit a dynamic neighbor: <ol style="list-style-type: none"> a. Select the existing dynamic neighbor address. b. Click the pencil icon to edit the selected dynamic neighbor address. <p>The Edit Dynamic Neighbor window appears with editable fields.</p> c. Click OK to save changes. 3. To delete a dynamic neighbor: <ol style="list-style-type: none"> a. Select the existing dynamic neighbor address. b. Click the delete icon (X) to delete the selected dynamic neighbor address. |

Table 157: Fields on the Add a Group Page (Continued)

| Field | Action |
|------------------|---|
| Static Neighbors | <p>Configures a static neighbor (peer).</p> <p>Select one of the following options:</p> <ol style="list-style-type: none"> 1. To add a static neighbor: <ol style="list-style-type: none"> a. Click +. <p>The Add Static Neighbor window appears.</p> b. Enter the following details: <ul style="list-style-type: none"> • Addresses—Select IPv4 or IPv6. • IP Address—Enter the IPv4 address for static neighbor. • Local Address—Enter the IP address for static neighbor. • Preference—Enter the preference value for an external route. The route with the highest local preference value is preferred. • Description—Enter a description. • Hold Time—Enter the hold timeout interval period. • Out Delay—Enter the output delay time. <p>Range: 0 through 65,535 seconds.</p> • Passive—Select the check box to enable the device to be passive. The routing device will wait for the peer to issue an open request before a message is sent. • As Override—Select the check box to replace all occurrences of the peer AS number in the AS path with its own AS number before advertising the route to the peer. • Import Policy—Select one of the following options: <ul style="list-style-type: none"> • +—Adds an import policy. |

Table 157: Fields on the Add a Group Page *(Continued)*

| Field | Action |
|---------------------|--|
| | <ul style="list-style-type: none"> • Move up—Moves the selected policy up the list of policies. • Move down—Moves the selected policy down. • X—Removes an import policy. • Export Policy—Select one of the following options: <ul style="list-style-type: none"> • +—Adds an import policy. • Move up—Moves the selected policy up the list of policies. • Move down—Moves the selected policy down. • X—Removes an import policy. <p>c. Click OK to save changes.</p> <p>2. To edit a static neighbor:</p> <ol style="list-style-type: none"> a. Select the existing static neighbor address. b. Click the pencil icon to edit the selected static neighbor address. The Edit Static Neighbor window appears with editable fields. c. Click OK to save changes. <p>3. To delete a static neighbor:</p> <ol style="list-style-type: none"> a. Select the existing static neighbor address. b. Click the delete icon (X) to delete the selected static neighbor address. |
| Policies Tab | |

Table 157: Fields on the Add a Group Page (Continued)

| Field | Action |
|---------------|--|
| Import Policy | <p>Specifies one or more routing policies for routes being imported into the routing table from BGP.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> • +–—Adds an import policy. • Move up—Moves the selected policy up the list of policies. • Move down—Moves the selected policy down. • X—Removes an import policy. |
| Export Policy | <p>Specifies one or more policies to routes being exported from the routing table into BGP.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> • +–—Adds an import policy. • Move up—Moves the selected policy up the list of policies. • Move down—Moves the selected policy down. • X—Removes an import policy. |

RELATED DOCUMENTATION

[Edit a BGP Group](#) | 558

Edit a BGP Group

You are here: **Network** > **Routing** > **BGP**.

To edit a BGP group :

1. Select an existing BGP group that you want to edit on the BGP page.
2. Click the pencil icon available on the upper-right corner of the BGP page.

The Edit a Group page appears with editable fields. For more information on the fields, see ["Add a BGP Group" on page 553](#) .

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

| [Delete a BGP Group](#) | 559

Delete a BGP Group

You are here: **Network** > **Routing** > **BGP**.

To delete a BGP group:

1. Select an existing BGP group that you want to delete on the BGP page.
2. Click the delete icon available on the upper-right corner of the BGP page.
A confirmation window appears.
3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

| [Edit Global Information](#) | 559

Edit Global Information

You are here: **Network** > **Routing** > **BGP**.

To edit BGP global information:

1. Select an existing global information that you want to edit on the BGP page.
2. Click the pencil icon available on the upper-right corner of the Global Information table.
The Edit Global Settings page appears.
3. Complete the configuration according to the guidelines provided in [Table 158 on page 560](#) .
4. Click **OK** to save the changes.

Table 158: Fields on the Edit Global Settings Page

| Field | Action |
|----------------------|--|
| General | |
| Router ASN | Enter the router ASN value. |
| Router Identifier | Enter the router identification IP address. |
| BGP Status | Select an option from the list: Enable or Disable. |
| Preference | Enter the degree of preference value for an external route. The route with the highest local preference value is preferred. |
| Description | Enter the description. |
| Confederation Number | Enter the router confederation ASN value. |

Table 158: Fields on the Edit Global Settings Page (*Continued*)

| Field | Action |
|------------------------|---|
| Confederation Members | <p>Specifies the AS numbers for the confederation members.</p> <p>Select one of the following options:</p> <ol style="list-style-type: none"> 1. To add a member ASN: <ol style="list-style-type: none"> a. Click +. <p>The Confederation Members window appears.</p> b. Enter member ASN value in the Member ASN field. c. Click OK to save changes. 2. To edit a member ASN: <ol style="list-style-type: none"> a. Select an existing member ASN value and click the pencil icon. <p>The Confederation Members window appears.</p> b. Edit member ASN value in the Member ASN field. c. Click OK to save changes. 3. To delete a member ASN: <ol style="list-style-type: none"> a. Select an existing member ASN value. <p>The Confederation Members window appears.</p> b. Click the delete icon to delete the member ASN value. |
| Advance Options | |
| Keep Route | <p>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.</p> <p>Select All or None to configure keep routes.</p> |
| TCP MSS | <p>Enter the maximum segment size (MSS) for the TCP connection.</p> <p>Range: 1 through 4096.</p> |
| MTU Discovery | <p>Select the check box to enable MTU discovery.</p> |

Table 158: Fields on the Edit Global Settings Page (*Continued*)

| Field | Action |
|--------------------|--|
| Remove Private ASN | Select the check box to enable removal of private ASNs. |
| Graceful Restart | <p>Enter the following details:</p> <ul style="list-style-type: none"> Restart Time—Enter the period of time after which a restart is expected to be complete. Stale Routes Time—Enter the maximum time that stale routes are kept during restart. |
| Multihop | <p>Specifies the maximum time-to-live (TTL) value for the TTL in the IP header of BGP packets.</p> <p>Enter the following details:</p> <ul style="list-style-type: none"> Nexthop Change—Select the check box to allow unconnected third-party next hops. TTL—Enter a TTL value. |
| Authentication | <p>Enter the following details:</p> <ul style="list-style-type: none"> Authentication Algorithm—Select an option from the list: None, MD5, or SHA1. Authentication Key—Enter an MD5 authentication key (password). This option is available if you select MD5 as authentication algorithm. |

Policies Tab

NOTE: If you log in as a tenant user, Policy tab is not displayed.

Table 158: Fields on the Edit Global Settings Page (*Continued*)

| Field | Action |
|--------------------------|---|
| Import Policy | <p>Applies one or more policies to routes being imported into the local routing device from the neighbors.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> • +—Adds an import policy. • Move up—Moves the selected policy up the list of policies. • Move down—Moves the selected policy down. • X—Removes an import policy. |
| Export Policy | <p>Specifies one or more policies to control which summary LSAs are flooded into an area.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> • +—Adds an import policy. • Move up—Moves the selected policy up the list of policies. • Move down—Moves the selected policy down. • X—Removes an import policy. |
| Trace Options Tab | |
| File Name | Enter the name of the file to receive the output of the trace operation. |
| Number of Files | Enter the maximum number of trace files. |
| File Size | Enter the maximum size for each trace file. |

Table 158: Fields on the Edit Global Settings Page *(Continued)*

| Field | Action |
|----------------|--|
| World Readable | <p>Specifies whether the trace file can be read by any user.</p> <p>Select an option:</p> <ul style="list-style-type: none"> • True—Allows any user to read the file. • False—Prevents all users from reading. |
| Flags | <p>Select one or more flags from the Available Flags column and move it to the Configured Flags column using the arrow.</p> |

RELATED DOCUMENTATION

| [About the BGP Page](#) | 549

Routing Instances

IN THIS CHAPTER

- [About the Routing Instances Page | 565](#)
- [Add a Routing Instance | 567](#)
- [Edit a Routing Instance | 568](#)
- [Delete a Routing Instance | 569](#)

About the Routing Instances Page

IN THIS SECTION

- [Tasks You Can Perform | 565](#)
- [Field Descriptions | 566](#)

You are here: **Network** > **Routing** > **Routing Instances**.

Use this page to configure routing instances.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a routing instance. See ["Add a Routing Instance" on page 567](#) .
- Edit a routing instance. See ["Edit a Routing Instance" on page 568](#) .
- Delete a routing instance. See ["Delete a Routing Instance" on page 569](#) .

- Show or hide columns in the Routing Instance table. To do this, use the Show Hide Columns icon in the upper-right corner of the page and select the options you want to show or deselect to hide options on the page.
- Advance search for a routing instance. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

For an advanced search:

1. Enter the search string in the text box.

Based on your input, a list of items from the filter context menu appears.

2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.

3. Press Enter to display the search results in the grid.

Field Descriptions

[Table 159 on page 566](#) describes the fields on the Routing Instances page.

Table 159: Fields on the Routing Instances Page

| Field | Description |
|---------------------|--|
| 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. |

RELATED DOCUMENTATION

| [Add a Routing Instance](#) | 567

Add a Routing Instance

You are here: **Network** > **Routing** > **Routing Instances**.

To add a routing interface:

1. Click **+** available on the upper-right corner of the Routing Instances page.
The Create Routing Instance page appears.
2. Complete the configuration according to the guidelines provided in [Table 160 on page 567](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.
If you click **OK**, a new routing instance is added with the provided configuration.

Table 160: Fields on the Add Routing Instance

| Field | Description |
|-------------------------|---|
| General Settings | |
| Name | 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 | Enter a description for the routing instance. We recommend that you enter a maximum of 255 characters. |
| Instance Type | Select the type of routing instance from the 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. |

Table 160: Fields on the Add Routing Instance *(Continued)*

| Field | Description |
|------------|--|
| Interfaces | <p>Select interfaces from the Available column and move it to the Selected column using the arrow.</p> <ul style="list-style-type: none"> • Name—Displays the interface name. • Zone—Displays the zone name corresponding to the interface name. <p>This is used to validate that all the interfaces of the selected zone(s) must belong to the same routing instance.</p> |

RELATED DOCUMENTATION

[About the Routing Instances Page | 565](#)

[Edit a Routing Instance | 568](#)

Edit a Routing Instance

You are here: **Network** > **Routing** > **Routing Instances**.

To edit a routing instance:

1. Select a routing instance that you want to edit on the Routing Instances page.
2. Click the pencil icon available on the upper-right corner of the page.

The Edit Routing Instance page appears with editable fields. For more information on the fields, see ["Add a Routing Instance" on page 567](#).

NOTE: As the Instance Type field is not editable, you can delete the existing routing instance and create a new one with the required routing instance type.

3. Click **OK** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

[About the Routing Instances Page | 565](#)

Delete a Routing Instance

You are here: **Network** > **Routing** > **Routing Instances**.

To delete a routing instance:

1. Select one or more routing instance that you want to delete on the Routing Instances page.
2. Click the delete icon available on the upper-right corner of the page.
A confirmation window appears.
3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

[About the Routing Instances Page | 565](#)

[Add a Routing Instance | 567](#)

[Edit a Routing Instance | 568](#)

Routing—Policies

IN THIS CHAPTER

- [About the Policies Page | 570](#)
- [Global Options | 572](#)
- [Add a Policy | 573](#)
- [Clone a Policy | 585](#)
- [Edit a Policy | 585](#)
- [Delete a Policy | 585](#)
- [Test a Policy | 586](#)

About the Policies Page

IN THIS SECTION

- [Tasks You Can Perform | 570](#)
- [Field Descriptions | 571](#)

You are here: **Network** > **Routing** > **Policies**.

Use this page to configure policies.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create global options. See ["Global Options" on page 572](#) .
- Create a policy. See ["Add a Policy" on page 573](#) .

- Clone a policy. See ["Clone a Policy" on page 585](#) .
- Edit a policy. See ["Edit a Policy" on page 585](#) .
- Delete a policy. See ["Delete a Policy" on page 585](#) .
- Term Up—Moves a term up in a selected list policies configuration.
- Term Down—Moves a term down in a selected list policies configuration.
- Test a policy. See ["Test a Policy" on page 586](#) .

Field Descriptions

[Table 161 on page 571](#) describes the fields on the Policies page.

Table 161: Fields on the Policies Page

| Field | Description |
|----------------------------|---|
| Name | Displays the name of the policy. |
| From: Prefix | Displays the policy prefix. |
| From: Protocol | Displays the selected source protocol. |
| From: Interface or Address | Displays the selected source interface or IP address. |
| To: Protocol | Displays the source destination protocol. |
| To: Interface or Address | Displays the selected interface or address. |
| Action | Displays the selected action. |
| Move To | Displays if the action is to move to next policy or term. |

RELATED DOCUMENTATION

| [Global Options](#) | [572](#)

Global Options

You are here: **Network** > **Routing** > **Policies**.

To edit global options:

1. Select an existing configuration that you want to edit on the Global Options page.
2. Click the pencil icon available on the upper-right corner of the page.

The Edit Global Options page appears. You can modify any previous changes done. For more information on the options, see [Table 162 on page 572](#).

3. Click **OK** to save the changes.

Table 162: Fields on the Global Options Page

| Field | Action |
|------------------------|---|
| Add Prefix List | |
| Name | <p>Enter the name of the prefix list.</p> <p>Select an option from the list:</p> <ul style="list-style-type: none"> • Add—Adds the prefix list. • Edit—Edits the prefix list. • X—Removes the prefix list. |
| Members | |
| IP Address | <p>To add prefix list members:</p> <ol style="list-style-type: none"> 1. Click +. <p>The Add Prefix List Members page appears.</p> <ol style="list-style-type: none"> 2. Enter the following details: <ul style="list-style-type: none"> • IP Address—Enter the prefix list IP address. • Subnet Mask—Enter the subnet mask IP address 3. Click OK to save changes. <p>Click the pencil icon to edit the IP address. You can click X to delete the IP address.</p> |

Table 162: Fields on the Global Options Page (Continued)

| Field | Action |
|----------------------|--|
| As Path | |
| As Path | <p>Click + to add As path.</p> <p>As Path Name—Enter the name of the As path.</p> <p>Regular Expression—Enter the regular expression of the As path.</p> <p>Click the pencil icon to edit the As path. You can click X to delete the As path.</p> |
| BGP Community | |
| BGP Community | <p>Click + to add a BGP community.</p> <p>Name—Enter the BGP community name.</p> <p>Click the pencil icon to edit the As path. You can click X to delete the As path.</p> |
| Members | <p>Click + to add a BGP community member.</p> <p>Community ID—Enter the BGP community ID.</p> |

RELATED DOCUMENTATION

[Add a Policy](#) | 573

Add a Policy

You are here: **Network** > **Routing** > **Policies**.

To add a policy:

1. Click + > **New** on the upper-right corner of the Policies page.
The Add Policy page appears.
2. Complete the configuration according to the guidelines provided in [Table 163 on page 574](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

If you click **OK**, a new policy is added with the provided configuration.

Table 163: Fields on the Policy Page

| Field | Description |
|------------------|--|
| Policy Name | Enter the policy name. |
| Terms | Click one of the following: <ul style="list-style-type: none"> • +—Adds the term. • Edit—Edits the term. • X—Deletes the term, |
| Add Term | |
| Term Name | Enter the term name. |
| Source | |
| Family | Select a family protocol address from the list. |
| Routing Instance | Select a routing instance from the list. |
| RIB | Select a routing table from the list. |
| Preference | Enter a preference value for the route. |
| Metric | Enter the metric value. You can specify up to four metric values. |

Table 163: Fields on the Policy Page *(Continued)*

| Field | Description |
|-----------|---|
| Interface | <p>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> <p>Choose one of the following options:</p> <ol style="list-style-type: none"> 1. To add an interface <ol style="list-style-type: none"> a. Click + and select Interface. The Available Interfaces page appears. b. Select an interface from the list and click OK. The selected interface is added. 2. To add an IP address <ol style="list-style-type: none"> a. Click + and select Address. The Add IP Address page appears. b. Enter IP address from the list and click OK. The selected IP address is added. 3. To delete an interface or an IP address: <ol style="list-style-type: none"> a. Select an existing interface or address from Interfaces. b. Click X. The selected interface or IP address is deleted. |

Table 163: Fields on the Policy Page *(Continued)*

| Field | Description |
|-------------|---|
| Prefix List | <p>Specifies a named list of IP addresses. You can specify an exact match with incoming routes.</p> <p>Choose one of the following options:</p> <ol style="list-style-type: none"> 1. To add a prefix list: <ol style="list-style-type: none"> a. Click +. The Available Prefix List page appears. b. Select a prefix list from the list and click OK. The selected prefix list is added. 2. To delete a prefix list: <ol style="list-style-type: none"> a. Select an existing prefix list. b. Click X. The selected prefix list is deleted. |
| Protocol | <p>Specifies the name of the protocol from which the route was learned or to which the route is being advertised.</p> <p>Choose one of the following options:</p> <ol style="list-style-type: none"> 1. To add a protocol: <ol style="list-style-type: none"> a. Click +. The Available Protocols page appears. b. Select a protocol from the list and click OK. The selected protocol is added. 2. To delete a protocol: <ol style="list-style-type: none"> a. Select an existing protocol. b. Click X. The selected protocol is deleted. |

Table 163: Fields on the Policy Page *(Continued)*

| Field | Description |
|---------------------|---|
| Policy | <p>Specifies the name of a policy to evaluate as a subroutine.</p> <p>Choose one of the following options:</p> <ol style="list-style-type: none"> 1. To add a policy: <ol style="list-style-type: none"> a. Click +. The Available Policies page appears. b. Select a policy from the list and click OK. The selected policy is added. 2. To delete a policy: <ol style="list-style-type: none"> a. Select an existing policy. b. Click X. The selected policy is deleted. |
| More | <p>Click More for advanced configuration options for policies.</p> <p>The More Options page appears.</p> <p>Click OK to save changes after the configuration is complete.</p> |
| More Options | |
| OSPF Area ID | Enter the IP address for the area identifier. |
| BGP Origin | Select a value from the list to specify the origin of the AS path information. |
| Local Preference | Type a BGP local preference value. |

Table 163: Fields on the Policy Page *(Continued)*

| Field | Description |
|---------|---|
| AS Path | <p>Specifies the name of an AS path regular expression.</p> <p>Choose one of the following options:</p> <ol style="list-style-type: none"> 1. To add an As path: <ol style="list-style-type: none"> a. Click +. <p>The Available AS Paths page appears.</p> b. Select an As path from the list and click OK. <p>The selected As path is added.</p> 2. To delete an As path: <ol style="list-style-type: none"> a. Select an existing As path. b. Click X. <p>The selected As path is deleted.</p> |
| Route | <p>Enter the following details:</p> <ul style="list-style-type: none"> • External—Select the check box to enable external routing. • OSPF Type—Select an OSPF type from the list. |

Table 163: Fields on the Policy Page (*Continued*)

| Field | Description |
|--------------------|---|
| Community | <p>Specifies the name of one or more communities.</p> <p>Choose one of the following options:</p> <ol style="list-style-type: none"> 1. To add a community: <ol style="list-style-type: none"> a. Click +. <p>The Available Communities page appears.</p> b. Select a community from the list and click OK. <p>The selected community is added.</p> 2. To delete a community: <ol style="list-style-type: none"> a. Select an existing community. b. Click X. <p>The selected community is deleted.</p> |
| Destination | |
| Family | Select a value for address family protocol from the list. |
| Routing Instance | Select a routing instance from the list. |
| RIB | Select a name of a routing table from the list. |
| Preference | Type a preference value for the route. |
| Metric | Type a metric value. |

Table 163: Fields on the Policy Page *(Continued)*

| Field | Description |
|-----------|---|
| Interface | <p>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> <p>Choose one of the following options:</p> <ol style="list-style-type: none"> 1. To add an interface: <ol style="list-style-type: none"> a. Click + and select Interface. The Available Interfaces page appears. b. Select an interface from the list and click OK. The selected interface is added. 2. To add an IP address: <ol style="list-style-type: none"> a. Click + and select Address. The Add IP Address page appears. b. Enter IP address from the list and click OK. The selected IP address is added. 3. To delete an interface or an IP address: <ol style="list-style-type: none"> a. Select an existing interface or address from Interfaces. b. Click X. The selected interface or IP address is deleted. |

Table 163: Fields on the Policy Page (*Continued*)

| Field | Description |
|----------|---|
| Protocol | <p>Specifies the name of the protocol from which the route was learned or to which the route is being advertised.</p> <p>Choose one of the following options:</p> <ol style="list-style-type: none"> 1. To add a protocol: <ol style="list-style-type: none"> a. Click +. The Available Protocols page appears. b. Select a protocol from the list and click OK. The selected protocol is added. 2. To delete a protocol: <ol style="list-style-type: none"> a. Select an existing protocol. b. Click X. The selected protocol is deleted. |
| Policy | <p>Displays the name of the policy.</p> <p>Choose one of the following options:</p> <ol style="list-style-type: none"> 1. To add a policy: <ol style="list-style-type: none"> a. Click +. The Available Policies page appears. b. Select a policy from the list and click OK. The selected policy is added. 2. To delete a policy: <ol style="list-style-type: none"> a. Select an existing policy. b. Click X. The selected policy is deleted. |

Table 163: Fields on the Policy Page *(Continued)*

| Field | Description |
|-----------------|---|
| More | <p>Click More for advanced configuration options for policies.</p> <p>The More Options page appears.</p> <p>Click OK to save changes after the configuration is complete.</p> |
| Action | |
| Action | Select an action value from the list. |
| Default Action | <p>Select a value from the list.</p> <p>Specifies that any action that is intrinsic to the protocol is overridden. This action is also non terminating so that various policy terms can be evaluated before the policy is terminated.</p> |
| Next | <p>Select a value from the list.</p> <p>Specifies the default control action if a match occurs, and there are no further terms in the current routing policy.</p> |
| Priority | <p>Select a value from the list.</p> <p>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.</p> |
| BGP Origin | <p>Select a value from the list.</p> <p>Specifies the BGP origin attribute.</p> |
| AS Path Prepend | <p>Enter AS path prepend value.</p> <p>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 non confederation sequence.</p> |

Table 163: Fields on the Policy Page (*Continued*)

| Field | Description |
|-------------------------|--|
| AS Path Expand | <p>Enter the following details:</p> <ul style="list-style-type: none"> • Type—Select the type and type a value. <p>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 non confederation sequence. This option is typically used in non-IBGP export policies.</p> <ul style="list-style-type: none"> • Value—Enter the As path value. |
| Preference | <p>Enter the following details:</p> <ul style="list-style-type: none"> • Action—Select the preference action and type a value. • Value—Enter the preference value. |
| Local Preference | <p>Enter the following details:</p> <ul style="list-style-type: none"> • Action—Select the preference action and type a value. • Value—Enter the preference value. |
| Load Balance Per Packet | <p>Select the check box to enable this option.</p> <p>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.</p> |
| Tag | <p>Enter the following details:</p> <ul style="list-style-type: none"> • Action—Select the action and type a value. <p>Changes the metric (MED) value by the specified negative or positive offset. This action is useful only in an external BGP (EBGP) export policy.</p> <ul style="list-style-type: none"> • Value—Enter the tag value. |

Table 163: Fields on the Policy Page (*Continued*)

| Field | Description |
|------------------|---|
| Metric | <p>Enter the following details:</p> <ul style="list-style-type: none"> Action—Select the action and type a value. <p>Specifies the tag value. The tag action sets the 32-bit tag field in OSPF external link-state advertisement (LSA) packets.</p> <ul style="list-style-type: none"> Value—Enter the metric value. |
| Route | <p>Enter the following details:</p> <ul style="list-style-type: none"> External—Select the check box to enable this option. OSPF Type—Select an option from the list. |
| Class of Service | <p>Enter the following details:</p> <ul style="list-style-type: none"> Class—Select None from the list. <p>Specifies the class-of-service parameters to be applied to routes installed into the routing table.</p> <ul style="list-style-type: none"> Source Class—Enter the source class. <p>Specifies that the value entered here maintains the packet counts for a route passing through your network, based on the source address.</p> <ul style="list-style-type: none"> Destination Class—Enter the destination class. <p>Specifies the value entered here maintains packet counts for a route passing through your network, based on the destination address in the packet.</p> <ul style="list-style-type: none"> Forwarding Class—Enter the forwarding class. <p>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.</p> |

RELATED DOCUMENTATION

[Clone a Policy](#) | 585

Clone a Policy

You are here: **Network** > **Routing** > **Policies**.

To clone a policy:

1. Select a policy that you want to clone and select **Clone** from the More link.
The Clone Policy page appears with editable fields. For more information on the fields, see ["Add a Policy" on page 573](#) .
2. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

RELATED DOCUMENTATION

| [Edit a Policy | 585](#)

Edit a Policy

You are here: **Network** > **Routing** > **Policies**.

To edit a policy:

1. Select a policy that you want to edit on the Policies page.
2. Click the pencil icon available on the upper-right corner of the Policies page.
The Edit Policy page appears with editable fields. For more information on the options, see ["Add a Policy" on page 573](#) .
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

| [Delete a Policy | 585](#)

Delete a Policy

You are here: **Network** > **Routing** > **Policies**.

To delete a policy configuration:

1. Select one or more policies that you want to delete from the Policies page.
2. Click the delete icon available on the upper-right corner of the Policies page.
A confirmation window appears.
3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

[Test a Policy | 586](#)

Test a Policy

You are here: **Network** > **Routing** > **Policies**.

To test a policy:

1. Select a policy you want to test.
2. Click **Test Policy** at the upper-right corner of the Policies page.
The Test Policy page appears.
3. Click **Start** to test the policy.
You can click **Generate Report** to get the test reports.

RELATED DOCUMENTATION

[Add a Policy | 573](#)

[Edit a Policy | 585](#)

[Delete a Policy | 585](#)

Routing—Forwarding Mode

IN THIS CHAPTER

- [About the Forwarding Mode Page | 587](#)

About the Forwarding Mode Page

IN THIS SECTION

- [Field Descriptions | 587](#)

You are here: **Network** > **Routing** > **Forwarding Mode**.

Use this page to view the forwarding configuration details.

Field Descriptions

[Table 164 on page 588](#) describes the fields on the Forwarding Mode page.

Once the configuration is complete, click **Save** to save the changes or click **Cancel** to discard the changes.

Table 164: Fields on the Forwarding Mode Page

| Field | Description |
|---|---|
| Family IPv6 | <p>Supports IPv6 protocol traffic, including Routing Information Protocol for IPv6 (RIPng).</p> <p>Select an option from the list:</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> |
| Family ISO NOTE: This option is not available for SRX5000 line of devices. | <p>Supports IS-IS traffic.</p> <p>Select an option from the list:</p> <ul style="list-style-type: none"> • None • packet-based |
| Family MPLS NOTE: This option is not available for SRX5000 line of devices. | <p>Supports MPLS traffic.</p> <p>Select an option from the list:</p> <ul style="list-style-type: none"> • None • flow-based • packet-based |

CoS—Value Aliases

IN THIS CHAPTER

- [About the Value Aliases Page | 589](#)
- [Add a Code Point Alias | 590](#)
- [Edit a Code Point Alias | 591](#)
- [Delete a Code Point Alias | 592](#)

About the Value Aliases Page

IN THIS SECTION

- [Tasks You Can Perform | 589](#)
- [Field Descriptions | 590](#)

You are here: **Network** > **Class of Service(CoS)** > **Value Aliases**.

Use this page to view, add, and remove value aliases details.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a code point alias. See ["Add a Code Point Alias" on page 590](#) .
- Edit a code point alias. See ["Edit a Code Point Alias" on page 591](#) .
- Delete a code point alias. See ["Delete a Code Point Alias" on page 592](#) .

Field Descriptions

Table 165 on page 590 describes the fields on the Value Alias page.

Table 165: Fields on the Value Alias Page

| Field | Description |
|----------------|--|
| 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> |

RELATED DOCUMENTATION

| [Add a Code Point Alias](#) | 590

Add a Code Point Alias

You are here: **Network** > **Class of Service(CoS)** > **Value Aliases**.

To add a code point alias:

1. Click + available on the upper-right corner of the Value Aliases page.

The Add Code Point Alias page appears.

2. Complete the configuration according to the guidelines provided in [Table 166 on page 591](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 166: Fields on the Add Code Point Alias Page

| Field | Description |
|-----------------------|---|
| Code point name | Enter a name for the CoS point alias. |
| Code point type | Select a code point type from the list. |
| Code point value bits | Select a COS value for which an alias is defined. |

RELATED DOCUMENTATION

[Edit a Code Point Alias | 591](#)

Edit a Code Point Alias

You are here: **Network** > **Class of Service(CoS)** > **Value Aliases**.

To edit a code point alias:

1. Select a code point alias that you want to edit on the Value Aliases page.
2. Click the pencil icon available on the upper-right corner of the Value Aliases page.

The Code Point options appears with editable fields. For more information on the options, see "[Add a Code Point Alias](#)" on page 590.

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[Delete a Code Point Alias | 592](#)

Delete a Code Point Alias

You are here: **Network** > **Class of Service(CoS)** > **Value Aliases**.

To delete a code point alias:

1. Select a code point alias that you want to delete on the Value Aliases page.
2. Click the delete icon available on the upper-right corner of the Value Aliases page.
A confirmation window appears.
3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

| [About the Value Aliases Page](#) | 589

CoS—Forwarding Classes

IN THIS CHAPTER

- [About the Forwarding Classes Page | 593](#)
- [Add a Forwarding Class | 594](#)
- [Edit a Forwarding Class | 595](#)
- [Delete a Forwarding Class | 595](#)

About the Forwarding Classes Page

IN THIS SECTION

- [Tasks You Can Perform | 593](#)
- [Field Descriptions | 594](#)

You are here: **Network** > **Class of Service(CoS)** > **Forwarding Classes**.

Use this page to view, add, and delete Forwarding Classes.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a forwarding class. See "[Add a Forwarding Class](#)" on page 594 .
- Edit a forwarding class. See "[Edit a Forwarding Class](#)" on page 595 .
- Delete forwarding class. See "[Delete a Forwarding Class](#)" on page 595 .

Field Descriptions

Table 167 on page 594 describes the fields on the Forwarding Classes page.

Table 167: Fields on the Forwarding Classes Page

| Field | Description |
|-----------------------|--|
| Forwarding class name | Displays the forwarding class name assigned to the internal queue number. By default, four forwarding classes are assigned to queue numbers: 0 (best-effort), 1 (assured-forwarding), 5 (expedited-forwarding), and 7 (network-connect). |
| Queue number | Displays the internal queue numbers to which forwarding classes are assigned. 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. |
| Queue characteristics | Displays the queue characteristics, for example, video or voice. |

RELATED DOCUMENTATION

| [Add a Forwarding Class](#) | 594

Add a Forwarding Class

You are here: **Network** > **Class of Service(CoS)** > **Forwarding Classes**.

To add a forwarding class:

1. Click **+** available on the upper-right corner of the Forwarding Class page.
The Add Forwarding Class page appears.
2. Complete the configuration according to the guidelines provided in [Table 168 on page 595](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 168: Fields on the Add Forwarding Class page

| Field | Description |
|-----------------------|---|
| Queue number | Select the internal queue number to which a forwarding class is assigned. |
| Forwarding class name | Enter the forwarding class name assigned to the internal queue number. |

RELATED DOCUMENTATION

| [Edit a Forwarding Class](#) | 595

Edit a Forwarding Class

You are here: **Network** > **Class of Service(CoS)** > **Forwarding Classes**.

To edit a forwarding class:

1. Select an existing forwarding class that you want to edit on the Forwarding Classes page.
2. Click the pencil icon available on the upper-right corner of the Forwarding Classes page.
The Edit Forwarding Class options appears with editable fields. For more information on the options, see "[Add a Forwarding Class](#)" on page 594 for options available for editing.
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

| [Delete a Forwarding Class](#) | 595

Delete a Forwarding Class

You are here: **Network** > **Class of Service(CoS)** > **Forwarding Classes**.

To delete a forwarding class:

1. Select an existing forwarding class that you want to delete on the Forwarding Classes page.

2. Click the delete icon available on the upper-right corner of the Forwarding Classes page.
A confirmation window appears.
3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

| [About the Forwarding Classes Page](#) | 593

CoS Classifiers

IN THIS CHAPTER

- [About the Classifiers Page | 597](#)
- [Add a Classifier | 599](#)
- [Edit a Classifier | 600](#)
- [Delete a Classifier | 601](#)

About the Classifiers Page

IN THIS SECTION

- [Tasks You Can Perform | 597](#)
- [Field Descriptions | 598](#)

You are here: **Network** > **Class of Service(CoS)** > **Classifiers**.

Use this page to view, add, and delete Classifier Page configuration.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a classifier. See ["Add a Classifier" on page 599](#) .
- Edit a classifier. See ["Edit a Classifier" on page 600](#) .
- Delete classifier. See ["Delete a Classifier" on page 601](#) .

Field Descriptions

Table 169 on page 598 describes the fields on the Classifiers page.

Table 169: Fields on the Classifiers Page

| Field | Description |
|-------------------------------|---|
| Classifier name | Displays the name of a classifier. |
| Classifier type | <p>Displays the classifier type.</p> <p>The following type of classifiers are available:</p> <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). NOTE: This option is not available on SRX4000 lines of devices. • exp—MPLS experimental (EXP) bits classifier NOTE: This option is not available on SRX4000 lines of devices and SRX5000 lines of devices. • ieee-802.1—IEEE-802.1 classifier • ieee-802.1ad—IEEE-802.1ad classifier NOTE: This option is not available on SRX4000 lines of devices. • inet-precedence—IPv4 precedence classifier (default and compatibility) |
| 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. |

RELATED DOCUMENTATION

[Add a Classifier](#) | 599

Add a Classifier

You are here: **Network** > **Class of Service(CoS)** > **Classifiers**.

To add a classifier:

1. Click **+** available on the upper-right corner of the Classifiers page.
The Add Classifier page appears.
2. Complete the configuration according to the guidelines provided in [Table 170 on page 599](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 170: Fields on the Add Classifier Page

| Field | Description |
|-----------------|---|
| Classifier name | Enter the classifier name. |
| Classifier type | <p>Select a classifier type from the list.</p> <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). NOTE: This option is not available on SRX4000 lines of devices. • exp—MPLS experimental (EXP) bits classifier NOTE: This option is not available on SRX4000 lines of devices and SRX5000 lines of devices. • ieee-802.1—IEEE-802.1 classifier • ieee-802.1ad—IEEE-802.1ad classifier NOTE: This option is not available on SRX4000 lines of devices. • inet-precedence—IPv4 precedence classifier (default and compatibility) |

Table 170: Fields on the Add Classifier Page (Continued)

| Field | Description |
|--------------------|--|
| Code point mapping | <p>Specifies the code point mapping created.</p> <p>The available options are as follows:</p> <ul style="list-style-type: none"> • Add—Click + to add a code point mapping. • Edit—Click pencil icon to edit the selected code point mapping. • Delete—Deletes the code point mapping. |
| Code point | Select the CoS value in bits and the alias of a classifier from the list. |
| Forwarding class | Select the forwarding class for the specified CoS value and alias from the list. |
| Loss priority | Select the loss priority for the specified CoS value and alias from the list. |

RELATED DOCUMENTATION

| [Edit a Classifier](#) | 600

Edit a Classifier

You are here: **Network** > **Class of Service(CoS)** > **Classifiers**.

To edit a classifier:

1. Select an existing classifier configuration that you want to edit on the Classifiers page.
2. Click the pencil icon available on the upper-right corner of the Classifiers page.

The Edit Classifiers page appears with editable fields. For more information on the options, see "[Add a Classifier](#)" on page 599 .

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

| [Delete a Classifier](#) | 601

Delete a Classifier

You are here: **Network** > **Class of Service(CoS)** > **Classifiers**.

To delete a classifier:

1. Select a classifier that you want to delete on the Classifiers Page.
2. Click the delete icon available on the upper-right corner of the Classifiers page.
A confirmation window appears.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

| [About the Classifiers Page](#) | 597

CoS—Rewrite Rules

IN THIS CHAPTER

- [About the Rewrite Rules Page | 602](#)
- [Add a Rewrite Rule | 603](#)
- [Edit a Rewrite Rule | 605](#)
- [Delete a Rewrite Rule | 605](#)

About the Rewrite Rules Page

IN THIS SECTION

- [Tasks You Can Perform | 602](#)
- [Field Descriptions | 603](#)

You are here: **Network** > **Class of Service(CoS)** > **Rewrite Rules**.

Use this page to add, edit, or delete rewrite rule configurations.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a rewrite rule. See ["Add a Rewrite Rule" on page 603](#) .
- Edit a rewrite rule. See ["Edit a Rewrite Rule" on page 605](#) .
- Delete rewrite rule. See ["Delete a Rewrite Rule" on page 605](#) .

Field Descriptions

Table 171 on page 603 describes the fields on the Rewrite Rules page.

Table 171: Fields on the Rewrite Rules Page

| Field | Description |
|----------------------------|---|
| 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. |

RELATED DOCUMENTATION

[Add a Rewrite Rule](#) | 603

Add a Rewrite Rule

You are here: **Network** > **Class of Service(CoS)** > **Rewrite Rules**.

To add a rule configuration:

1. Click **+** available on the upper-right corner of the Forwarding Class page.
The Add Rewrite Rule page appears.
2. Complete the configuration according to the guidelines provided in [Table 172 on page 604](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 172: Fields on the Add Rewrite Rule Page

| Field | Action |
|----------------------------|---|
| Rewrite rule name | Enter the name of a defined rewrite rule. |
| Rewrite rule type | <p>Select a rewrite rule type from the list.</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. <p>NOTE: This option is not available on SRX4000 lines of devices and SRX5000 lines of devices.</p> <ul style="list-style-type: none"> • dscp-ipv6—Defines the Differentiated Services code point rewrite rule for IPv6. <p>NOTE: This option is not available on SRX4000 lines of devices.</p> <ul style="list-style-type: none"> • ieee-802.1ad—Defines the IEEE-802.1ad rewrite rule. <p>NOTE: This option is not available on SRX4000 lines of devices.</p> <ul style="list-style-type: none"> • frame-relay-de—Defines the frame relay discard eligible bit rewrite rule. <p>NOTE: This option is not available on SRX4000 lines of devices and SRX5000 lines of devices.</p> |
| Code point mapping | <p>Specifies the code point mapping created.</p> <p>Click one:</p> <ul style="list-style-type: none"> • Add—Click + to add a code point mapping. • Edit—Click pencil icon to edit the selected code point mapping. • Delete—Deletes the code point mapping. |
| Egress/Outgoing Code point | Select a CoS value and alias from the list. |

Table 172: Fields on the Add Rewrite Rule Page *(Continued)*

| Field | Action |
|------------------|--|
| Forwarding class | Select the forwarding class of the rewrite rule from the list. |
| Loss priority | Select the loss priority of the rewrite rule from the list. |

RELATED DOCUMENTATION

[Edit a Rewrite Rule](#) | 605

Edit a Rewrite Rule

You are here: **Network** > **Class of Service(CoS)** > **Rewrite Rules**.

To edit a rewrite rule:

1. Select an existing rule configuration you want to edit on the Rewrite Rules page.
2. Click the pencil icon available on the upper-right corner of the Rewrite Rules page.

The Edit Rewrite Rule page appears with editable fields. For more information on the options, see ["Add a Rewrite Rule" on page 603](#).

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[Delete a Rewrite Rule](#) | 605

Delete a Rewrite Rule

You are here: **Network** > **Class of Service(CoS)** > **Rewrite Rules**.

To delete a rewrite rule:

1. Select an existing rule configuration you want to delete on the Rewrite Rules page.

2. Click the delete icon available on the upper-right corner of the Rewrite Rules page.
A confirmation window appears.
3. Click **Yes** to delete or click **No** to retain the previous configuration.

RELATED DOCUMENTATION

| [About the Rewrite Rules Page](#) | 602

CoS—Schedulers

IN THIS CHAPTER

- [About the Schedulers Page | 607](#)
- [Add a Scheduler | 608](#)
- [Edit a Scheduler | 610](#)
- [Delete a Scheduler | 611](#)

About the Schedulers Page

IN THIS SECTION

- [Tasks You Can Perform | 607](#)
- [Field Descriptions | 608](#)

You are here: **Network** > **Class of Service(CoS)** > **Schedulers**.

Use this page to add, edit or delete configuration of schedulers and enable or disable global settings.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a scheduler. See "[Add a Scheduler](#)" on page 608 .
- Edit a scheduler. See "[Edit a Scheduler](#)" on page 610 .
- Delete scheduler. See "[Delete a Scheduler](#)" on page 611 .

Field Descriptions

Table 173 on page 608 describes the fields on the Schedulers page.

Table 173: Fields on the Schedulers Page

| Field | Description |
|----------------------------------|--|
| Schedulers Global Setting | |
| Enable Non Strict Priority | Applies non-strict priority policy to all the schedulers. |
| Schedulers Configuration | |
| 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. |

RELATED DOCUMENTATION

[Add a Scheduler](#) | 608

Add a Scheduler

You are here: **Network** > **Class of Service(CoS)** > **Schedulers**.

To add a scheduler:

1. Click + available on the upper-right corner of the Scheduler page.

The Add Scheduler page appears.

2. Complete the configuration according to the guidelines provided in [Table 174 on page 609](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 174: Fields on the Add Scheduler Page

| Field | Action |
|--------------------|---|
| Scheduler name | Enter the scheduler name. |
| Scheduler priority | <p>Select an option 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 | <p>Select an option 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 | <p>Enter the minimum bandwidth allocated to a queue.</p> <p>Select an option 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. |

Table 174: Fields on the Add Scheduler Page (Continued)

| Field | Action |
|---------------|--|
| Transmit rate | <p>Enter the transmission rate of a scheduler.</p> <p>Select an option 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. |

RELATED DOCUMENTATION

[Edit a Scheduler](#) | 610

Edit a Scheduler

You are here: **Network** > **Class of Service(CoS)** > **Schedulers**.

To edit a scheduler:

1. Select an existing scheduler that you want to edit on the Schedulers page.
2. Click the pencil icon available on the upper-right corner of the Schedulers page.
The Edit Scheduler appears with editable fields. For more information on the options, see "[Add a Scheduler](#)" on page 608 .
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[Delete a Scheduler](#) | 611

Delete a Scheduler

You are here: **Network** > **Class of Service(CoS)** > **Schedulers**.

To delete a scheduler:

1. Select an existing scheduler that you want to delete on the Schedulers page.
2. Click the delete icon available on the upper-right corner of the Schedulers page.
A confirmation window appears.
3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

[About the Schedulers Page](#) | 607

CoS—Scheduler Maps

IN THIS CHAPTER

- [About the Scheduler Maps Page | 612](#)
- [Add a Scheduler Map | 613](#)
- [Edit a Scheduler Map | 614](#)
- [Delete a Scheduler Map | 615](#)

About the Scheduler Maps Page

IN THIS SECTION

- [Tasks You Can Perform | 612](#)
- [Field Descriptions | 613](#)

You are here: **Network** > **Class of Service(CoS)** > **Scheduler Maps**.

Use this page to add, edit, or delete schedulers maps configurations.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a scheduler map. See "[Add a Scheduler Map](#)" on page 613 .
- Edit a scheduler map. See "[Edit a Scheduler Map](#)" on page 614 .
- Delete a scheduler map. See "[Delete a Scheduler Map](#)" on page 615 .

Field Descriptions

Table 175 on page 613 describes the fields on the Scheduler Maps page.

Table 175: Fields on the Scheduler Maps Page

| Field | Description |
|------------------------------|---|
| 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. |

RELATED DOCUMENTATION

[Add a Scheduler Map | 613](#)

Add a Scheduler Map

You are here: **Network** > **Class of Service(CoS)** > **Scheduler Maps**.

To add a scheduler map:

1. Click **+** available on the upper-right corner of the Scheduler Map page.
The Add Scheduler Map page appears.
2. Complete the configuration according to the guidelines provided in [Table 176 on page 614](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 176: Fields on the Add Scheduler Map Page

| Field | Action |
|----------------------|--|
| Scheduler map name | Enter a name for the scheduler map. |
| best-effort | Select an option from the list. Specifies no service profile. Loss priority is typically not carried in a CoS value. |
| expedited-forwarding | Select an option from the list. Specifies end-to-end service with low loss, low latency, low jitter, and assured bandwidth. |
| assured-forwarding | Select an option from the list. Specifies the group of defined values. |
| network-control | Select an option from the list. Specifies CoS packet forwarding class of high priority. |

RELATED DOCUMENTATION

| [Edit a Scheduler Map](#) | 614

Edit a Scheduler Map

You are here: **Network** > **Class of Service(CoS)** > **Scheduler Maps**.

To edit a scheduler map:

1. Select an existing scheduler map that you want to edit on the Schedulers page.
2. Click the pencil icon available on the upper-right corner of the Schedulers page.

The Edit Scheduler Map page appears with editable fields. For more information on the options, see ["Add a Scheduler Map" on page 613](#) .

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

| [Delete a Scheduler Map | 615](#)

Delete a Scheduler Map

You are here: **Network** > **Class of Service(CoS)** > **Scheduler Maps**.

To delete a scheduler map:

1. Select an existing scheduler map that you want to delete on the Schedulers page.
2. Click the delete icon available on the upper-right corner of the Schedulers page.
A confirmation window appears.
3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

| [About the Scheduler Maps Page | 612](#)

CoS—Drop Profile

IN THIS CHAPTER

- [About the Drop Profile Page | 616](#)
- [Add a Drop Profile | 617](#)
- [Edit a Drop Profile | 619](#)
- [Delete a Drop Profile | 619](#)

About the Drop Profile Page

IN THIS SECTION

- [Tasks You Can Perform | 616](#)
- [Field Descriptions | 617](#)

You are here: **Network** > **Class of Service(CoS)** > **Drop Profile**.

Use this page to configure drop profiles.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a drop profile. See ["Add a Drop Profile" on page 617](#) .
- Edit a drop profile. See ["Edit a Drop Profile" on page 619](#) .
- Delete a drop profile. See ["Delete a Drop Profile" on page 619](#) .

Field Descriptions

Table 177 on page 617 describes the fields on the Drop Profile page.

Table 177: Fields on the Drop Profile Page

| Field | Description |
|-------------------|--|
| 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. |

RELATED DOCUMENTATION

| [About the Drop Profile Page](#) | 616

Add a Drop Profile

You are here: **Network** > **Class of Service(CoS)** > **Drop Profile**.

To add a drop profile:

1. Click **+** available on the upper-right corner of the Drop Profile page.
The Add Drop Profile page appears.
2. Complete the configuration according to the guidelines provided in [Table 178 on page 617](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 178: Fields on the Add Drop Profile Page

| Field | Action |
|-------------------|----------------------------|
| Drop Profile Name | Enter a drop profile name. |

Table 178: Fields on the Add Drop Profile Page (Continued)

| Field | Action |
|--------------|---|
| Interpolated | Select the option to specify whether the value pairs are interpolated to produce a smooth profile. |
| Segmented | Select the option to specify whether the value pairs are represented by line fragments, which connect each data point on the graph to produce a segmented profile. |
| Data point | <p>To add a data point:</p> <ol style="list-style-type: none"> Click +. <p>The Add Data Point page appears.</p> <ol style="list-style-type: none"> Enter the following details: <ul style="list-style-type: none"> Fill Level—Enter a percentage value for queue buffer fullness for the X-coordinate. For example, 95. Drop Probability—Enter a percentage value for drop probability for the Y-coordinate. For example, 85. Click OK to save changes. <p>To edit a data point:</p> <ol style="list-style-type: none"> Select the existing data point and click the pencil icon. <p>The Edit Data Point page appears.</p> <ol style="list-style-type: none"> Enter a percentage value for Drop Probability. Click OK to save changes. <p>To delete a data point, select the existing data point and click the delete (X) icon. Then, click Yes to delete it.</p> |

RELATED DOCUMENTATION

[Edit a Drop Profile](#) | 619

Edit a Drop Profile

You are here: **Network** > **Class of Service(CoS)** > **Drop Profile**.

To edit a drop profile:

1. Select an existing drop profile that you want to edit on the Drop Profile page.
2. Click the pencil icon available on the upper-right corner of the Drop Profile page.

The Edit Drop Profile page appears with editable fields. For more information on the options, see ["Add a Drop Profile" on page 617](#) .

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

| [Delete a Drop Profile | 619](#)

Delete a Drop Profile

You are here: **Network** > **Class of Service(CoS)** > **Drop Profile**.

To delete a drop profile:

1. Select an existing drop profile that you want to delete on the Drop Profile page.
2. Click the delete icon available on the upper-right corner of the Drop Profile page.

A confirmation window appears.

3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

| [About the Drop Profile Page | 616](#)

CoS—Virtual Channel Groups

IN THIS CHAPTER

- [About the Virtual Channel Groups Page | 620](#)
- [Add a Virtual Channel | 621](#)
- [Edit a Virtual Channel | 622](#)
- [Delete a Virtual Channel | 623](#)

About the Virtual Channel Groups Page

IN THIS SECTION

- [Tasks You Can Perform | 620](#)
- [Field Descriptions | 621](#)

You are here: **Network** > **Class of Service(CoS)** > **Virtual Channel Groups**.

NOTE: This menu is not available for SRX4000 line of devices and SRX5000 line of devices.

Use this page to configure virtual channel group.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a virtual channel. See ["Add a Virtual Channel" on page 621](#) .
- Edit a virtual channel. See ["Edit a Virtual Channel" on page 622](#) .

- Delete a virtual channel. See "[Delete a Virtual Channel](#)" on page 623 .

Field Descriptions

[Table 179 on page 621](#) describes the fields on the Virtual Channel Groups page.

Table 179: Fields on the Virtual Channel Groups Page

| Field | Description |
|----------------------------|--|
| 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. |

RELATED DOCUMENTATION

| [Add a Virtual Channel](#) | 621

Add a Virtual Channel

You are here: **Network** > **Class of Service(CoS)** > **Virtual Channel Groups**.

NOTE: This menu is not available for SRX4000 line of devices and SRX5000 line of devices.

To add a virtual channel to the virtual channel group:

1. Click **Add** on the Virtual Channel page.
The Virtual Channel Information page appears.
2. Complete the configuration according to the guidelines provided in [Table 180 on page 622](#) .

3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 180: Fields on the Virtual Channel Information Page

| Field | Action |
|----------------------|--|
| Virtual Channel Name | Select a predefined name from the list or enter a new virtual channel name. |
| Scheduler Map | Select a scheduler map from the list. Specifies a predefined scheduler map to assign to a virtual channel. The scheduler maps associate schedulers with forwarding classes. |
| Shaping Rate | Enter the shaping rate for a virtual channel. 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: Select an option from the list: <ul style="list-style-type: none"> • Unconfigured—Select the option for no shaping rate. • Absolute Rate—Configures a shaping rate as an absolute number of bits per second. Range: 3200 through 320000000000. • Percent—Configures a shaping rate as a percentage. Range: 0 through 100. |

RELATED DOCUMENTATION

[Edit a Virtual Channel](#) | 622

Edit a Virtual Channel

You are here: **Network** > **Class of Service(CoS)** > **Virtual Channel Groups**.

NOTE: This menu is not available for SRX4000 line of devices and SRX5000 line of devices.

To edit a virtual channel in the virtual channel group:

1. Click on the existing virtual channel name that you want to edit on the Virtual Channel Groups page. The Virtual Channel Information page appears with editable fields. For more information on the options, see ["Add a Virtual Channel" on page 621](#) .
2. Click **OK** to save the changes.

RELATED DOCUMENTATION

| [Delete a Virtual Channel | 623](#)

Delete a Virtual Channel

You are here: [Network](#) > [Class of Service\(CoS\)](#) > [Virtual Channel Groups](#).

NOTE: This menu is not available for SRX4000 line of devices and SRX5000 line of devices.

To delete a virtual channel:

1. Select an existing virtual channel name that you want to delete on the Virtual Channel Groups page.
2. Click **Delete** on the Virtual Channel Groups page.

RELATED DOCUMENTATION

| [About the Virtual Channel Groups Page | 620](#)

CoS—Assign To Interface

IN THIS CHAPTER

- [About the Assign To Interface Page | 624](#)
- [Edit a Port | 626](#)
- [Add a Logical Interface | 626](#)
- [Edit a Logical Interface | 628](#)
- [Delete a Logical Interface | 629](#)

About the Assign To Interface Page

IN THIS SECTION

- [Tasks You Can Perform | 624](#)
- [Field Descriptions | 625](#)

You are here: **Network** > **Class of Service(CoS)** > **Assign To Interface**.

Use this page to add, edit, or delete interface configuration.

Tasks You Can Perform

You can perform the following tasks from this page:

- Edit a port. See ["Edit a Port" on page 626](#) .
- Add a Logical Interface. See ["Add a Logical Interface" on page 626](#) .
- Edit a Logical Interface. See ["Edit a Logical Interface" on page 628](#) .

- Delete Logical Interface. See ["Delete a Logical Interface" on page 629](#) .

Field Descriptions

[Table 181 on page 625](#) describes the fields on the Assign To Interface page.

Table 181: Fields on the Assign To Interface Page

| Field | Description |
|--------------------------------------|---|
| 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,dscpv6,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,dscpv6,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. |

RELATED DOCUMENTATION

[Edit a Port | 626](#)

Edit a Port

You are here: **Network** > **Class of Service(CoS)** > **Assign To Interface**.

To edit a port:

1. Select an existing port profile that you want to edit on the Assign To Interface page.
2. The Edit page appears with editable fields. For more information on the options, see [Table 182 on page 626](#).
3. Click **OK** to save the changes.

Table 182: Fields on the Edit Port Page

| Field | Action |
|--|--|
| Interface Name | Displays the selected interface name. |
| Associate system default scheduler map | Select Associate system default scheduler map . Specifies that you can associate the system default scheduler map with the selected interface. |
| Select the scheduler map | Select Select the scheduler map and select a value from the list. Specifies the scheduler map to the selected interface. |

RELATED DOCUMENTATION

[Add a Logical Interface](#) | 626

Add a Logical Interface

You are here: **Network** > **Class of Service(CoS)** > **Assign To Interface**.

To add a logical interface:

1. Click **+** available on the upper-right corner of the Logical Interface page.
The Add Logical Interface page appears.
2. Complete the configuration according to the guidelines provided in [Table 183 on page 627](#).

3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 183: Fields on the Add Logical Interface

| Field | Action |
|-----------------------|--|
| Unit | Enter a logical interface name. |
| Scheduler map | Select a scheduler map from the list. |
| Forwarding class | Select a forwarding class from the list. |
| Virtual channel group | Select a virtual channel group from the list. |
| Classifiers | |
| dscp | Select a classifier DSCP value from the list. Specifies the Differentiated Services Code Point of the classifier type assigned to a particular interface. |
| dscp v6 | Select a classifier DSCPv6 value from the list. Specifies the Differentiated Services Code Point version 6 of the classifier type assigned to a particular interface. |
| exp | Select an EXP classifier value from the list. Specifies the EXP classifier type assigned to a particular interface. |
| inet precedence | Select an IPv4 precedence classifier value from the list. Specifies the IPv4 precedence classifier type assigned to a particular interface. |
| Rewrite rules | |
| dscp | Select a rewrite rule DSCP value from the list. Specifies the Differentiated Services Code Point of the rewrite rule type assigned to a particular interface |

Table 183: Fields on the Add Logical Interface (Continued)

| Field | Action |
|-----------------|--|
| dscp v6 | Select a rewrite rule DSCPv6 value from the list. Specifies the Differentiated Services Code Point version 6 of the rewrite rule type assigned to a particular interface. |
| exp | Select an EXP rewrite rule value from the list. Specifies the EXP rewrite rule type assigned to a particular interface. |
| inet precedence | Select an IPv4 precedence rewrite rule value from the list. Specifies the IPv4 precedence rewrite rule type assigned to a particular interface. |

RELATED DOCUMENTATION

[Edit a Logical Interface](#) | 628

Edit a Logical Interface

You are here: **Network** > **Class of Service(CoS)** > **Assign To Interface**.

To edit a logical interface:

1. Select an existing logical interface that you want to edit on the Logical Interface page.
2. Click the pencil icon available on the upper-right corner of the Logical Interface page.

The Edit Logical Interface page appears with editable fields. For more information on the options, see "[Add a Logical Interface](#)" on page 626 .

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[Delete a Logical Interface](#) | 629

Delete a Logical Interface

You are here: **Network** > **Class of Service(CoS)** > **Assign To Interface**.

To delete a logical interface:

1. Select an existing logical interface that you want to delete on the Logical Interface page.
2. Click the delete icon available on the upper-right corner of the Logical Interface page.
A confirmation window appears.
3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

[About the Assign To Interface Page | 624](#)

Application QoS

IN THIS CHAPTER

- [About the Application QoS Page | 630](#)
- [Add an Application QoS Profile | 633](#)
- [Edit an Application QoS Profile | 635](#)
- [Clone an Application QoS Profile | 635](#)
- [Delete an Application QoS Profile | 636](#)
- [Add a Rate Limiter Profile | 636](#)
- [Edit a Rate Limiter Profile | 637](#)
- [Clone a Rate Limiter Profile | 638](#)
- [Delete a Rate Limiter Profile | 638](#)

About the Application QoS Page

IN THIS SECTION

- [Tasks You Can Perform | 631](#)
- [Field Descriptions | 632](#)

You are here: **Network** > **Application QoS**.

Application quality of service (AppQoS) provides the ability to prioritize and meter application traffic to provide better service to business-critical or high-priority application traffic.

The AppQoS feature expands the capability of Junos OS class of service (CoS) to include marking DSCP values based on Layer-7 application types, honoring application-based traffic through loss priority

settings, and controlling transfer rates on egress Physical Interface Cards (PICs) based on Layer-7 application types.

Use this page to add, edit, clone, and delete an AppQoS profile and a rate limiter profile.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add an AppQoS profile. See ["Add an Application QoS Profile" on page 633](#) .
- Edit an AppQoS profile. See ["Edit an Application QoS Profile" on page 635](#) .
- Clone an AppQoS profile. See ["Clone an Application QoS Profile" on page 635](#) .
- Delete AppQoS profile. See ["Delete an Application QoS Profile" on page 636](#) .
- Add a rate limiter profile. See ["Add a Rate Limiter Profile" on page 636](#) .
- Edit a rate limiter profile. See ["Edit a Rate Limiter Profile" on page 637](#) .
- Clone a rate limiter profile. See ["Clone a Rate Limiter Profile" on page 638](#) .
- Delete rate limiter profile. See ["Delete a Rate Limiter Profile" on page 638](#) .
- Show or hide columns in the AppQoS Profile or Rate Limiter Profile table. To do this, click Show Hide Columns icon in the upper-right corner of the page and select the columns you want to display or deselect to hide columns on the page.
- Advanced search for an AppQoS or rate limiter profile. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. An example filter condition is displayed in the search text box when you hover over the Search icon. When you start entering the search string, the icon indicates whether the filter string is valid or not.

For an advanced search:

1. Enter the search string in the text box.

Based on your input, a list of items from the filter context menu appears.

2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace to delete a character of the search string.

3. Press Enter to display the search results in the grid.

Field Descriptions

Table 184 on page 632 describes the fields on the Application QoS page.

Table 184: Fields on the Application QoS Page

| Field | Description |
|-----------------------------|--|
| AppQoS Profile | |
| Name | Displays the AppQoS profile name. |
| Traffic Direction | Displays whether the traffic direction is client-to-server and server-to-client. NOTE: If the same rate limiter profile is associated with client-to-server and server-to-client traffic, then Both status will be displayed. |
| Rate Limiter | Displays the rate limiter profile name. |
| Forwarding Class | Displays the forwarding class name. |
| Rate Limiter Profile | |
| Name | Displays the rate limiter profile name. |
| Maximum Bandwidth | Displays the maximum bandwidth (in Mbps) to be transmitted for the rate limiter. |
| Maximum Burst Size | Displays maximum burst size (in MB) to be transferred in a single burst or time-slice. |
| Associated AppQoS Profile | Displays the AppQoS profile name associated with the rate limiter profile. |

Add an Application QoS Profile

You are here: **Network** > **Application QoS**.

To add an AppQoS profile:

1. Click **+** available on the upper-right corner of the Application QoS page.
The Add AppQoS Profile page appears.
2. Complete the configuration according to the guidelines provided in [Table 185 on page 633](#) through [Table 186 on page 634](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 185: Fields on the Add AppQoS Profile Page

| Field | Action |
|--------------------------|---|
| Name | Enter a name for the AppQoS profile. The name must be a string beginning with a letter or underscore and consisting of letters, numbers, dashes and underscores, and length should be maximum 53 characters. |
| Rate Limiter | |
| Traffic Direction | |
| Client to Server | Select a rate limiter from the list to be associated with client-to-server traffic for this application. Click Add New to add a new rate limiter profile. For more information on creating a new rate limiter, see "Add a Rate Limiter Profile" on page 636 . |
| Server to Client | Select a rate limiter from the list to be associated with server-to-client traffic for this application. Click Add New to add a new rate limiter profile. For fields information, see "Add a Rate Limiter Profile" on page 636 . |

Table 185: Fields on the Add AppQoS Profile Page (Continued)

| Field | Action |
|----------------------|---|
| Action | <p>Select one of the following actions to configure the AppQoS rules:</p> <ul style="list-style-type: none"> • Drop—Drops out-of-profile packets. • Loss Priority High—Elevates the loss priority to maximum. <p>NOTE: This option is not supported for SRX4600 and SRX5000 line of devices.</p> |
| QoS Marking | |
| DSCP | Select an option from the list to mark Differentiated Services code point (DSCP) alias or bit map with matching applications to establish the output queue. |
| Forwarding Class | <p>Select an option from the list to mark the AppQoS class with matching applications.</p> <p>Click Add New to add a new forwarding class. For more information in adding a new forwarding class, see Table 186 on page 634 .</p> <p>NOTE: Add New is not supported for the logical systems and tenants. You can only select the predefined value.</p> |
| Packet Loss Priority | <p>Select an option from the list to mark loss priority with matching applications.</p> <p>Possible values are none, high, low, medium-high, and medium-low. A high loss priority means that there is an 80% chance of packet loss in congestion.</p> |
| Logs | Enable this option to log AppQoS events. |

Table 186: Fields on the Add Forwarding Class page

| Field | Action |
|--------------|--|
| Name | Enter a name for the forwarding class. |
| Queue Number | <p>Enter an output queue number to associate with the forwarding class.</p> <p>Range is 0 through 7.</p> |

Table 186: Fields on the Add Forwarding Class page (Continued)

| Field | Action |
|----------|---|
| Priority | Select the forwarding class queuing priority from the list. |

RELATED DOCUMENTATION

[About the Application QoS Page | 630](#)

[Edit an Application QoS Profile | 635](#)

[Clone an Application QoS Profile | 635](#)

[Delete an Application QoS Profile | 636](#)

Edit an Application QoS Profile

You are here: **Network** > **Application QoS**.

To edit an AppQoS profile:

1. Select an existing AppQoS profile that you want to edit on the Application QoS page.
2. Click the pencil icon available on the upper right-side of the page.

The Edit AppQoS Profile page appears with editable fields. For more information on editing the fields, see ["Add an Application QoS Profile" on page 633](#) .

3. Click **OK** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

[About the Application QoS Page | 630](#)

[Clone an Application QoS Profile | 635](#)

[Delete an Application QoS Profile | 636](#)

Clone an Application QoS Profile

You are here: **Network** > **Application QoS**.

To clone an AppQoS profile:

1. Select an existing AppQoS profile that you want to clone on the Application QoS page.
2. Click **More** > **Clone** available on the upper right-side of the page.

The Clone AppQoS Profile page appears with editable fields. For more information on editing the fields, see "[Add an Application QoS Profile](#)" on page 633 .

3. Click **OK** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

[About the Application QoS Page](#) | 630

[Edit an Application QoS Profile](#) | 635

[Delete an Application QoS Profile](#) | 636

Delete an Application QoS Profile

You are here: **Network** > **Application QoS**.

To delete AppQoS profile(s):

1. Select one or more AppQoS profiles that you want to delete on the Application QoS page.
2. Click the delete icon available on the upper-right corner of the page.
3. Click **Yes** to delete the selected AppQoS profiles or click **No** to retain the profiles.

RELATED DOCUMENTATION

[About the Application QoS Page](#) | 630

[Add an Application QoS Profile](#) | 633

[Edit an Application QoS Profile](#) | 635

[Clone an Application QoS Profile](#) | 635

Add a Rate Limiter Profile

You are here: **Network** > **Application QoS**.

To add a rate limiter profile:

1. Click **+** available on the upper-right corner of the Application QoS page.
The Add Rate Limiter Profile page appears.
2. Complete the configuration according to the guidelines provided in [Table 187 on page 637](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 187: Fields on the Add Rate Limiter Profile Page

| Field | Action |
|--------------------|---|
| Name | <p>Enter a name for the rate limiter profile. It is applied in AppQoS rules to share device resources based on quality-of-service requirements.</p> <p>Name must be a string beginning with a letter or underscore and consisting of letters, numbers, dashes and underscores and length should be maximum 63 characters.</p> |
| Maximum Bandwidth | <p>Enter the maximum bandwidth to be transmitted in Mbps, for this rate limiter. You can provision up to 10240 Mbps of bandwidth among multiple rate limiters to share the resource proportionally.</p> <p>Range is 64 kbps through 10240 Mbps.</p> |
| Maximum Burst Size | <p>Enter the maximum burst size (in MB) to be transferred in a single burst or time-slice. This limit ensures that a high-priority transmission does not keep a lower priority transmission from transmitting.</p> <p>Range is 1 byte through 1280 MB.</p> |

RELATED DOCUMENTATION

[About the Application QoS Page | 630](#)

[Edit a Rate Limiter Profile | 637](#)

[Clone a Rate Limiter Profile | 638](#)

[Delete a Rate Limiter Profile | 638](#)

Edit a Rate Limiter Profile

You are here: **Network** > **Application QoS**.

To edit a rate limiter profile:

1. Select an existing rate limiter profile that you want to edit on the Application QoS page.
2. Click the pencil icon available on the upper right-side of the page.
The Edit Rate Limiter Profile page appears with editable fields. For more information on editing the fields, see ["Add a Rate Limiter Profile" on page 636](#) .
3. Click **OK** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

[About the Application QoS Page | 630](#)

[Clone a Rate Limiter Profile | 638](#)

[Delete a Rate Limiter Profile | 638](#)

Clone a Rate Limiter Profile

You are here: **Network** > **Application QoS**.

To clone a rate limiter profile:

1. Select an existing rate limiter profile that you want to clone on the Application QoS page.
2. Click **More** > **Clone** available on the upper right-side of the page.
The Clone Rate Limiter Profile page appears with editable fields. For more information on editing the fields, see ["Add a Rate Limiter Profile" on page 636](#) .
3. Click **OK** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

[About the Application QoS Page | 630](#)

[Edit a Rate Limiter Profile | 637](#)

[Delete a Rate Limiter Profile | 638](#)

Delete a Rate Limiter Profile

You are here: **Network** > **Application QoS**.

To delete rate limiter profile(s):

1. Select one or more rate limiter profiles that you want to delete on the Application QoS page.
2. Click the delete icon available on the upper-right corner of the page.
3. Click **Yes** to delete rate limiter profiles or click **No** to retain the profiles.

RELATED DOCUMENTATION

[About the Application QoS Page | 630](#)

[Add a Rate Limiter Profile | 636](#)

[Edit a Rate Limiter Profile | 637](#)

[Clone a Rate Limiter Profile | 638](#)

IPsec VPN

IN THIS CHAPTER

- [About the IPsec VPN Page | 640](#)
- [IPsec VPN Global Settings | 643](#)
- [Create a Site-to-Site VPN | 647](#)
- [Create a Remote Access VPN—Juniper Secure Connect | 664](#)
- [Create a Remote Access VPN—NCP Exclusive Client | 687](#)
- [Edit an IPsec VPN | 700](#)
- [Delete an IPsec VPN | 701](#)

About the IPsec VPN Page

IN THIS SECTION

- [Tasks You Can Perform | 640](#)
- [Field Descriptions | 641](#)

You are here: **Network > VPN > IPsec VPN.**

A VPN is a private network that uses a public network to connect two or more remote sites. Instead of using dedicated connections between networks, VPNs use virtual connections routed (tunneled) through public networks. IPsec VPN is a protocol, consists of set of standards used to establish a VPN connection. Use this page to configure IPsec VPN.

Tasks You Can Perform

You can perform the following tasks from this page:

- Configure IPsec VPN global settings. See ["IPsec VPN Global Settings" on page 643](#) .
- Create a Site-to-Site VPN. See ["Create a Site-to-Site VPN" on page 647](#) .
- Create a remote access VPN. See ["Create a Remote Access VPN—Juniper Secure Connect" on page 664](#) and ["Create a Remote Access VPN—NCP Exclusive Client" on page 687](#) .
- Edit an IPsec VPN configuration. See ["Edit an IPsec VPN" on page 700](#) .
- Delete an IPsec VPN configuration. See ["Delete an IPsec VPN" on page 701](#) .
- Show or hide columns in the IPsec VPN table. To do this, click the Show Hide Columns icon in the upper-right corner of the page and select the columns you want to display or deselect to hide columns on the page.
- Advance search for an IPsec VPN. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. An example filter condition is displayed in the search text box when you hover over the Search icon. When you start entering the search string, the icon indicates whether the filter string is valid or not.

For an advanced search:

1. Enter the search string in the text box.

Based on your input, a list of items from the filter context menu appears.

2. Select a value from the list and choose a valid operator for your advanced search.

NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace to delete a character of the search string.

3. Press Enter to display the search results in the grid.

Field Descriptions

[Table 188 on page 641](#) describes the fields on the IPsec VPN page.

Table 188: Fields on the IPsec VPN Page

| Field | Description |
|-------|-------------------------------------|
| Name | Displays the name of the IPsec VPN. |

Table 188: Fields on the IPsec VPN Page *(Continued)*

| Field | Description |
|---------------------|--|
| IKE Status | Displays the Phase I Internet Key Exchange (IKE) status. |
| VPN Topology | <p>Displays the name of the VPN topology:</p> <ul style="list-style-type: none"> • Site to Site VPN—Connects two sites in an organization together and allows secure communications between the sites. • Remote Access VPN—Allows a user who is working at home or traveling to connect to the corporate office and its resources. This topology is sometimes referred to as an end-to-site tunnel. <p>The options available are Remote Access VPN (Juniper Secure Connect) and Remote Access VPN (NCP Exclusive Client).</p> <ul style="list-style-type: none"> • Other topologies which are displayed and you cannot add or edit are: <ul style="list-style-type: none"> • Dynamic VPN—The dynamic VPN feature simplifies remote access by enabling users to create IPsec VPN tunnels without having to manually configure settings on their PCs or laptops. This feature is supported on SRX300, SRX320, SRX340, SRX345, and SRX550HM devices. • Hub-and-spoke VPNs—Connects branch offices to the corporate office in an enterprise network. You can also use this topology to connect spokes together by sending traffic through the hub. • ADVPN Hub—Auto Discovery VPN (ADVPN) dynamically establishes VPN tunnels between spokes to avoid routing traffic through the Hub. • ADVPN Spoke—Allows the spokes to establish a shortcut tunnel between peers. |
| Dead Peer Detection | Displays if the dead peer detection (DPD) is enabled or disabled. |
| Routing Mode | Displays the name of the routing mode to send traffic to the IPsec VPN. |
| Connection Profile | <p>Displays the connection profile in the FQDN or FQDN/Realm format if configured. If not configured, the field displays as external-IP/VPN-Name.</p> <p>NOTE: Starting in Junos OS 23.1R1 Release, Remote Access column is renamed as Connection Profile.</p> |

RELATED DOCUMENTATION

[Create a Site-to-Site VPN | 647](#)

[Edit an IPsec VPN | 700](#)

[Delete an IPsec VPN | 701](#)

IPsec VPN Global Settings

IN THIS SECTION

- [Field Descriptions | 643](#)

You are here: **Network > VPN > IPsec VPN.**

Use this page to view or add the VPN global configuration details. Click **Global Settings** on the IPsec VPN page.

Field Descriptions

[Table 189 on page 643](#) describes the fields on the Global Settings page.

Table 189: Fields on the Global Settings Page

| Field | Description |
|--------------------------|---|
| General | |
| IKE - respond to bad-spi | Enable this option if you want the device to respond to IPsec packets with invalid IPsec Security Parameter Index (SPI) values. |
| Max responses | Enter a value from 1 through 30 to respond to invalid SPI values per gateway. The default is 5. This option is available when Response Bad SPI is selected. |
| IKE SNMP trap | Enable this option to control the sending of SNMP traps. |

Table 189: Fields on the Global Settings Page (Continued)

| Field | Description |
|---------------------------|---|
| Tunnel down | <p>Enable this option to generate traps for IPsec tunnel going down only when the associated peer IKE SA is up.</p> <p>NOTE: This option is available when IKE SNMP trap is selected.</p> |
| Peer down | <p>Enable this option to generate traps when peer goes down.</p> <p>NOTE: This option is available when IKE SNMP trap is selected.</p> |
| IPsec VPN monitor options | <p>Enable this option if you want the device to monitor VPN liveliness.</p> |
| Interval (seconds) | <p>Enter a value from 2 through 3600 seconds after which Internet Control Message Protocol (ICMP) requests are sent to the peer.</p> |
| Threshold | <p>Enter a value from 1 through 65,536 to specify the number of consecutive unsuccessful pings before the peer is declared unreachable.</p> |
| Remote Access VPN | |
| Default profile name | <p>Select a default profile name from the list.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • This option is available when at least one Juniper Secure Connect VPN is created. • Starting in Junos OS 23.1R1 Release, default profile is deprecated in J-Web. |
| SSL VPN tunnel tracking | <p>Enable this option to track Encapsulated Security Payload (ESP) tunnels.</p> |

Table 189: Fields on the Global Settings Page (Continued)

| Field | Description |
|------------------|---|
| SSL VPN profiles | <p>Lists the SSL VPN profiles.</p> <p>NOTE: This option displays associated IPsec VPNs when at least one Juniper Secure Connect VPN is created.</p> <p>To add a new SSL VPN profile:</p> <ol style="list-style-type: none"> 1. Click +. <ul style="list-style-type: none"> The Add SSL VPN Profile page appears. 2. Enter the following details: <ul style="list-style-type: none"> • Name—Enter the name for an SSL VPN profile. • Logging—Enable this option to log for SSL VPN. • SSL Termination Profile—Select an SSL termination profile from the list. <p>To add a new SSL termination profile:</p> <ol style="list-style-type: none"> a. Click Add. <ul style="list-style-type: none"> The Create SSL Termination Profile page appears. b. Enter the following details: <ul style="list-style-type: none"> • Name—Enter a name for the SSL termination profile. • Server Certificate—Select a server certificate from the list. <p>To add a certificate, click Add. For more information on adding a device certificate, see No Link Title.</p> <p>To import a certificate, click Import. For more information on importing a device certificate, see No Link Title.</p> <ul style="list-style-type: none"> • Click OK. c. Click OK. 3. Click OK. <p>To edit an SSL termination profile, select the profile you want to edit and click on the pencil icon.</p> |

Table 189: Fields on the Global Settings Page (Continued)

| Field | Description |
|--|---|
| | To delete an SSL termination profile, select the profile you want to delete and click on the delete icon. |
| Internal SA Encryption | |
| Algorithm | Select an encryption algorithm from the list. That is, 3DES-CBC or AES-128-CBC. |
| Key | Enter the encryption key. You must ensure that the manual encryption key is in ASCII text and 16 (for AES-128-CBC algorithm) or 24 (for 3DES-CBC algorithm) characters long; otherwise, the configuration will result in a commit failure. NOTE: Key field will be enabled only if you select an algorithm. |
| IKE HA link | Use this toggle to enable or disable HA link encryption IKE internal messages for HA devices. By default, IKE HA link is disabled. |
| IKE Package | |
| NOTE: | |
| <ul style="list-style-type: none"> • If the device is in chassis cluster mode, you must install junos-ike package on both primary node and secondary node. As J-Web server runs only on primary node, you can install junos-ike package only on primary node. Use the CLI to install junos-ike package on secondary node. • Junos-ike package is not supported for SRX300 Series Firewall. • For SRX1600 and SRX2300 Firewalls, junos-ike package is already installed. | |
| Install IKE package | Use this to install junos-ike package on your device. NOTE: You must reboot your device once the junos-ike package is installed on your device to avoid configuration mismatch error. |
| Uninstall IKE package | Use this to uninstall junos-ike package from your device. NOTE: You must reboot your device once the junos-ike package is uninstalled from your device to avoid configuration mismatch error. |

Table 189: Fields on the Global Settings Page (Continued)

| Field | Description |
|---------------|--|
| Reboot Device | <p>To reboot your device, do the following:</p> <ol style="list-style-type: none"> 1. Click the reboot device button. The Reboot Device window appears. 2. Select and set the reboot time. That is: <ul style="list-style-type: none"> • Now— Device reboots immediately • In— Set the Reboot Time (minutes). • At— Set the Reboot atto schedule the reboot at particular time. <p>NOTE: Restart your device to ensure proper operation of J-web.</p> 3. Click OK. |

RELATED DOCUMENTATION

[About the IPsec VPN Page | 640](#)

[Edit an IPsec VPN | 700](#)

[Delete an IPsec VPN | 701](#)

Create a Site-to-Site VPN

You are here: **Network** > **VPN** > **IPsec VPN**.

To create a site-to-site VPN:

1. Click **Create VPN** and select **Site to Site** on the upper-right corner of the IPsec VPN page.
The Create Site to Site VPN page appears.
2. Complete the configuration according to the guidelines provided in [Table 190 on page 648](#) through [Table 195 on page 658](#) .
The VPN connectivity will change from grey to blue line in the topology to show that the configuration is complete.
3. Click **Save** to save the changes.
If you want to discard your changes, click **Cancel**.

Table 190: Fields on the Create IPsec VPN Page

| Field | Action |
|--------------|--|
| Name | Enter a name for the VPN. |
| Description | Enter a description. This description will be used for the IKE and IPsec proposals and policies. During edit, the IPsec policy description will be displayed and updated. |
| Routing Mode | Select the routing mode to which this VPN will be associated: <ul style="list-style-type: none">• Traffic Selector (Auto Route Insertion)• Static Routing• Dynamic Routing – OSPF• Dynamic Routing – BGP For each topology, J-Web auto generates the relevant CLIs. Traffic Selector is the default mode. |

Table 190: Fields on the Create IPsec VPN Page (Continued)

| Field | Action |
|-----------------------|--|
| Authentication Method | <p>Select an authentication method from the list that the device uses to authenticate the source of Internet Key Exchange (IKE) messages:</p> <ul style="list-style-type: none"> • Certificate Based—Types of digital signatures, which are certificates that confirm the identity of the certificate holder. <p>The following are the authentication methods for a certificate based:</p> <ul style="list-style-type: none"> • rsa-signatures—Specifies that a public key algorithm, which supports encryption and digital signatures, is used. • dsa-signatures—Specifies that the Digital Signature Algorithm (DSA) is used. • ecdsa-signatures-256—Specifies that the Elliptic Curve DSA (ECDSA) using the 256-bit elliptic curve secp256r1, as specified in the Federal Information Processing Standard (FIPS) Digital Signature Standard (DSS) 186-3, is used. • ecdsa-signatures-384—Specifies that the ECDSA using the 384-bit elliptic curve secp384r1, as specified in the FIPS DSS 186-3, is used. • ecdsa-signatures-521—Specifies that the ECDSA using the 521-bit elliptic curve secp521r1 is used. <p>NOTE: ecdsa-signatures-521 supports only SRX5000 line of devices with SPC3 card and junos-ike package installed.</p> <ul style="list-style-type: none"> • Pre-shared Key (default method)—Specifies that a preshared key, which is a secret key shared between the two peers, is used during authentication to identify the peers to each other. The same key must be configured for each peer. This is the default method. |

Table 190: Fields on the Create IPsec VPN Page (Continued)

| Field | Action |
|-----------------------------|---|
| Auto-create Firewall Policy | <p>If you select Yes, a firewall policy is automatically between internal zone and tunnel interface zone with local protected networks as source address and remote protected networks as destination address.</p> <p>Another firewall policy will be created visa-versa.</p> <p>If you choose No, you don't have a firewall policy option. You need to manually create the required firewall policy to make this VPN work.</p> <p>NOTE: If you do not want to auto-create a firewall policy in the VPN workflow, then the protected network is hidden for dynamic routing in both local and remote gateway.</p> |
| Remote Gateway | <p>Displays the remote gateway icon in the topology. Click the icon to configure the remote gateway.</p> <p>The gateway identifies the remote peer with the IPsec VPN peers and defines the appropriate parameters for that IPsec VPN.</p> <p>For fields information, see Table 191 on page 651 .</p> |
| Local Gateway | <p>Displays the local gateway icon in the topology. Click the icon to configure the local gateway.</p> <p>For fields information, see Table 193 on page 653 .</p> |

Table 190: Fields on the Create IPsec VPN Page (Continued)

| Field | Action |
|------------------------|--|
| IKE and IPsec Settings | <p>Configure the custom IKE or IPsec proposal and the custom IPsec proposal with recommended algorithms or values.</p> <p>For fields information, see Table 195 on page 658 .</p> <p>NOTE:</p> <ul style="list-style-type: none"> • J-Web supports only one custom IKE proposal and does not support the predefined proposal-set. Upon edit and save, J-Web deletes the predefined proposal set if configured. • On the remote gateway of the VPN tunnel, you must configure the same custom proposal and policy. • Upon edit, J-Web shows the first custom IKE and IPsec proposal when more than one custom proposal is configured. |

Table 191: Fields on the Remote Gateway Page

| Field | Action |
|-----------------------|--|
| Gateway is behind NAT | If enabled, the configured external IP address (IPv4 or IPv6) is referred to as the NAT device IP address. |
| IKE Identity | Select an option from the list to configure remote identity. |
| Host name | Enter a remote host name. |
| IPv4 Address | Enter a remote IPv4 address. |
| IPv6 Address | Enter a remote IPv6 address. |

Table 191: Fields on the Remote Gateway Page (Continued)

| Field | Action |
|---------------------|---|
| Key ID | Enter a Key ID. |
| E-mail Address | Enter an e-mail address. |
| External IP Address | <p>Enter the peer IPv4 or IPv6 address. You can create one primary peer network with up to four backups.</p> <p>You must enter one IPv4 or IPv6 address or you can enter up to five IP addresses separated by comma.</p> |
| Protected Networks | <p>When you select a routing mode, lists all the global address(es).</p> <p>Select the addresses from the Available column and then click the right arrow to move it to the Selected column.</p> <p>When the routing mode is:</p> <ul style="list-style-type: none"> • Traffic Selector—The IP addresses will be used as remote IP in traffic selector configuration. • Static Routing: <ul style="list-style-type: none"> • Static route will be configured for the selected global address(es). • The tunnel interface (st0.x) of the local gateway will be used as the next-hop. • Dynamic Routing—Default value is any. You can also select specific global address(es). The selected value is configured as destination address in the firewall policy. |
| Add | <p>Click +.</p> <p>The Create Global Address page appears. See Table 192 on page 653 for fields information.</p> |

Table 192: Fields on the Create Global Address Page

| Field | Action |
|------------|--|
| Subnet | Enter the subnet for IPv4 or IPv6 address. |
| Identifier | Enter a name for the global address. |

Table 193: Fields on the Local Gateway Page

| Field | Action |
|-----------------------|--|
| Gateway is behind NAT | Enable this option when the local gateway is behind a NAT device. |
| IKE Identity | Select an option from the list to configure local identity. When Gateway is behind NAT is enabled, you can configure an IPv4 or IPv6 address to reference the NAT device. |
| Host name | Enter a host name. NOTE: This option is available only if Gateway is behind NAT is disabled. |
| IPv4 Address | Enter an IPv4 address. |
| IPv6 Address | Enter an IPv6 address. |
| Key ID | Enter a Key ID. NOTE: This option is available only if Gateway is behind NAT is disabled. |
| E-mail Address | Enter an E-mail address. NOTE: This option is available only if Gateway is behind NAT is disabled. |

Table 193: Fields on the Local Gateway Page (*Continued*)

| Field | Action |
|--------------------------|--|
| External Interface | <p>Select an outgoing interface from the list for IKE negotiations.</p> <p>The list contains all available IP addresses if more than one IP address is configured to the specified interface. The selected IP address will be configured as the local address under the IKE gateway.</p> |
| Tunnel Interface | <p>Select an interface from the list to bind it to the tunnel interface (route-based VPN).</p> <p>Click Add to add a new interface. The Create Tunnel Interface page appears. See Table 194 on page 657 .</p> |
| Router ID | <p>Enter the routing device's IP address.</p> <p>NOTE: This option is available if the routing mode is Dynamic Routing - OSPF or BGP.</p> |
| Area ID | <p>Enter an area ID within the range of 0 to 4,294,967,295, where the tunnel interfaces of this VPN need to be configured.</p> <p>NOTE: This option is available if the routing mode is Dynamic Routing - OSPF.</p> |
| Tunnel Interface Passive | <p>Enable this option to bypass traffic of the usual active IP checks.</p> <p>NOTE: This option is available if the routing mode is Dynamic Routing - OSPF.</p> |
| ASN | <p>Enter the routing device's AS number.</p> <p>Use a number assigned to you by the NIC. Range: 1 through 4,294,967,295 (232 - 1) in plain-number format for 4-byte AS numbers.</p> <p>NOTE: This option is available if the routing mode is Dynamic Routing - BGP.</p> |

Table 193: Fields on the Local Gateway Page (*Continued*)

| Field | Action |
|-----------------|---|
| Neighbor ID | <p>Enter IP address of a neighboring router.</p> <p>NOTE: This option is available if the routing mode is Dynamic Routing - BGP.</p> |
| BGP Group Type | <p>Select the type of BGP peer group from the list:</p> <ul style="list-style-type: none"> • external—External group, which allows inter-AS BGP routing. • internal—Internal group, which allows intra-AS BGP routing. <p>NOTE: This option is available if the routing mode is Dynamic Routing - BGP.</p> |
| Peer ASN | <p>Enter the neighbor (peer) autonomous system (AS) number.</p> <p>NOTE: This option is available if you choose external as BGP Group Type.</p> |
| Import Policies | <p>Select one or more routing policies from the list to routes being imported into the routing table from BGP.</p> <p>Click Clear All to clear the selected polices.</p> <p>NOTE: This option is available if the routing mode is Dynamic Routing - BGP.</p> |
| Export Policies | <p>Select one or more policies from the list to routes being exported from the routing table into BGP.</p> <p>Click Clear All to clear the selected polices.</p> <p>NOTE: This option is available if the routing mode is Dynamic Routing - BGP.</p> |

Table 193: Fields on the Local Gateway Page (*Continued*)

| Field | Action |
|----------------------------------|--|
| Local certificate | <p>Select a local certificate identifier when the local device has multiple loaded certificates.</p> <p>NOTE: This option is available if the authentication method is Certificate Based.</p> <p>Click Add to generate a new certificate. Click Import to import a device certificate. For more information see Manage Device Certificates.</p> |
| Trusted CA/Group | <p>Select the certificate authority (CA) profile from list to associate it with the local certificate.</p> <p>NOTE: This option is available if the authentication method is Certificate Based.</p> <p>Click Add to add a new CA profile. For more information see Manage Trusted Certificate Authority.</p> |
| Pre-shared Key | <p>Enter the value of the preshared key. The key can be one of the following:</p> <ul style="list-style-type: none"> • <code>ascii-text</code>—ASCII text key. • <code>hexadecimal</code>—Hexadecimal key. <p>NOTE: This option is available if the authentication method is Pre-shared Key.</p> |
| Protected Networks | Click + . The Create Protected Networks page appears. |
| Create Protected Networks | |
| Zone | Select a security zone from the list that will be used as a source zone in the firewall policy. |
| Global Address | Select the addresses from the Available column and then click the right arrow to move it to the Selected column. |

Table 193: Fields on the Local Gateway Page (Continued)

| Field | Action |
|--------|--|
| Add | <p>Click Add.</p> <p>The Create Global Address page appears. See Table 192 on page 653.</p> |
| Edit | <p>Select the protected network you want to edit and click on the pencil icon.</p> <p>The Edit Global Address page appears with editable fields.</p> |
| Delete | <p>Select the protected network you want to edit and click on the delete icon.</p> <p>The confirmation message pops up.</p> <p>Click Yes to delete.</p> |

Table 194: Fields on the Create Tunnel Interface Page

| Field | Action |
|------------------|---|
| Interface Unit | Enter the logical unit number. |
| Description | Enter a description for the logical interface. |
| Zone | <p>Select a zone for the logical interface from the list to use as a source zone in the firewall policy.</p> <p>Click Add to add a new zone. Enter zone name and description and click OK on the Create Security Zone page.</p> |
| Routing Instance | Select a routing instance from the list. |

IPv4

NOTE: This option is available only if you select routing mode as Dynamic Routing - OSPF or BGP.

Table 194: Fields on the Create Tunnel Interface Page (Continued)

| Field | Action |
|---|--|
| IPv4 Address | Enter a valid IPv4 address. |
| Subnet Prefix | Enter a subnet mask for the IPv4 address. |
| IPv6 | |
| NOTE: This option is available only if you select routing mode as Dynamic Routing - OSPF or BGP. | |
| IPv6 Address | Enter a valid IPv6 address. |
| Subnet Prefix | Enter a subnet mask for the network range. Once entered, the value is validated. |

Table 195: IKE and IPsec Settings

| Field | Action |
|----------------------|---|
| IKE Settings | |
| IKE Version | Select the required IKE version, either v1 or v2 to negotiate dynamic security associations (SAs) for IPsec. Default value is v2. |
| IKE Mode | Select the IKE policy mode from the list: <ul style="list-style-type: none"> aggressive—Take half the number of messages of main mode, has less negotiation power, and does not provide identity protection. main—Use six messages, in three peer-to-peer exchanges, to establish the IKE SA. These three steps include the IKE SA negotiation, a Diffie-Hellman exchange, and authentication of the peer. Also provides identity protection. |
| Encryption Algorithm | Select the appropriate encryption mechanism from the list. Default value is aes-256-gcm. |

Table 195: IKE and IPsec Settings (Continued)

| Field | Action |
|--------------------------|---|
| Authentication Algorithm | <p>Select the authentication algorithm from the list. For example, hmac-md5-96—Produces a 128-bit digest and hmac-sha1-96—Produces a 160-bit digest.</p> <p>NOTE: This option is available when the encryption algorithm is not gcm.</p> <p>NOTE: Starting in Junos OS 23.4R1 Release, J-Web supports SHA 512-bit authentication algorithm for junos-ike package installed devices.</p> |
| DH group | <p>A Diffie-Hellman (DH) exchange allows participants to generate a shared secret value. Select the appropriate DH group from the list. Default value is group19.</p> <p>NOTE: Starting in Junos OS 23.4R1 Release, J-Web supports group 15, group 16, and group 21 DH groups for junos-ike package installed devices.</p> |
| Lifetime Seconds | <p>Select a lifetime of an IKE security association (SA). Default: 28,800 seconds. Range: 180 through 86,400 seconds.</p> |
| Dead Peer Detection | <p>Enable this option to send dead peer detection requests regardless of whether there is outgoing IPsec traffic to the peer.</p> |
| DPD Mode | <p>Select one of the options from the list:</p> <ul style="list-style-type: none"> • optimized—Send probes only when there is outgoing traffic and no incoming data traffic - RFC3706 (default mode). • probe-idle-tunnel—Send probes same as in optimized mode and also when there is no outgoing and incoming data traffic. • always-send—Send probes periodically regardless of incoming and outgoing data traffic. |
| DPD Interval | <p>Select an interval in seconds to send dead peer detection messages. The default interval is 10 seconds. Range is 2 to 60 seconds.</p> |
| DPD Threshold | <p>Select a number from 1 to 5 to set the failure DPD threshold.</p> <p>This specifies the maximum number of times the DPD messages must be sent when there is no response from the peer. The default number of transmissions is 5 times.</p> |

Table 195: IKE and IPsec Settings *(Continued)*

| Field | Action |
|---|--|
| Advance Configuration (Optional) | |
| General IKE ID | Enable this option to accept peer IKE ID. |
| IKEv2 Re-authentication | Configure the reauthentication frequency to trigger a new IKEv2 reauthentication. |
| IKEv2 Re-fragmentation | This option is enabled by default. |
| IKEv2 Re-fragment Size | Select the maximum size, in bytes, of an IKEv2 message before it is split into fragments. The size applies to both IPv4 and IPv6 messages. Range: 570 to 1320 bytes. Default values are: <ul style="list-style-type: none"> • IPv4 messages—576 bytes. • IPv6 messages—1280 bytes. |
| NAT-T | Enable this option for IPsec traffic to pass through a NAT device. NAT-T is an IKE phase 1 algorithm that is used when trying to establish a VPN connection between two gateway devices, where there is a NAT device in front of one of the SRX Series Firewalls. |
| NAT Keep Alive | Select appropriate keepalive interval in seconds. Range: 1 to 300. If the VPN is expected to have large periods of inactivity, you can configure keepalive values to generate artificial traffic to keep the session active on the NAT devices. |
| IPsec Settings | |
| Protocol | Select either Encapsulation Security Protocol (ESP) or Authentication Header (AH) protocol from the list to establish VPN. Default value is ESP. |

Table 195: IKE and IPsec Settings (*Continued*)

| Field | Action |
|-------------------------------|---|
| Encryption Algorithm | Select the encryption method. Default value is aes-256-gcm. NOTE: This option is available only for the ESP protocol. |
| Authentication Algorithm | Select the IPsec authentication algorithm from the list. For example, hmac-md5-96—Produces a 128-bit digest and hmac-sha1-96—Produces a 160-bit digest. NOTE: This option is available when the encryption algorithm is not gcm. NOTE: Starting in Junos OS 23.4R1 Release, J-Web supports HMAC-SHA 384 and HMAC-SHA 512 authentication algorithm for junos-ike package installed devices. |
| Perfect Forward Secrecy | Select Perfect Forward Secrecy (PFS) from the list. The device uses this method to generate the encryption key. Default value is group19. PFS generates each new encryption key independently from the previous key. The higher numbered groups provide more security, but require more processing time. NOTE: group15, group16, and group21 support only the SRX5000 line of devices with an SPC3 card and junos-ike package installed. NOTE: Starting in Junos OS 23.4R1 Release, J-Web supports group 15, group 16, and group 21 PFS for junos-ike package installed devices. |
| Lifetime Seconds | Select the lifetime (in seconds) of an IPsec security association (SA). When the SA expires, it is replaced by a new SA and security parameter index (SPI) or terminated. Default is 3,600 seconds. Range: 180 through 86,400 seconds. |
| Lifetime Kilobytes | Select the lifetime (in kilobytes) of an IPsec SA. Default is 128kb. Range: 64 through 4294967294. |
| Establish Tunnel | Enable this option to establish the IPsec tunnel. IKE is activated immediately (default value) after a VPN is configured and the configuration changes are committed. |
| Advanced Configuration | |
| VPN Monitor | Enable this option to use it in a destination IP address. NOTE: This option is not available for Traffic Selectors routing mode. |

Table 195: IKE and IPsec Settings (Continued)

| Field | Action |
|------------------|---|
| Destination IP | <p>Enter the destination of the Internet Control Message Protocol (ICMP) pings. The device uses the peer's gateway address by default.</p> <p>NOTE: This option is not available for Traffic Selectors routing mode.</p> |
| Optimized | <p>Enable this option for the VPN object. If enabled, the SRX Series Firewall only sends ICMP echo requests (pings) when there is outgoing traffic and no incoming traffic from the configured peer through the VPN tunnel. If there is incoming traffic through the VPN tunnel, the SRX Series Firewall considers the tunnel to be active and does not send pings to the peer.</p> <p>This option is disabled by default.</p> <p>NOTE: This option is not available for Traffic Selectors routing mode.</p> |
| Source Interface | <p>Select the source interface for ICMP requests from the list. If no source interface is specified, the device automatically uses the local tunnel endpoint interface.</p> <p>NOTE: This option is not available for Traffic Selectors routing mode.</p> |
| Verify-path | <p>Enable this option to verify the IPsec datapath before the secure tunnel (st0) interface is activated and route(s) associated with the interface are installed in the Junos OS forwarding table.</p> <p>This option is disabled by default.</p> <p>NOTE: This option is not available for Traffic Selectors routing mode.</p> |
| Destination IP | <p>Enter the destination IP address. Original, untranslated IP address of the peer tunnel endpoint that is behind a NAT device. This IP address must not be the NAT translated IP address. This option is required if the peer tunnel endpoint is behind a NAT device. The verify-path ICMP request is sent to this IP address so that the peer can generate an ICMP response.</p> <p>NOTE: This option is not available for Traffic Selectors routing mode.</p> |
| Packet size | <p>Enter the size of the packet that is used to verify an IPsec datapath before the st0 interface is brought up. Range: 64 to 1350 bytes. Default value is 64 bytes.</p> <p>NOTE: This option is not available for Traffic Selectors routing mode.</p> |

Table 195: IKE and IPsec Settings (*Continued*)

| Field | Action |
|-------------------------|---|
| Anti Replay | <p>IPsec protects against VPN attack by using a sequence of numbers built into the IPsec packet—the system does not accept a packet with the same sequence number.</p> <p>This option is enabled by default. The Anti-Replay checks the sequence numbers and enforce the check, rather than just ignoring the sequence numbers.</p> <p>Disable Anti-Replay if there is an error with the IPsec mechanism that results in out-of-order packets, which prevents proper functionality.</p> |
| Install Interval | <p>Select the maximum number of seconds to allow for the installation of a rekeyed outbound security association (SA) on the device. Select a value from 1 to 10.</p> |
| Idle Time | <p>Select the idle time interval. The sessions and their corresponding translations time out after a certain period of time if no traffic is received. Range is 60 to 999999 seconds.</p> |
| DF Bit | <p>Select how the device handles the Don't Fragment (DF) bit in the outer header:</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. |
| Copy Outer DSCP | <p>This option enabled by default. This enables copying of Differentiated Services Code Point (DSCP) (outer DSCP+ECN) from the outer IP header encrypted packet to the inner IP header plain text message on the decryption path. Enabling this feature, after IPsec decryption, clear text packets can follow the inner CoS (DSCP+ECN) rules.</p> |
| ICMP big packet warning | <p>Use this option to enable or disable sending ICMP packet too big notifications for IPv6 packets.</p> <p>NOTE: This option is available only for junos-ike package installed devices.</p> |
| ESN | <p>Enable this to allow IPsec to use 64-bit sequence number. If ESN is not enabled, 32-bit sequence number will be used by default. Ensure ESN is not enabled when anti-replay is disabled.</p> <p>NOTE: This option is available only for junos-ike package installed devices.</p> |

Table 195: IKE and IPsec Settings (Continued)

| Field | Action |
|------------|---|
| Tunnel MTU | <p>Enter the maximum transmit packet size for IPsec tunnels.</p> <p>Range: 256 through 9192.</p> <p>NOTE: This option is available only for junos-ike package installed devices.</p> |

RELATED DOCUMENTATION

[About the IPsec VPN Page | 640](#)

[IPsec VPN Global Settings | 643](#)

[Edit an IPsec VPN | 700](#)

[Delete an IPsec VPN | 701](#)

Create a Remote Access VPN—Juniper Secure Connect

You are here: **Network > VPN > IPsec VPN.**

Juniper Secure Connect is Juniper's client-based SSL-VPN solution that offers secure connectivity for your network resources.

Juniper Secure Connect provides secure remote access for the users to connect to the corporate networks and resources remotely using the Internet. Juniper Secure Connect downloads the configuration from SRX Services devices and chooses the most effective transport protocols during connection establishment to deliver a great administrator and user experience.

To create a remote access VPN for Juniper secure connect:

1. Choose **Create VPN > Remote Access > Juniper Secure Connect** on the upper right-side of the IPsec VPN page.

The Create Remote Access (Juniper Secure Connect) page appears.

NOTE: Starting in Junos OS Release 23.2R1, when you create or edit the Juniper Secure Connect VPNs, the ike-user-type is group-ike-id if the Junos-ike package is already installed.

This helps to enable you with the multi device access. This is not supported for SRX300 line of Firewalls and SRX550HM Firewall.

2. Complete the configuration according to the guidelines provided in [Table 196 on page 665](#) through [Table 201 on page 682](#).

The VPN connectivity will change from grey to blue line in the topology to show that the configuration is complete.

3. Click **Save** to complete Secure Connect VPN Configuration and associated policy if you have selected the auto policy creation option.

If you want to discard your changes, click **Cancel**.

Table 196: Fields on the Create Remote Access (Juniper Secure Connect) Page

| Field | Action |
|--------------|--|
| Name | Enter a name for the remote access connection. This name will be displayed as the end users realm name in the Juniper Secure Connect Client. |
| Description | Enter a description. This description will be used for the IKE and IPsec proposals, policies, remote access profile, client configuration, and NAT rule set. During edit the IPsec policy description will be displayed. IPsec policy and remote access profile descriptions will be updated. |
| Routing Mode | This option is disabled for the remote access. Default mode is Traffic Selector (Auto Route Insertion). |

Table 196: Fields on the Create Remote Access (Juniper Secure Connect) Page (Continued)

| Field | Action |
|-----------------------|---|
| Authentication Method | <p>Select an authentication method from the list that the device uses to authenticate the source of Internet Key Exchange (IKE) messages:</p> <ul style="list-style-type: none"> • EAP-MSCHAPv2 (Username & Password)—Uses the user account credentials verified by the RADIUS server (for external user authentication) to authenticate for network access. • EAP-TLS (Certificate)—Uses the TLS public key certificate authentication mechanism within EAP to provide mutual client-server and server-client authentication. With EAP-TLS, both the client and the server must be assigned a digital certificate signed by a Certificate Authority (CA) that they both trust. <p>NOTE: Starting in Junos OS Release 23.1R1, EAP-TLS is not available in Juniper Secure Connect > Remote User.</p> <ul style="list-style-type: none"> • Pre-shared Key (Username & Password)—A secret key shared between the two peers, is used during authentication to identify the peers to each other. <p>NOTE: Starting in Junos OS Release 23.2R1, when you create or edit the Juniper Secure Connect VPNs, the ike-user-type is group-ike-id. This helps to enable you with the multi device access. This is not supported for SRX300 line of Firewalls and SRX550HM Firewall.</p> |

Table 196: Fields on the Create Remote Access (Juniper Secure Connect) Page (Continued)

| Field | Action |
|-----------------------------|---|
| Auto-create Firewall Policy | <p>If you select Yes, a firewall policy is automatically created between internal zone and tunnel interface zone with local protected networks as source address and remote protected networks as destination address.</p> <p>Another firewall policy will be created visa-versa.</p> <p>If you choose No, you don't have a firewall policy option. You need to manually create the required firewall policy to make this VPN work.</p> <p>NOTE: If you do not want to auto-create a firewall policy in the VPN workflow, then the protected network is hidden for dynamic routing in both local and remote gateway.</p> |
| Remote User | <p>Displays the remote user icon in the topology. Click the icon to configure the Juniper Secure Connect client settings.</p> <p>For more information on the fields, see Table 197 on page 668 .</p> <p>NOTE: Starting in Junos OS 23.1R1 Release, J-Web displays the remote user in FQDN or FQDN/Realm format if connection profile is configured. If not configured, J-Web displays the external interface IP (for default profile) or external interface IP/VPN-Name (for non-default profile).</p> |
| Local Gateway | <p>Displays the local gateway icon in the topology. Click the icon to configure the local gateway.</p> <p>For more information on the fields, see Table 198 on page 675 .</p> |

Table 196: Fields on the Create Remote Access (Juniper Secure Connect) Page *(Continued)*

| Field | Action |
|------------------------|---|
| IKE and IPsec Settings | <p>Configure the custom IKE or IPsec proposal and the custom IPsec proposal with recommended algorithms or values.</p> <p>For more information on the fields, see Table 201 on page 682.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • J-Web supports only one custom IKE proposal and does not support the predefined proposal-set. Upon edit and save, J-Web deletes the predefined proposal set if configured. • On the remote gateway of the VPN tunnel, you must configure the same custom proposal and policy. • Upon edit, J-Web shows the first custom IKE and IPsec proposal when more than one custom proposal is configured. |

Table 197: Fields on the Remote User Page

| Field | Action |
|-----------------|---|
| Default Profile | <p>Enable this option to use the configured VPN name as remote access default profile.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • Starting in Junos OS 23.1R1 Release, default profile is deprecated in J-Web. • The field displays the configured value, if default profile is configured under VPN > IPsec VPN > Global Settings > Remote Access VPN. |

Table 197: Fields on the Remote User Page (Continued)

| Field | Action |
|--------------------------|--|
| Connection Mode | <p>Select one of the following options from the list to establish the Juniper Secure Connect client connection:</p> <ul style="list-style-type: none"> • Manual—You need manually connect to the VPN tunnel every time you log in. • Always—You are automatically connected to the VPN tunnel every time you log in. <p>The default connection mode is Manual.</p> |
| SSL VPN | <p>Enable this option to establish SSL VPN connection from the Juniper Secure Connect Client to the SRX Series Firewall.</p> <p>By default, this option is enabled.</p> <p>NOTE: This is a fallback option when IPsec ports are not reachable.</p> |
| Biometric authentication | <p>Enable this option to authenticate the client system using unique configured methods.</p> <p>An authentication prompt is displayed when you connect in the client system. The VPN connection will only be initiated after successful authentication through the method configured for <i>Windows Hello</i> (fingerprint recognition, face recognition, PIN entry, and so on).</p> <p><i>Windows Hello</i> must be preconfigured on the client system if the Biometric authentication option is enabled.</p> |

Table 197: Fields on the Remote User Page (Continued)

| Field | Action |
|---------------------|--|
| Dead Peer Detection | <p>Enable the dead peer detection (DPD) option to allow the Juniper Secure Connect client to detect if the SRX Series Firewall is reachable.</p> <p>Disable this option to allow the Juniper Secure Connect client to detect till the SRX Series Firewall connection reachability is restored.</p> <p>This option is enabled by default.</p> |
| DPD Interval | <p>Enter the amount of time that the peer waits for traffic from its destination peer before sending a dead-peer-detection (DPD) request packet. The Range is 2 through 60 seconds and default is 60 seconds.</p> |
| DPD Threshold | <p>Enter the maximum number of unsuccessful dead peer detection (DPD) requests to be sent before the peer is considered unavailable. The Range is 1 through 5 and default is 5.</p> |
| Certificates | <p>Enable Certificates to configure certificate options on Secure Client Connect.</p> <p>NOTE: This option is available only if you select the EAP-TLS (Certificate) authentication method.</p> |
| Expiry Warning | <p>Enable this option to display the certificate expiry warning on the Secure Connect Client.</p> <p>This option is enabled by default.</p> <p>NOTE: This option is available only if you enable Certificates.</p> |

Table 197: Fields on the Remote User Page (Continued)

| Field | Action |
|------------------------|---|
| Warning Interval | <p>Enter the interval (days) at which the warning to be displayed.</p> <p>Range is 1 through 90. Default value is 60.</p> <p>NOTE: This option is available only if you enable Certificates.</p> |
| Pin Req Per Connection | <p>Enable this option to enter the certificate pin on every connection.</p> <p>This option is enabled by default.</p> <p>NOTE: This option is available only if you enable Certificates.</p> |
| Save username | <p>Starting in Junos OS Release 22.1R1, you can enable this option to save the remote username.</p> |
| Save password | <p>Starting in Junos OS Release 22.1R1, you can enable this option to save both the remote username and password.</p> |
| Windows Logon | <p>Enable this option to provide users to securely log on to the Windows domain before logging on to the Windows system. The client supports domain logon using a credential service provider after establishing a VPN connection to the company network.</p> |
| Domain Name | <p>Enter the system domain name on to which the Users Machine logs.</p> |

Table 197: Fields on the Remote User Page (Continued)

| Field | Action |
|----------------------------|--|
| Mode | <p>Select one of the following options from the list to log on to Windows domain.</p> <ul style="list-style-type: none"> • Manual—You must manually enter your logon data on the Windows logon screen. • Automatic—The client software transfers the data entered here to the Microsoft logon interface (Credential Provider) without your action. |
| Disconnect at Logoff | <p>Enable this option to shut down the connection when the system switches to hibernation or standby mode. When the system resumes from hibernation or standby mode the connection has to be re-established.</p> |
| Flush Credential at Logoff | <p>Enable this option to delete username and password from the cache. You must reenter the username and password.</p> |
| Lead Time Duration | <p>Enter the lead time duration to initialize time between network logon and domain logon.</p> <p>After the connection is set up, the Windows logon will only be executed after the initialization time set here has elapsed.</p> |
| EAP Authentication | <p>Enable this option to execute EAP authentication prior to the destination dialog in the credential provider. Then, system will ask for the necessary PIN, regardless of whether EAP will be required for subsequent dial-in.</p> <p>If this option is disabled, then EAP authentication will be executed after the destination selection.</p> |

Table 197: Fields on the Remote User Page (Continued)

| Field | Action |
|---------------------|---|
| Auto Dialog Open | <p>Enable this option to select whether a dialog should open automatically for connection establishment to a remote domain.</p> <p>If this option is disabled, then the password and PIN for the client will only be queried after the Windows logon.</p> |
| Multi device access | <p>NOTE: Starting in Junos OS Release 23.2R1, J-Web supports Multi Device Access option for Remote User page. This option is not supported for SRX300 line of Firewalls and SRX550HM Firewall.</p> <p>Enable this option to connect you from multiple devices.</p> <p>NOTE: To use multi device access, the junos-ike package must be installed on your SRX Series Firewall. Run the following command on your SRX Series Firewall to install the junos-ike package:</p> <pre>request system software add optional: //junos-ike.tgz</pre> |

Table 197: Fields on the Remote User Page (Continued)

| Field | Action |
|--------------------|---|
| Application bypass | <p>Enable this option to configure which applications, domains, or both can bypass the VPN tunnel. You can select the configured application bypass profiles in the grid view.</p> <p>To add a new application bypass term:</p> <ol style="list-style-type: none"> 1. Click the + icon. 2. Enter the following details: <ul style="list-style-type: none"> • Name—Enter a name for the term. • Description—Enter application bypass term description. • Protocol—Select the protocol available from the list. The following options are available: <ul style="list-style-type: none"> • TCP & UDP—Bypasses both TCP and UDP traffic. • TCP—Bypasses only TCP traffic. • UDP—Bypasses only UDP traffic. <p>By default, TCP & UDP is selected.</p> • Domain Type—Select the domain type available from the list. The following options are available: <ul style="list-style-type: none"> • Contains—Any domain name (for example, abc.com). • FQDN—Domain name contains the fully qualified domain name (for example, www.abc.com). • Wildcard—Domain name contains any subdomain (for example, .abc.com). |

Table 197: Fields on the Remote User Page (Continued)

| Field | Action |
|------------|---|
| | <p>When wildcard is selected, “.” is prepopulated in the domain value field by default.</p> <ul style="list-style-type: none"> • Domain Value—Enter the domain name to bypass VPN tunnel. <ol style="list-style-type: none"> 3. Click the tick icon to save the changes and create application bypass term. Click X to discard. 4. Click the edit icon available above the grid to edit the application bypass term and click the delete icon to delete any application bypass term. <p>NOTE: When editing the remote user, if you toggle off Application Bypass, the configured Application bypass terms under the remote user will be deleted.</p> |
| Compliance | <p>NOTE: Starting in Junos OS Release 23.2R1, J-Web supports Compliance option for Remote User page. This option is not supported for SRX300 line of Firewalls and SRX550HM Firewall.</p> <p>Select the compliance rule from the list which will be validated by the SRX Series Firewall to establish a VPN tunnel before a user logs in.</p> <p>To create a new compliance rule, click Create. The Create Pre-Logon Compliance page appears. For the field information, see "Create Pre-Logon Compliance" on page 712 .</p> |

Table 198: Fields on the Local Gateway Page

| Field | Action |
|-----------------------|---|
| Gateway is behind NAT | Enable this option when the local gateway is behind a NAT device. |

Table 198: Fields on the Local Gateway Page (*Continued*)

| Field | Action |
|--------------------|--|
| NAT IP Address | <p>Enter the public (NAT) IP address of the SRX Series Firewall.</p> <p>NOTE: This option is available only when Gateway is behind NAT is enabled. You can configure an IPv4 address to reference the NAT device.</p> |
| External Interface | <p>Select an outgoing interface from the list for which the client will connect to.</p> <p>The list contains all available IP addresses if more than one IPv4 or IPv6 address is configured to the specified interface. The selected IP address will be configured as the local address under the IKE gateway.</p> <p>NOTE: Starting in Junos OS Release 23.4R1, J-Web supports IPv6 address for the junos-ike package installed devices.</p> |

Table 198: Fields on the Local Gateway Page (Continued)

| Field | Action |
|--------------------|---|
| Connection profile | <p>This is a mandatory field. Enter the connection profile in the format of IP address or FQDN or FQDN/Realm.</p> <p>Connection profile can be any string and can have periods and slashes; 255 characters maximum.</p> <p>IKE ID is automatically derived from connection profile.</p> <p>NOTE:</p> <ul style="list-style-type: none"> Starting in Junos OS 23.1R1 Release, IKE ID will be automatically derived using connection profile. If system hostname is configured, IKE ID will be configured as <configured-hostname>@connection-profile else it will be no-config-hostname@connection-profile. If connection profile has realm (/hr), while forming IKE ID, '/' will be replaced with '.'. For existing VPN where remote access profile name does not contain a dot (.), connection profile will be displayed as external-IP for default profile or external-IP/VPN-Name for non-default profile. Once you update existing VPN, the default profile name is updated with the connection profile value. If you change the connection profile value, IKE ID will be auto updated. |
| Tunnel Interface | <p>Select an interface from the list for the client to connect to.</p> <p>Click Add to add a new interface. The Create Tunnel Interface page appears. For more information on creating a new tunnel interface, see Table 199 on page 681.</p> <p>Click Edit to edit the selected tunnel interface.</p> |

Table 198: Fields on the Local Gateway Page (*Continued*)

| Field | Action |
|---------------------|--|
| Pre-shared Key | <p>Enter one of the following values of the preshared key:</p> <ul style="list-style-type: none"> • <code>ascii-text</code>—ASCII text key. • <code>hexadecimal</code>—Hexadecimal key. <p>NOTE: This option is available if the authentication method is Pre-shared Key.</p> |
| Local certificate | <p>Select a local certificate from the list.</p> <p>Local certificate lists only the RSA certificates.</p> <p>NOTE: This option is available only if you select the EAP-TLS (Certificate) authentication method.</p> <p>Starting in Junos OS 23.1R1 Release, all device certificates are listed in local certificates. For example, Let's Encrypt and ACME certificates. For more information on device certificates, see "Create a Device Certificate" on page 255</p> |
| User Authentication | <p>This field is mandatory. Select the authentication profile from the list that will be used to authenticate user accessing the remote access VPN.</p> <p>Click Add to create a new Profile. For more information on creating a new access profile, see "Add an Access Profile" on page 1078 .</p> |

Table 198: Fields on the Local Gateway Page (Continued)

| Field | Action |
|-----------------|---|
| SSL VPN Profile | <p>Select the SSL VPN Profile from the list that will be used to terminate the remote access connections.</p> <p>To create a new SSL VPN profile:</p> <ol style="list-style-type: none"> 1. Click Add. 2. Enter the following details: <ul style="list-style-type: none"> • Name—Enter the name for an SSL VPN profile. • Logging—Enable this option to log for SSL VPN. • SSL Termination Profile—Select an SSL termination profile from the list. <p>To add a new SSL termination profile:</p> <ol style="list-style-type: none"> a. Click Add. <p>The Create SSL Termination Profile page appears.</p> <ol style="list-style-type: none"> b. Enter the following details: <ul style="list-style-type: none"> • Name—Enter a name for the SSL termination profile. • Server Certificate—Select a server certificate from the list. <p>To add a certificate, click Add. For more information on adding a device certificate, see No Link Title.</p> <p>To import a certificate, click Import. For more information on importing a device certificate, see No Link Title.</p> <ul style="list-style-type: none"> • Click OK. c. Click OK. 3. Click OK. |

Table 198: Fields on the Local Gateway Page (Continued)

| Field | Action |
|----------------------------------|--|
| Source NAT Traffic | <p>This option is enabled by default.</p> <p>All traffic from the Juniper Secure Connect client is NATed to the selected interface by default.</p> <p>If disabled, you must ensure that you have a route from your network pointing to the SRX Series Firewalls for handling the return traffic correctly.</p> |
| Interface | Select an interface from the list through which the source NAT traffic pass through. |
| Protected Networks | Click + . The Create Protected Networks page appears. |
| Create Protected Networks | |
| Zone | Select a security zone from the list that will be used as a source zone in the firewall policy. |
| Global Address | <p>Select the addresses from the Available column and then click the right arrow to move it to the Selected column.</p> <p>Click Add to select the networks the Client can connect to.</p> <p>The Create Global Address page appears. For more information on the fields, see Table 200 on page 681 .</p> |
| Edit | <p>Select the protected network you want to edit and click on the pencil icon.</p> <p>The Edit Protected Networks page appears with editable fields.</p> |

Table 198: Fields on the Local Gateway Page *(Continued)*

| Field | Action |
|--------|--|
| Delete | <p>Select the protected network you want to edit and click on the delete icon.</p> <p>The confirmation message pops up.</p> <p>Click Yes to delete the protected network.</p> |

Table 199: Fields on the Create Tunnel Interface Page

| Field | Action |
|------------------|--|
| Interface Unit | Enter the logical unit number. |
| Description | Enter a description for the logical interface. |
| Zone | <p>Select a zone from the list to add it to the tunnel interface.</p> <p>This zone is used in the auto-creation of the firewall policy.</p> <p>Click Add to add a new zone. Enter zone name and description and click OK on the Create Security Zone page.</p> |
| Routing Instance | <p>Select a routing instance from the list.</p> <p>NOTE: The default routing instance, primary, refers to the main inet.0 routing table in the logical system.</p> |

Table 200: Fields on the Create Global Address Page

| Field | Action |
|--------|---|
| Subnet | <p>Enter the subnet for IPv4 or IPv6 address.</p> <p>NOTE: Starting in Junos OS Release 23.4R1, J-Web supports IPv6 address for the junos-ike package installed devices.</p> |

Table 200: Fields on the Create Global Address Page (Continued)

| Field | Action |
|------------|--------------------------------------|
| Identifier | Enter a name for the global address. |

Table 201: IKE and IPsec Settings

| Field | Action |
|-------|--------|
|-------|--------|

IKE Settings

NOTE: The following parameters are generated automatically and are not displayed in the J-Web UI:

- If the authentication method is Pre-Shared Key, the IKE version is v1, ike-user-type is shared-ike-id, and mode is Aggressive.
- If the authentication method is Certificate Based, the IKE version is v2, ike-user-type is shared-ike-id, and mode is Main.
- Starting in Junos OS Release 23.2R1, the ike-user-type is group-ike-id. This helps to enable you with the multi device access. You can edit and save the existing VPN to convert to group-ike-id.

This is not supported for SRX300 line of Firewalls and SRX550HM Firewall.

| | |
|--------------------------|--|
| Encryption Algorithm | Select the appropriate encryption mechanism from the list. Default value is AES-CBC 256-bit. |
| Authentication Algorithm | Select the authentication algorithm from the list. For example, SHA 256-bit. NOTE: Starting in Junos OS 23.4R1 Release, J-Web supports SHA 512-bit authentication algorithm for junos-ike package installed devices. |
| DH group | A Diffie-Hellman (DH) exchange allows participants to generate a shared secret value. Select the appropriate DH group from the list. Default value is group19. NOTE: Starting in Junos OS 23.4R1 Release, J-Web supports group 15, group 16, and group 21 DH groups for junos-ike package installed devices. |
| Lifetime Seconds | Select a lifetime duration (in seconds) of an IKE security association (SA). Default value is 28,800 seconds. Range: 180 through 86,400 seconds. |

Table 201: IKE and IPsec Settings (Continued)

| Field | Action |
|---------------------|--|
| Dead Peer Detection | Enable this option to send dead peer detection requests regardless of whether there is outgoing IPsec traffic to the peer. |
| DPD Mode | Select one of the options from the list: <ul style="list-style-type: none"> • optimized—Send probes only when there is outgoing traffic and no incoming data traffic - RFC3706 (default mode). • probe-idle-tunnel—Send probes same as in optimized mode and also when there is no outgoing and incoming data traffic. • always-send—Send probes periodically regardless of incoming and outgoing data traffic. |
| DPD Interval | Select an interval (in seconds) to send dead peer detection messages. The default interval is 10 seconds. Range is 2 to 60 seconds. |
| DPD Threshold | Select a number from 1 to 5 to set the failure DPD threshold. This specifies the maximum number of times the DPD messages must be sent when there is no response from the peer. The default number of transmissions is 5 times. |

Advance Configuration (Optional)

| | |
|----------------|--|
| NAT-T | Enable this option for IPsec traffic to pass through a NAT device. NAT-T is an IKE phase 1 algorithm that is used when trying to establish a VPN connection between two gateway devices, where there is a NAT device in front of one of the SRX Series Firewalls. |
| NAT Keep Alive | Select appropriate keepalive interval in seconds. Range: 1 to 300. If the VPN is expected to have large periods of inactivity, you can configure keepalive values to generate artificial traffic to keep the session active on the NAT devices. |

Table 201: IKE and IPsec Settings (Continued)

| Field | Action |
|---|--|
| IKE Connection Limit | <p>Enter the number of concurrent connections that the VPN profile supports.</p> <p>Range is 1 through 4294967295.</p> <p>When the maximum number of connections is reached, no more remote access user (VPN) endpoints attempting to access an IPsec VPN can begin Internet Key Exchange (IKE) negotiations.</p> |
| IKEv2 Fragmentation | <p>This option is enabled by default. IKEv2 fragmentation splits a large IKEv2 message into a set of smaller ones so that there is no fragmentation at the IP level. Fragmentation takes place before the original message is encrypted and authenticated, so that each fragment is separately encrypted and authenticated.</p> <p>NOTE: This option is available if the authentication method is Certificated Based.</p> |
| IKEv2 Fragment Size | <p>Select the maximum size, in bytes, of an IKEv2 message before it is split into fragments.</p> <p>The size applies to IPv4 message. Range: 570 to 1320 bytes.</p> <p>Default value is 576 bytes.</p> <p>NOTE: This option is available if the authentication method is Certificated Based.</p> |
| IPsec Settings | |
| <p>NOTE: The authentication method is Pre-Shared Key or Certificate Based, it automatically generates protocol as ESP.</p> | |
| Encryption Algorithm | Select the encryption method. Default value is AES-GCM 256-bit. |
| Authentication Algorithm | <p>Select the IPsec authentication algorithm from the list. For example, HMAC-SHA-256-128.</p> <p>NOTE: This option is available when the encryption algorithm is not gcm.</p> <p>NOTE: Starting in Junos OS 23.4R1 Release, J-Web supports HMAC-SHA 384 and HMAC-SHA 512 authentication algorithm for junos-ike package installed devices.</p> |

Table 201: IKE and IPsec Settings (Continued)

| Field | Action |
|-------------------------------|--|
| Perfect Forward Secrecy | <p>Select Perfect Forward Secrecy (PFS) from the list. The device uses this method to generate the encryption key. Default value is group19.</p> <p>PFS generates each new encryption key independently from the previous key. The higher numbered groups provide more security, but require more processing time.</p> <p>NOTE: group15, group16, and group21 support only the SRX5000 line of devices with an SPC3 card and junos-ike package installed.</p> <p>NOTE: Starting in Junos OS 23.4R1 Release, J-Web supports group 15, group 16, and group 21 PFS for junos-ike package installed devices.</p> |
| Lifetime Seconds | <p>Select the lifetime (in seconds) of an IPsec security association (SA). When the SA expires, it is replaced by a new SA and security parameter index (SPI) or terminated. Default is 3,600 seconds. Range: 180 through 86,400 seconds.</p> |
| Lifetime Kilobytes | <p>Select the lifetime (in kilobytes) of an IPsec SA. Default is 256kb. Range: 64 through 4294967294.</p> |
| Advanced Configuration | |
| Anti Replay | <p>IPsec protects against VPN attack by using a sequence of numbers built into the IPsec packet—the system does not accept a packet with the same sequence number.</p> <p>This option is enabled by default. The Anti-Replay checks the sequence numbers and enforce the check, rather than just ignoring the sequence numbers.</p> <p>Disable Anti-Replay if there is an error with the IPsec mechanism that results in out-of-order packets, which prevents proper functionality.</p> |
| Install Interval | <p>Select the maximum number of seconds to allow for the installation of a rekeyed outbound security association (SA) on the device. Select a value from 1 to 10 seconds.</p> |
| Idle Time | <p>Select the idle time interval. The sessions and their corresponding translations time out after a certain period of time if no traffic is received. Range is 60 to 999999 seconds.</p> |

Table 201: IKE and IPsec Settings (Continued)

| Field | Action |
|-------------------------|--|
| DF Bit | <p>Select how the device handles the Don't Fragment (DF) bit in the outer header:</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. |
| Copy Outer DSCP | <p>This option enabled by default. This enables copying of Differentiated Services Code Point (DSCP) (outer DSCP+ECN) from the outer IP header encrypted packet to the inner IP header plain text message on the decryption path. Enabling this feature, after IPsec decryption, clear text packets can follow the inner CoS (DSCP+ECN) rules.</p> |
| ICMP big packet warning | <p>Use this option to enable or disable sending ICMP packet too big notifications for IPv6 packets.</p> <p>NOTE: This option is available only for junos-ike package installed devices.</p> |
| ESN | <p>Enable this to allow IPsec to use 64-bit sequence number. If ESN is not enabled, 32-bit sequence number will be used by default. Ensure ESN is not enabled when anti-replay is disabled.</p> <p>NOTE: This option is available only for junos-ike package installed devices.</p> |
| Tunnel MTU | <p>Enter the maximum transmit packet size for IPsec tunnels.</p> <p>Range: 256 through 9192.</p> <p>NOTE: This option is available only for junos-ike package installed devices.</p> |

RELATED DOCUMENTATION

[About the IPsec VPN Page | 640](#)

[IPsec VPN Global Settings | 643](#)

[Edit an IPsec VPN | 700](#)

[Delete an IPsec VPN | 701](#)

Create a Remote Access VPN—NCP Exclusive Client

You are here: **Network > VPN > IPsec VPN.**

The NCP Exclusive Remote Access Client is part of the NCP Exclusive Remote Access solution for Juniper SRX Series Gateways. The VPN client is only available with NCP Exclusive Remote Access Management. Use the NCP Exclusive Client to establish secure, IPsec-based data links from any location when connected with SRX Series Gateways.

To create a remote access VPN for Juniper secure connect:

1. Choose **Create VPN > Remote Access > NCP Exclusive Client** on the upper right-side of the IPsec VPN page.

The Create Remote Access (NCP Exclusive Client) page appears.

2. Complete the configuration according to the guidelines provided in [Table 202 on page 687](#) through [Table 206 on page 695](#).

The VPN connectivity will change from grey to blue line in the topology to show that the configuration is complete.

3. Click **Save** to save the changes.

If you want to discard your changes, click **Cancel**.

Table 202: Fields on the Create Remote Access (NCP Exclusive Client) Page

| Field | Action |
|--------------|--|
| Name | Enter a name for the remote access connection. This name will be displayed as the end users connection name in the NCP exclusive client. |
| Description | Enter a description. This description will be used for the IKE and IPsec proposals, policies, remote access profile, client configuration, and NAT rule set. During edit the IPsec policy description will be displayed. IPsec policy and remote access profile descriptions will be updated. |
| Routing Mode | This option is disabled for the remote access. Default mode is Traffic Selector (Auto Route Insertion). |

Table 202: Fields on the Create Remote Access (NCP Exclusive Client) Page *(Continued)*

| Field | Action |
|-----------------------------|---|
| Authentication Method | <p>Select an authentication method from the list that the device uses to authenticate the source of Internet Key Exchange (IKE) messages:</p> <ul style="list-style-type: none"> • EAP Based—EAP-MSCHAPv2 uses the user account credentials verified by the RADIUS server (for external user authentication) to authenticate network access. • Pre-shared Key (Username & Password)—A secret key shared between the two peers, is used during authentication to identify the peers to each other. |
| Auto-create Firewall Policy | <p>If you select Yes, a firewall policy is automatically created between internal zone and tunnel interface zone with local protected networks as source address and remote protected networks as destination address.</p> <p>Another firewall policy will be created visa-versa.</p> <p>If you choose No, you don't have a firewall policy option. You need to manually create the required firewall policy to make this VPN work.</p> <p>NOTE: If you do not want to auto-create a firewall policy in the VPN workflow, then the protected network is hidden for dynamic routing in both local and remote gateway.</p> |
| Remote User | <p>Displays the remote user icon in the topology.</p> <p>This option is disabled.</p> |
| Local Gateway | <p>Displays the local gateway icon in the topology. Click the icon to configure the local gateway.</p> <p>For more information on the fields, see Table 203 on page 689 .</p> |

Table 202: Fields on the Create Remote Access (NCP Exclusive Client) Page *(Continued)*

| Field | Action |
|------------------------|---|
| IKE and IPsec Settings | <p>Configure the custom IKE or IPsec proposal and the custom IPsec proposal with recommended algorithms or values.</p> <p>For more information on the fields, see Table 206 on page 695.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • J-Web supports only one custom IKE proposal and does not support the predefined proposal-set. Upon edit and save, J-Web deletes the predefined proposal set if configured. • On the remote gateway of the VPN tunnel, you must configure the same custom proposal and policy. • Upon edit, J-Web shows the first custom IKE and IPsec proposal when more than one custom proposal is configured. |

Table 203: Fields on the Local Gateway Page

| Field | Action |
|-----------------------|---|
| Gateway is behind NAT | Enable this option when the local gateway is behind a NAT device. |
| NAT IP Address | <p>Enter the public (NAT) IP address of the SRX Series Firewall.</p> <p>NOTE: This option is available only when Gateway is behind NAT is enabled. You can configure an IPv4 address to reference the NAT device.</p> |
| IKE ID | This field is mandatory. Enter the IKE ID in the format user@example.com. |

Table 203: Fields on the Local Gateway Page (Continued)

| Field | Action |
|--------------------|--|
| External Interface | <p>Select an outgoing interface from the list for which the client will connect to.</p> <p>The list contains all available IP addresses if more than one IPv4 address is configured to the specified interface. The selected IP address will be configured as the local address under the IKE gateway.</p> |
| Tunnel Interface | <p>Select an interface from the list for the client to connect to.</p> <p>Click Add to add a new interface. The Create Tunnel Interface page appears. For more information on creating a new tunnel interface, see Table 204 on page 694.</p> <p>Click Edit to edit the selected tunnel interface.</p> |
| Pre-shared Key | <p>Enter one of the following values of the preshared key:</p> <ul style="list-style-type: none"> • <code>ascii-text</code>—ASCII text key. • <code>hexadecimal</code>—Hexadecimal key. <p>NOTE: This option is available if the authentication method is Pre-shared Key.</p> |
| Local certificate | <p>Select a local certificate from the list.</p> <p>Local certificate lists only the RSA certificates.</p> <p>To add a certificate, click Add. For more information on adding a device certificate, see No Link Title.</p> <p>To import a certificate, click Import. For more information on importing a device certificate, see No Link Title.</p> <p>NOTE: This option is available if the authentication method is Certificated Based.</p> |

Table 203: Fields on the Local Gateway Page (*Continued*)

| Field | Action |
|---------------------|--|
| Trusted CA/Group | <p>Select a trusted Certificate Authority/group profile from the list.</p> <p>To add a CA profile, click Add CA Profile. For more information on adding a CA profile, see No Link Title.</p> <p>NOTE: This option is available if the authentication method is Certificated Based.</p> |
| User Authentication | <p>This field is mandatory. Select the authentication profile from the list that will be used to authenticate user accessing the remote access VPN.</p> <p>Click Add to create a new Profile. For more information on creating a new access profile, see "Add an Access Profile" on page 1078 .</p> |

Table 203: Fields on the Local Gateway Page (Continued)

| Field | Action |
|-----------------|--|
| SSL VPN Profile | <p>Select the SSL VPN Profile from the list that will be used to terminate the remote access connections.</p> <p>To create a new SSL VPN profile:</p> <ol style="list-style-type: none"> 1. Click Add. 2. Enter the following details: <ul style="list-style-type: none"> • Name—Enter the name for an SSL VPN profile. • Logging—Enable this option to log for SSL VPN. • SSL Termination Profile—Select an SSL termination profile from the list. <p>To add a new SSL termination profile:</p> <ol style="list-style-type: none"> a. Click Add. b. Enter the following details: <ul style="list-style-type: none"> • Name—Enter a name for the SSL termination profile. • Server Certificate—Select a server certificate from the list. <p>To add a certificate, click Add. For more information on adding a device certificate, see No Link Title.</p> <p>To import a certificate, click Import. For more information on importing a device certificate, see No Link Title.</p> <ul style="list-style-type: none"> • Click OK. c. Click OK. 3. Click OK. |

Table 203: Fields on the Local Gateway Page (Continued)

| Field | Action |
|----------------------------------|--|
| Source NAT Traffic | <p>This option is enabled by default.</p> <p>All traffic from the Juniper Secure Connect client is NATed to the selected interface by default.</p> <p>If disabled, you must ensure that you have a route from your network pointing to the SRX Series Firewalls for handling the return traffic correctly.</p> |
| Interface | Select an interface from the list through which the source NAT traffic pass through. |
| Protected Networks | Click + . The Create Protected Networks page appears. |
| Create Protected Networks | |
| Zone | Select a security zone from the list that will be used as a source zone in the firewall policy. |
| Global Address | <p>Select the addresses from the Available column and then click the right arrow to move it to the Selected column.</p> <p>Click Add to select the networks the Client can connect to.</p> <p>The Create Global Address page appears. For more information on the fields, see Table 205 on page 694 .</p> |
| Edit | <p>Select the protected network you want to edit and click on the pencil icon.</p> <p>The Edit Protected Networks page appears with editable fields.</p> |

Table 203: Fields on the Local Gateway Page *(Continued)*

| Field | Action |
|--------|--|
| Delete | <p>Select the protected network you want to edit and click on the delete icon.</p> <p>The confirmation message pops up.</p> <p>Click Yes to delete the protected network.</p> |

Table 204: Fields on the Create Tunnel Interface Page

| Field | Action |
|------------------|--|
| Interface Unit | Enter the logical unit number. |
| Description | Enter a description for the logical interface. |
| Zone | <p>Select a zone from the list to add it to the tunnel interface.</p> <p>This zone is used in the auto-creation of the firewall policy.</p> <p>Click Add to add a new zone. Enter zone name and description and click OK on the Create Security Zone page.</p> |
| Routing Instance | <p>Select a routing instance from the list.</p> <p>NOTE: The default routing instance, primary, refers to the main inet.0 routing table in the logical system.</p> |

Table 205: Fields on the Create Global Address Page

| Field | Action |
|-------|---|
| Name | Enter a name for the global address. The name must be a unique string that must begin with an alphanumeric character and can include colons, periods, dashes, and underscores; no spaces allowed; 63-character maximum. |

Table 205: Fields on the Create Global Address Page (Continued)

| Field | Action |
|--------------|------------------------------------|
| IP Type | Select IPv4 . |
| IPv4 | |
| IPv4 Address | Enter a valid IPv4 address. |
| Subnet | Enter the subnet for IPv4 address. |

Table 206: IKE and IPsec Settings

| Field | Action |
|--|---|
| IKE Settings | |
| <p>NOTE: The following parameters are generated automatically and are not displayed in the J-Web UI:</p> <ul style="list-style-type: none"> • If the authentication method is Pre-Shared Key, the IKE version is 1, ike-user-type is shared-ike-id, and mode is Aggressive. • If the authentication method is Certificate Based, the IKE version is 2, ike-user-type is group-ike-id, and mode is Main. | |
| Encryption Algorithm | <p>Select the appropriate encryption mechanism from the list.</p> <p>Default value is AES-CBC 256-bit.</p> |
| Authentication Algorithm | <p>Select the authentication algorithm from the list. For example, SHA 256-bit.</p> <p>NOTE: Starting in Junos OS 23.4R1 Release, J-Web supports SHA 512-bit authentication algorithm for junos-ike package installed devices.</p> |
| DH group | <p>A Diffie-Hellman (DH) exchange allows participants to generate a shared secret value. Select the appropriate DH group from the list. Default value is group19.</p> <p>NOTE: Starting in Junos OS 23.4R1 Release, J-Web supports group 15, group 16, and group 21 DH groups for junos-ike package installed devices.</p> |

Table 206: IKE and IPsec Settings (Continued)

| Field | Action |
|---|--|
| Lifetime Seconds | Select a lifetime duration (in seconds) of an IKE security association (SA). Default value is 28,800 seconds. Range: 180 through 86,400 seconds. |
| Dead Peer Detection | Enable this option to send dead peer detection requests regardless of whether there is outgoing IPsec traffic to the peer. |
| DPD Mode | Select one of the options from the list: <ul style="list-style-type: none"> • optimized—Send probes only when there is outgoing traffic and no incoming data traffic - RFC3706 (default mode). • probe-idle-tunnel—Send probes same as in optimized mode and also when there is no outgoing and incoming data traffic. • always-send—Send probes periodically regardless of incoming and outgoing data traffic. |
| DPD Interval | Select an interval (in seconds) to send dead peer detection messages. The default interval is 10 seconds. Range is 2 to 60 seconds. |
| DPD Threshold | Select a number from 1 to 5 to set the failure DPD threshold. This specifies the maximum number of times the DPD messages must be sent when there is no response from the peer. The default number of transmissions is 5 times. |
| Advance Configuration (Optional) | |
| NAT-T | Enable this option for IPsec traffic to pass through a NAT device. NAT-T is an IKE phase 1 algorithm that is used when trying to establish a VPN connection between two gateway devices, where there is a NAT device in front of one of the SRX Series Firewalls. |
| NAT Keep Alive | Select appropriate keepalive interval in seconds. Range: 1 to 300. If the VPN is expected to have large periods of inactivity, you can configure keepalive values to generate artificial traffic to keep the session active on the NAT devices. |

Table 206: IKE and IPsec Settings (Continued)

| Field | Action |
|--------------------------|--|
| IKE Connection Limit | <p>Enter the number of concurrent connections that the VPN profile supports.</p> <p>Range is 1 through 4294967295.</p> <p>When the maximum number of connections is reached, no more remote access user (VPN) endpoints attempting to access an IPsec VPN can begin Internet Key Exchange (IKE) negotiations.</p> |
| IKEv2 Fragmentation | <p>This option is enabled by default. IKEv2 fragmentation splits a large IKEv2 message into a set of smaller ones so that there is no fragmentation at the IP level. Fragmentation takes place before the original message is encrypted and authenticated, so that each fragment is separately encrypted and authenticated.</p> <p>NOTE: This option is available if the authentication method is Certificated Based.</p> |
| IKEv2 Fragment Size | <p>Select the maximum size, in bytes, of an IKEv2 message before it is split into fragments.</p> <p>The size applies to IPv4 message. Range: 570 to 1320 bytes.</p> <p>Default value is 576 bytes.</p> <p>NOTE: This option is available if the authentication method is Certificated Based.</p> |
| IPsec Settings | |
| Encryption Algorithm | Select the encryption method. Default value is AES-GCM 256-bit. |
| Authentication Algorithm | <p>Select the IPsec authentication algorithm from the list. For example, HMAC-SHA-256-128.</p> <p>NOTE: This option is available when the encryption algorithm is not gcm.</p> <p>NOTE: Starting in Junos OS 23.4R1 Release, J-Web supports HMAC-SHA 384 and HMAC-SHA 512 authentication algorithm for junos-ike package installed devices.</p> |

Table 206: IKE and IPsec Settings (*Continued*)

| Field | Action |
|-------------------------------|--|
| Perfect Forward Secrecy | <p>Select Perfect Forward Secrecy (PFS) from the list. The device uses this method to generate the encryption key. Default value is group19.</p> <p>PFS generates each new encryption key independently from the previous key. The higher numbered groups provide more security, but require more processing time.</p> <p>NOTE: group15, group16, and group21 support only the SRX5000 line of devices with an SPC3 card and junos-ike package installed.</p> <p>NOTE: Starting in Junos OS 23.4R1 Release, J-Web supports group 15, group 16, and group 21 PFS for junos-ike package installed devices.</p> |
| Lifetime Seconds | <p>Select the lifetime (in seconds) of an IPsec security association (SA). When the SA expires, it is replaced by a new SA and security parameter index (SPI) or terminated. Default is 3,600 seconds. Range: 180 through 86,400 seconds.</p> |
| Lifetime Kilobytes | <p>Select the lifetime (in kilobytes) of an IPsec SA. Default is 256kb. Range: 64 through 4294967294.</p> |
| Advanced Configuration | |
| Anti Replay | <p>IPsec protects against VPN attack by using a sequence of numbers built into the IPsec packet—the system does not accept a packet with the same sequence number.</p> <p>This option is enabled by default. The Anti-Replay checks the sequence numbers and enforce the check, rather than just ignoring the sequence numbers.</p> <p>Disable Anti-Replay if there is an error with the IPsec mechanism that results in out-of-order packets, which prevents proper functionality.</p> |
| Install Interval | <p>Select the maximum number of seconds to allow for the installation of a rekeyed outbound security association (SA) on the device. Select a value from 1 to 10.</p> |
| Idle Time | <p>Select the idle time interval. The sessions and their corresponding translations time out after a certain period of time if no traffic is received. Range is 60 to 999999 seconds.</p> |

Table 206: IKE and IPsec Settings (Continued)

| Field | Action |
|-------------------------|--|
| DF Bit | <p>Select how the device handles the Don't Fragment (DF) bit in the outer header:</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. |
| Copy Outer DSCP | <p>This option enabled by default. This enables copying of Differentiated Services Code Point (DSCP) (outer DSCP+ECN) from the outer IP header encrypted packet to the inner IP header plain text message on the decryption path. Enabling this feature, after IPsec decryption, clear text packets can follow the inner CoS (DSCP+ECN) rules.</p> |
| ICMP big packet warning | <p>Use this option to enable or disable sending ICMP packet too big notifications for IPv6 packets.</p> <p>NOTE: This option is available only for junos-ike package installed devices.</p> |
| ESN | <p>Enable this to allow IPsec to use 64-bit sequence number. If ESN is not enabled, 32-bit sequence number will be used by default. Ensure ESN is not enabled when anti-replay is disabled.</p> <p>NOTE: This option is available only for junos-ike package installed devices.</p> |
| Tunnel MTU | <p>Enter the maximum transmit packet size for IPsec tunnels.</p> <p>Range: 256 through 9192.</p> <p>NOTE: This option is available only for junos-ike package installed devices.</p> |

RELATED DOCUMENTATION

[About the IPsec VPN Page | 640](#)

[IPsec VPN Global Settings | 643](#)

[Edit an IPsec VPN | 700](#)

[Delete an IPsec VPN | 701](#)

Edit an IPsec VPN

You are here: **Network > VPN > IPsec VPN.**

You can edit any of the following IPsec VPNs:

- Site-to-Site VPN
- Remote Access VPN (Juniper Secure Connect)
- Remote Access VPN (NCP Exclusive Client)

To edit IPsec VPN:

NOTE:

- When the IKE status is up and if you edit the IPsec VPN, the topology diagram is shown in green.
- All local gateway protected networks will form traffic selectors with all remote gateway protected networks and vice-versa.

1. Select an existing IPsec VPN configuration that you want to edit on the IPsec VPN page.
2. Click the pencil icon available on the upper right-side of the page.

The edit page for the selected IPsec VPN page appears with editable fields. You can modify any previous changes done to Site-to-Site VPN, Remote Access VPN (Juniper Secure Connect), and Remote Access VPN (NCP Exclusive Client).

3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

NOTE:

- During edit, Auto-create Firewall Policy and Gateway behind NAT options are not supported. Gateway behind NAT is supported only for remote access VPN.
- The Source NAT Traffic option is only supported when creating remote access VPN. During edit, this option is not supported.
- For Site-to-Site VPN, when the routing mode is Traffic Selector, the traffic selector creates the complete mesh between the local and remote addresses.

RELATED DOCUMENTATION

[Create a Site-to-Site VPN | 647](#)

[Create a Remote Access VPN—Juniper Secure Connect | 664](#)

[Create a Remote Access VPN—NCP Exclusive Client | 687](#)

[Delete an IPsec VPN | 701](#)

Delete an IPsec VPN

You are here: **Network > VPN > IPsec VPN.**

You can delete any of the VPN topologies.

To delete any IPsec VPN configurations:

1. Select existing an IPsec VPN configuration(s) that you want to delete on the IPsec VPN page.
2. Click the delete icon available on the upper-right corner of the page.

The Confirm Delete window appears.

NOTE:

- For Site-to-Site VPN, only the associated IPsec VPN routing configuration such as static route or OSPF is deleted.
- Remote Access VPN default profile will be deleted only if the deleting VPN is configured as default profile. You need to configure the default profile under **VPN > IPsec VPN > Global Settings > Remote Access VPN.**

3. Click **Yes** to delete or click **No** to retain the configuration.

RELATED DOCUMENTATION

[About the IPsec VPN Page | 640](#)

[IPsec VPN Global Settings | 643](#)

[Create a Site-to-Site VPN | 647](#)

[Edit an IPsec VPN | 700](#)

Dynamic VPN

IN THIS CHAPTER

- [About the Dynamic VPN Page | 702](#)
- [Global Settings | 704](#)
- [IPsec Template | 706](#)
- [Add a Dynamic VPN | 707](#)
- [Edit a Dynamic VPN | 708](#)
- [Delete a Dynamic VPN | 709](#)

About the Dynamic VPN Page

IN THIS SECTION

- [Tasks You Can Perform | 702](#)
- [Field Descriptions | 703](#)

You are here: **Network > VPN > Dynamic VPN.**

You can view and add, edit, or delete dynamic VPN global configuration options.

NOTE: This menu is available only for SRX300 line of devices and SRX550M devices.

Tasks You Can Perform

You can perform the following tasks from this page:

- Configure global settings. See ["Global Settings" on page 704](#) .
- Add DVPN IPsec template. See ["IPsec Template" on page 706](#) .
- Add a dynamic VPN. See ["Add a Dynamic VPN" on page 707](#) .
- Edit a dynamic VPN. See ["Edit a Dynamic VPN" on page 708](#) .
- Delete dynamic VPN. See ["Delete a Dynamic VPN" on page 709](#) .
- Launch VPN wizard. To do this, click Launch Wizard available on the upper right corner of the Dynamic VPN table. Follow the guided steps to configure the VPN wizard.

Field Descriptions

[Table 207 on page 703](#) describes the fields on the Dynamic VPN page.

Table 207: Fields on the Dynamic VPN Page

| Field | Description |
|----------------|--|
| Access Profile | <p>Select a previously created access profile from the list displayed in Global Settings.</p> <p>Specify the access profile to use for Extended Authentication for remote users trying to download the Access Manager.</p> <p>NOTE: This Access Profile option does not control authentication for VPN sessions. For more information, see Add a Gateway and Add a VPN.</p> |
| Client VPNs | Create a client configuration for the dynamic VPN feature. |
| Name | Enter a name for dynamic VPN. |
| User | Enter an username. Specifies the list of users who can use this client configuration. |
| IP Address | Enter an IP address and netmask for the users. |
| IPsec VPN | Select a previously configured IKE AutoKey configuration from the list. |

Table 207: Fields on the Dynamic VPN Page (Continued)

| Field | Description |
|----------------------------|--|
| Remote Protected Resources | Enter an IP address and netmask 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. |

RELATED DOCUMENTATION

[Global Settings | 704](#)

[Edit a Dynamic VPN | 708](#)

[Delete a Dynamic VPN | 709](#)

Global Settings

You are here: **VPN > Dynamic VPN.**

To add global settings:

1. Click **Global Settings** available on the upper-right corner of the Resource Profiles page.
The DVPN - Global Settings page appears.
2. Complete the configuration according to the guidelines provided in [Table 208 on page 704](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 208: Fields on the Global Settings page

| Field | Action |
|---------------------------------|---|
| Access Profile | Select an access profile from the list to use for Extended Authentication for remote users trying to download the Access Manager. |
| Address Profile Settings | |
| Address Pool | Select an address pool from the list |

Table 208: Fields on the Global Settings page (Continued)

| Field | Action |
|-------------------------|---|
| + | Click + to add a new address pool. The New Address Pool page appears. |
| New Address Pool | |
| Name | Enter a name for address pool. |
| Network Address | Enter the network prefix for the address pool for IPv4 or IPv6 addresses. |
| Address Ranges | |
| + | Click + to add the address range for DVPN. |
| Address Range Name | Enter an address range name. |
| Lower Limit | Enter the lower boundary for the IPv4 or IPv6 address range. |
| High Limit | Enter the upper boundary for the IPv4 or IPv6 address range. |
| X | Click X to delete the address ranges of DVPN. |
| XAUTH Attributes | |
| Primary DNS Sever | Enter the primary DNS IP address. |
| Secondary DNS Sever | Enter the secondary DNS IP address. |
| Primary WINS Sever | Enter the primary WINS IP address. |
| Secondary WINS Sever | Enter the secondary WINS IP address. |

RELATED DOCUMENTATION

[About the Dynamic VPN Page | 702](#)

[IPsec Template | 706](#)

[Add a Dynamic VPN | 707](#)

IPsec Template

You are here: **VPN > Dynamic VPN.**

To add a dynamic VPN IPsec template:

1. Click **IPsec Template** available on the upper-right corner of the Dynamic VPN page.
The DVPN IPsec Template page appears.
2. Complete the configuration according to the guidelines provided in [Table 209 on page 706](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 209: Fields on the DVPN IPsec Template Page

| Field | Action |
|---------------------------------------|--|
| Clone IPsec from DVPN template | |
| Name | Displays the name of the cloned DVPN template. |
| Preshared Key | Enter the authorization key. |
| IKE ID | Specify the IKE IDs for the DVPN. |
| External Interface | Select the external interface from the list. |

RELATED DOCUMENTATION

[About the Dynamic VPN Page | 702](#)

[Global Settings | 704](#)

[Add a Dynamic VPN | 707](#)

Add a Dynamic VPN

You are here: **Network > VPN > Dynamic VPN.**

To add a dynamic VPN:

1. Click **+** available on the upper-right corner of the Dynamic VPN page.
The Add DVPN page appears.
2. Complete the configuration according to the guidelines provided in [Table 210 on page 707](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 210: Fields on the DVPN Page

| Field | Action |
|------------------------|--|
| Name | Enter the name of the client configuration. |
| IPsec VPN | Select a previously configured IKE AutoKey configuration from the list to use when establishing the VPN tunnel. |
| Access Users | |
| Local Users in Profile | <p>Specifies the list of users who can use this client configuration.</p> <p>Select the users and click on the arrow button to move to copy to DVPN.</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> |
| Users in DVPN | Specifies the list of users copied from the local users in profile or the newly added users. |
| Username | Enter a username. |
| Password | Enter a password for the username. |

Table 210: Fields on the DVPN Page (Continued)

| Field | Action |
|----------------------------|--|
| IP | Enter an IP address for the user. |
| + | Click + and select Add to DVPN or Add to Both to add the user to either in Users in DVPN or to both DVPN and Local Users in Profile. |
| Remote Protected Resources | Enter an IP address and net mask and click +. 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. NOTE: The device does not validate that the IP/net mask combination that you enter here matches up with your security policies. |
| Remote Exceptions | Enter an IP address and net mask and click +. Specifies the IP address and net mask of exceptions to the remote protected resources list. |

RELATED DOCUMENTATION

[About the Dynamic VPN Page | 702](#)

[Edit a Dynamic VPN | 708](#)

[Delete a Dynamic VPN | 709](#)

Edit a Dynamic VPN

You are here: **Network > VPN > Dynamic VPN.**

To edit a dynamic VPN setting:

1. Select the existing a dynamic VPN settings policy that you want to edit on the Dynamic VPN page.
2. Click the pencil icon available on the upper-right corner of the page.

The Edit DVPN page appears with editable fields. For more information on the options, see ["Add a Dynamic VPN" on page 707](#).

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[About the Dynamic VPN Page | 702](#)

[Global Settings | 704](#)

[IPsec Template | 706](#)

[Add a Dynamic VPN | 707](#)

Delete a Dynamic VPN

You are here: **Network** > **VPN** > **Dynamic VPN**.

To delete a dynamic VPN:

1. Select a dynamic VPN policy that you want to delete on the Dynamic VPN page.
2. Click the delete icon available on the upper-right corner of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the Dynamic VPN Page | 702](#)

[Global Settings | 704](#)

[IPsec Template | 706](#)

[Add a Dynamic VPN | 707](#)

[Edit a Dynamic VPN | 708](#)

Compliance

IN THIS CHAPTER

- About the Compliance Page | 710
- Create Pre-Logon Compliance | 712
- Edit Pre-Logon Compliance | 718
- Delete Pre-Logon Compliance | 718

About the Compliance Page

You are here: **Network** > **VPN** > **Compliance**.

NOTE: Starting in Junos OS Release 23.2R1, J-Web supports new **Compliance** sub-menu under **Network** menu. This sub-menu is not supported for SRX300 line of Firewalls and SRX550HM Firewall.

Create compliance rules for users in the SRX Series Firewall to validate application version, OS version, hostname, domain, workgroup, and action. When a user initiates a connection, the SRX Series Firewall validates the request using the compliance rules. Once validated, the Juniper Secure Connect application connects to the SRX Series Firewall through a VPN tunnel to gain access to the networks protected resources.

You can perform the following tasks:

- Click **More** available on the upper-right corner of the Compliance page or right-click on the compliance rule to do the following:
 - Move term up and down.
 - Create pre-logon compliance term.
 - Create pre-logon compliance term before and after.

- View the details of a pre-logon compliance rule. To do this, select an existing rule and follow the available options:
 - Click **More** and select **Detailed View**.
 - Right-click on the selected rule and select **Detailed View**.
- Create pre-logon compliance. See ["Create Pre-Logon Compliance" on page 712](#) .
- Edit pre-logon compliance. See ["Edit Pre-Logon Compliance" on page 718](#) .
- Delete pre-logon compliance. See ["Delete Pre-Logon Compliance" on page 718](#) .
- Show or hide columns in the Compliance table. To do this, use the **Show Hide Columns** icon in the upper-right corner of the page and select the options you want to show or deselect to hide options on the page.
- Advanced search for compliance rule. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. An example filter condition is displayed in the search text box when you hover over the Search icon. When you start entering the search string, the icon indicates whether the filter string is valid or not.

For an advanced search:

1. Enter the search string in the text box.

Based on your input, a list of items from the filter context menu appears.

2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace to delete a character of the search string.

3. Press Enter to display the search results in the grid.

Click **X** to clear the search entries.

[Table 211 on page 711](#) provides the details of the fields on the Compliance page.

Table 211: Fields on the Compliance page

| Field | Description |
|-------|--|
| Name | Displays the pre-logon compliance rule name. |

Table 211: Fields on the Compliance page (Continued)

| Field | Description |
|------------------|---|
| Term | Displays the number of pre-logon compliance rule terms created. |
| Secure connect | Displays the client's secure connect version. |
| Operation system | Displays the client's operating system version. |
| Device IDs | Displays user device ID. |
| Hostnames | Displays hostnames defined in the compliance rule term. |
| Domains | Displays domain names defined in the compliance rule term. |
| Workgroups | Displays workgroups defined in the compliance rule term. |
| Action | Displays the action defined in the compliance rule term. |

Create Pre-Logon Compliance

You are here: **Network** > **VPN** > **Compliance**.

NOTE: Starting in Junos OS Release 23.2R1, J-Web supports new **Compliance** sub-menu under **Network** menu. This sub-menu is not supported for SRX300 line of Firewalls and SRX550HM Firewall.

To create a pre-logon compliance:

1. Click + available on the upper-right corner of the Compliance page.

The Create Pre-Logon Compliance page appears.

2. Complete the configuration according to the guidelines provided in [Table 212 on page 713](#).
3. On this page, you can perform the following tasks:
 - a. Click **More** available above the table grid or right-click on the compliance rule term to do the following:
 - Create term before and after.
 - Move term up and down.
 - View the details of a pre-logon compliance rule term.
 - b. Create pre-logon compliance rule terms. See [Table 212 on page 713](#) for more information.
 - c. Edit pre-logon compliance rule terms.
 - d. Delete pre-logon compliance rule terms.
 - e. Show or hide columns in the Terms table. To do this, use the **Show Hide Columns** present above the table grid and select the options you want to show or deselect to hide options on the page.
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.
If you click **OK**, a new pre-logon compliance with the provided configuration is created.

Table 212: Fields on the Create Pre-Logon Compliance page

| Fields | Description |
|--------|---|
| Name | Enter a name for the pre-logon compliance. Name must be a string that begins with an alphanumeric character and can include dashes, underscores, and periods; no spaces allowed; 32-character maximum. |

Table 212: Fields on the Create Pre-Logon Compliance page (Continued)

| Fields | Description |
|--------|---|
| Terms | <p>To create pre-logon compliance terms:</p> <ol style="list-style-type: none"> 1. Click + available above the table grid. The Create Term page appears. 2. Enter the following details: <ul style="list-style-type: none"> • Name—Enter a pre-logon compliance rule term name. • Action—Select Allow or Deny actions for resources and applications access request. • Secure connect—Configure client's secure connect version. Maximum allowed count is 16. To configure, do the following: <ol style="list-style-type: none"> a. Click +. b. Select an operating system from the list. c. Select an operator available in the list. d. Enter the secure connect version. e. Click the tick icon to save the changes. If you want to discard your changes, click X. <p>You can edit and delete the existing secure connect configuration using the edit icon and delete icon respectively.</p> • Operating systems—Configure client's operating system version. Maximum allowed count is 16. To configure, do the following: <ol style="list-style-type: none"> a. Click +. b. Select an operating system from the list. |

Table 212: Fields on the Create Pre-Logon Compliance page (*Continued*)

| Fields | Description |
|--------|--|
| | <ul style="list-style-type: none"> c. Select an operator available in the list. d. Enter the OS version. e. Click the tick icon to save the changes. If you want to discard your changes, click X. You can edit and delete the existing operating system configuration using the edit icon and delete icon respectively. <ul style="list-style-type: none"> • Device IDs—Configure user device IDs. Maximum allowed device IDs are 1024. To configure, do the following: <ul style="list-style-type: none"> a. Click +. b. Enter the device ID. Device ID must begin with an alphanumeric character and must contain "+", "/", and "=" only. c. Click the tick icon to save the changes. If you want to discard your changes, click X. You can edit and delete the existing device IDs using the edit icon and delete icon respectively. • Hostnames—Configure hostnames. Maximum allowed hostnames are 1024. To configure, do the following: <ul style="list-style-type: none"> a. Click +. b. Enter the hostname. |

Table 212: Fields on the Create Pre-Logon Compliance page (*Continued*)

| Fields | Description |
|--------|--|
| | <p>Hostname must begin with an alphanumeric character and must contain dashes and underscores only.</p> <p>c. Click the tick icon to save the changes.</p> <p>If you want to discard your changes, click X.</p> <p>You can edit and delete the existing hostnames using the edit icon and delete icon respectively.</p> <ul style="list-style-type: none"> • Domains—Configure domain names. Maximum allowed domains are 16. To configure, do the following: <ul style="list-style-type: none"> a. Click +. b. Enter the domain. <p>Domain name must begin with an alphanumeric character and must contain "." and "-" only.</p> <p>c. Click the tick icon to save the changes.</p> <p>If you want to discard your changes, click X.</p> <p>You can edit and delete the existing domain names using the edit icon and delete icon respectively.</p> • Workgroups—Configure workgroups. Maximum allowed workgroups are 16. To configure, do the following: <ul style="list-style-type: none"> a. Click +. b. Enter the workgroup. <p>Workgroup must begin with an alphanumeric character and must contain "." and "-" only.</p> |

Table 212: Fields on the Create Pre-Logon Compliance page (*Continued*)

| Fields | Description |
|-------------------|---|
| | <p>c. Click the tick icon to save the changes.</p> <p>If you want to discard your changes, click X.</p> <p>You can edit and delete the existing workgroups using the edit icon and delete icon respectively.</p> <p>3. Click OK to save the changes. If you want to discard your changes, click Cancel.</p> <p>If you click OK, a new pre-logon compliance rule term with the provided configuration is created.</p> |
| Name | Displays pre-logon compliance rule term name. |
| Secure connect | Displays client's secure connect version |
| Operating systems | Displays client's operating system version. |
| Device IDs | Displays user device ID. |
| Hostnames | Displays hostnames defined in the compliance rule term. |
| Domains | Displays domain names defined in the compliance rule term. |
| Workgroups | Displays workgroups defined in the compliance rule term. |
| Action | Displays the action defined in the compliance rule term. |

RELATED DOCUMENTATION

[About the Compliance Page | 710](#)

[Edit Pre-Logon Compliance | 718](#)

Edit Pre-Logon Compliance

You are here: **Network** > **VPN** > **Compliance**.

NOTE: Starting in Junos OS Release 23.2R1, J-Web supports new **Compliance** sub-menu under **Network** menu. This sub-menu is not supported for SRX300 line of Firewalls and SRX550HM Firewall.

To edit a pre-logon compliance:

1. Select the pre-logon compliance that you want to edit on the Compliance page.
2. Click the edit icon available on the upper-right corner of the Compliance page.
The Edit Pre-Logon Compliance page appears.
3. Select the term that you want to edit.
The Edit Term page appears with editable fields. For more information on the options, see [Table 212 on page 713](#).
4. Click the tick icon to accept the changes. If you want to discard, click **X**.

RELATED DOCUMENTATION

[Create Pre-Logon Compliance | 712](#)

[Delete Pre-Logon Compliance | 718](#)

Delete Pre-Logon Compliance

You are here: **Network** > **VPN** > **Compliance**.

NOTE: Starting in Junos OS Release 23.2R1, J-Web supports new **Compliance** sub-menu under **Network** menu. This sub-menu is not supported for SRX300 line of Firewalls and SRX550HM Firewall.

To delete a pre-logon compliance:

1. Select the pre-logon compliance that you want to delete on the Compliance page.
2. Click the delete icon available on the upper-right corner of the Compliance page.

["Create Pre-Logon Compliance" on page 712](#)

A confirmation window appears.

3. Click **Yes** to delete.

RELATED DOCUMENTATION

[Edit Pre-Logon Compliance | 718](#)

[Create Pre-Logon Compliance | 712](#)

7

PART

Security Policies and Objects

[Security Policies | 721](#)

[Metadata Streaming Policy | 775](#)

[Zones/Screens | 780](#)

[Zone Addresses | 798](#)

[Global Addresses | 805](#)

[Services | 811](#)

[Dynamic Applications | 820](#)

[Application Tracking | 835](#)

[Schedules | 837](#)

[Proxy Profiles | 843](#)

Security Policies

IN THIS CHAPTER

- [About the Security Policies Page | 721](#)
- [Global Options | 726](#)
- [Add a Rule to a Security Policy | 729](#)
- [Clone a Security Policy Rule | 746](#)
- [Edit a Security Policy Rule | 747](#)
- [Delete a Security Policy Rule | 747](#)
- [Configure Captive Portal for Web Authentication and Firewall User Authentication | 748](#)

About the Security Policies Page

IN THIS SECTION

- [Tasks You Can Perform | 722](#)
- [Field Descriptions | 725](#)

You are here: **Security Policies & Objects > Security Policies.**

Use this page to get a high-level view of your firewall policy rules settings. The security policy applies the security rules to the transit traffic within a context (from-zone to to-zone). The traffic is classified by matching its source and destination zones, the source and destination addresses, and the application that the traffic carries in its protocol headers with the policy database in the data plane.

Using a global policy, you can regulate traffic with addresses and applications, regardless of their security zones, by referencing user-defined addresses or the predefined address “any.” These addresses can span multiple security zones.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add Global Options. See ["Global Options" on page 726](#) .
- Add a Rule. See ["Add a Rule to a Security Policy" on page 729](#) .
- Edit a Rule. See ["Edit a Security Policy Rule" on page 747](#) .
- Clone a Rule. See ["Clone a Security Policy Rule" on page 746](#) .
- Delete a Rule. See ["Delete a Security Policy Rule" on page 747](#) .
- To save the rules configuration, click **Save**.
- To delete the rules configuration, click **Discard**.
- Drag and drop the rules within a zone context. To do this, select the rule you want to place in a different sequence number within a zone context, drag and drop it using the cursor.

NOTE: If you drag and drop a rule outside the zone context, J-Web will display a warning message that you cannot move the rule into another zone context.

- Advanced search for policy rule. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. An example filter condition is displayed in the search text box when you hover over the Search icon. When you start entering the search string, the icon indicates whether the filter string is valid or not.

For an advanced search:

1. Enter the search string in the text box.

Based on your input, a list of items from the filter context menu appears.

2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace to delete a character of the search string.

3. Press Enter to display the search results in the grid.

The supported search scenarios and its examples are as follows:

1. Logical operators:

- AND operator for multiple parameters

Example: Name = Rule1 AND Dynamic Application = Malware

- OR operator for same and different parameters

Example for same parameters: Name = Rule1 OR Name = Rule2

Example for different parameters: Name = Rule1 OR Dynamic Application = Malware

- Combination of AND and OR operators

Example: Name = Rule1 AND (Dynamic Application = Malware OR Action = Reject)

- Comma (,) separated value

Example: Name = Rule1, Rule2

- != operator for single parameter

Example: Name != Rule1

2. Dynamic applications or service objects with matching characters of *Junos*

When you search for the matching characters of Junos, such as, jun, un, nos, and os, the result displays all the matched objects but without junos prefix. For example, if the configured dynamic application is *junos:01NET*, the search for dynamic applications with *jun* characters display only *01NET*.

3. Saved policy rules

When you add or edit a rule, click **Save** to save the configuration. To search for this saved configuration, you must wait for the device to synchronize the configuration.

- Show or hide columns in the policy rule table. To do this, click Show Hide Columns icon in the upper-right corner of the policy rule table and select the columns you want to display or deselect the columns you want to hide on the page.

[Table 213 on page 724](#) describes few more options on Rules.

Table 213: More Options on the Security Policies Page

| Field | Description |
|--------------------|---|
| Create Rule Before | <p>Adds a new rule before the selected rule.</p> <p>To add a new rule before the selected rule:</p> <ol style="list-style-type: none"> 1. Select an existing rule before which you want to create a rule. 2. Click More > Create Rule Before. <p>Alternatively, you can right-click on the selected rule and select Create Rule Before.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • When you create a new rule, it inherits the name, source zone, and destination zone same as parent (selected) rule. Source address and destination address will be any and the action will be Deny. • For global policy, source zone and destination zone will not be available. <ol style="list-style-type: none"> 3. Click tick mark to create the new rule. |
| Create Rule After | <p>Adds a new rule after the selected rule.</p> <p>To add a new rule after the selected rule:</p> <ol style="list-style-type: none"> 1. Select an existing rule after which you want to create a rule. 2. Click More > Create Rule After. <p>Alternatively, you can right-click on the selected rule and select Create Rule After.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • When you create a new rule, it inherits the name, source zone, and destination zone same as parent (selected) rule. Source address and destination address will be any and the action will be Deny. • For global policy, source zone and destination zone will not be available. <ol style="list-style-type: none"> 3. Click tick mark to create the new rule. |
| Clone | <p>Clones or copies the selected firewall policy configuration and enables you to update the details of the rule.</p> |
| Clear All | <p>Clears the selection of those rules that are selected.</p> |

Field Descriptions

Table 214 on page 725 describes the fields on the Security Policies page.

NOTE: On the Security Policies page:

- For logical systems and tenants, the URL Categories option will not be displayed.
- For tenants, the Dynamic Application option will not be displayed.

Table 214: Fields on the Security Policies Page

| Field | Description |
|---------------------|---|
| Seq | Displays the sequence number of rules in a zone pair. |
| Hits | Displays the number of hits the rule has encountered. |
| Rule Name | Displays the rule name. You can hover over the name column to view the rule name and its description. |
| 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 | Displays the dynamic application names for match criteria in application firewall rule set. An application firewall configuration permits, rejects, or denies traffic based on the application of the traffic. |

Table 214: Fields on the Security Policies Page (Continued)

| Field | Description |
|-------------------|---|
| Services | 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. |
| Advanced Security | Displays the security option that apply for this rule. |
| Rule Options | Displays the rule option while permitting the traffic. |
| Schedule | Displays the scheduler details that allow a policy to be activated for a specified duration. You can define schedulers for a single (nonrecurrent) or recurrent time slot within which a policy is active. |

RELATED DOCUMENTATION

| [Global Options](#) | 726

Global Options

You are here: **Security Policies & Objects > Security Policies.**

To add global options:

1. Click **Global Options** available on the upper-right corner of the Security Policies page.
The Global Options page appears.
2. Complete the configuration according to the guidelines provided in [Table 215 on page 727](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

[Table 215 on page 727](#) describes the fields on the Global Options page.

Table 215: Fields on the Global Options Page

| Field | Action |
|--|--|
| Pre-id Default Policy | |
| Session Timeout | |
| ICMP | Enter the timeout value for ICMP sessions ranging from 4 through 86400 seconds. |
| ICMP6 | Enter the timeout value for ICMP6 sessions ranging from 4 through 86400 seconds. |
| OSPF | Enter the timeout value for OSPF sessions ranging from 4 through 86400 seconds. |
| TCP | Enter the timeout value for TCP sessions ranging from 4 through 86400 seconds. |
| UDP | Enter the timeout value for UDP sessions ranging from 4 through 86400 seconds. |
| Others | Enter the timeout value for other sessions ranging from 4 through 86400 seconds. |
| Logging | |
| Session Initiate | <p>Enable this option to start logging at the beginning of a session.</p> <p>WARNING: Configuring session-init logging for the pre-id-default-policy can generate a large number of logs.</p> |
| Session Close | <p>Enable this option to start logging at the closure of a session.</p> <p>NOTE: Configuring session-close logging ensures that the SRX Series Firewall generates the security logs if a flow is unable to leave the pre-id-default-policy.</p> |
| Flow | |
| Aggressive Session Aging | |
| NOTE: This option is not supported for logical systems and tenants. | |

Table 215: Fields on the Global Options Page (Continued)

| Field | Action |
|-----------------------------------|---|
| Early Ageout | Enter a value from 1 through 65,535 seconds. The default value is 20 seconds. Specifies the amount of time before the device aggressively ages out a session from its session table. |
| Low watermark | Enter a value from 0 through 100 percent. The default value is 100 percent. Specifies the percentage of session table capacity at which the aggressive aging-out process ends. |
| High watermark | Enter a value from 0 through 100 percent. The default value is 100 percent. Specifies the percentage of session table capacity at which the aggressive aging-out process begins. |
| SYN Flood Protection | |
| SYN Flood Protection | Enable this option to defend against SYN attacks. |
| Mode | Select one of the following options: <ul style="list-style-type: none"> • Cookie—Uses a cryptographic hash to generate a unique Initial Sequence Number (ISN). This is enabled by default. • Proxy—Uses a proxy to handle the SYN attack. |
| TCP MSS | |
| All TCP Packets | Enter a maximum segment size value from 64 through 65,535 to override all TCP packets for network traffic. |
| Packets entering IPsec Tunnel | Enter a maximum segment size value from 64 through 65,535 bytes to override all packets entering an IPsec tunnel. The default value is 1320 bytes. |
| GRE Packets entering IPsec Tunnel | Enter a maximum segment size value from 64 through 65,535 bytes to override all generic routing encapsulation packets entering an IPsec tunnel. The default value is 1320 bytes. |

Table 215: Fields on the Global Options Page (Continued)

| Field | Action |
|----------------------------------|---|
| GRE Packets exiting IPsec Tunnel | Enter a maximum segment size value from 64 through 65,535 bytes to override all generic routing encapsulation packets exiting an IPsec tunnel. The default value is 1320 bytes. |
| TCP Session | |
| Sequence number check | By default, this option is enabled to check sequence numbers in TCP segments during stateful inspections. The device monitors the sequence numbers in TCP segments. |
| SYN flag check | By default, this option is enabled to check the TCP SYN bit before creating a session. 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. |

RELATED DOCUMENTATION

[Add a Rule to a Security Policy | 729](#)

Add a Rule to a Security Policy

You are here: **Security Policies & Objects > Security Policies.**

NOTE: To reference the Content Security policies and the AppQoS profiles in a security policy rules, create Content Security polices and AppQoS profiles before creating or editing security policy rules if required. To create Content Security policies, go to **Security Services > Content Security > Content Security Policies** and to create AppQoS profiles, go to **Network > Application QoS**.

To add a rule to a security policy:

1. Click **+** available on the upper-right corner of the Security Policies page.
The inline editable fields will appear.
2. Complete the configuration according to the guidelines provided in [Table 216 on page 730](#).

3. Click the tick icon on the upper right of the row once done with the configuration.

NOTE: Scroll back the horizontal bar if the inline tick and the cancel icons are not available when creating a new rule.

4. Click **Save** to save the changes or click **Discard** to discard the changes.

NOTE: You must perform Step 3 and Step 4 before performing any further actions in the J-Web UI.

Table 216: Fields on the Security Policies Page

| Field | Action |
|------------------|--|
| Rule Name | Enter a name for the new rule or policy. |
| Rule Description | Enter a description for the security policy. |
| Global Policy | Enable this option to specify that the policy defined is a global policy and zones are not required. |

Table 216: Fields on the Security Policies Page (*Continued*)

| Field | Action |
|-------------|---|
| Source Zone | <p>To add sources:</p> <ol style="list-style-type: none"> Click +. The Select Sources page appears. Enter the following details: <ul style="list-style-type: none"> Zone—Select the source zone from the list to which you want the rule to be associated. Addresses—Select any or Specific. <p>NOTE:</p> <ul style="list-style-type: none"> You can select the IP feeds to define the matching criteria for a policy. Also, you can view source type (Address, Address group, Wild card, Range, IP feeds) in the new Type column. Feeds are only displayed if you have enrolled to Juniper ATP Cloud. You can also download the feeds using the command, <code>request services security-intelligence download</code>. <p>To select a specific address or IP feed, select the addresses or IP feeds from the Available column and then click the right arrow to move it to the Selected column. You can select Exclude Selected to exclude only the selected address from the list.</p> <p>To create a new address, click +. The Create Address page appears. For more information on fields, see Table 217 on page 741 .</p> <ul style="list-style-type: none"> Source identity—Select the user identity from the Available column and then click the right arrow to move it to the Selected column. To create a source identity, click +. Enter a new username or identity in the Create Source Identity page and click OK. Source identity feed—You can select user identity threat feed to define the matching criteria for a policy. Select the user identity threat feed from the Available column and then click the right arrow to move it to the Selected column. |

Table 216: Fields on the Security Policies Page (*Continued*)

| Field | Action |
|-------|---|
| | <p>Maximum user identity threat feed count is 1024. That is, sum of source identity feed and destination identity feed per policy.</p> <p>NOTE: Feeds are only displayed if you have enrolled to Juniper ATP Cloud. You can also download the feeds using the command, <code>request services security-intelligence download</code>.</p> |

Table 216: Fields on the Security Policies Page (Continued)

| Field | Action |
|------------------|--|
| Destination Zone | <p>To add a destination:</p> <ol style="list-style-type: none"> Click +. The Select Destination page appears. Enter the following details: <ul style="list-style-type: none"> Zone—Select the destination zone from the list to which you want the rule to be associated. Addresses—Select any or Specific. <p>NOTE:</p> <ul style="list-style-type: none"> You can select the IP feeds to define the matching criteria for a policy. Also, you can view source type (Address, Address group, Wild card, Range, IP feeds) in the new Type column. Feeds are only displayed if you have enrolled to Juniper ATP Cloud. You can also download the feeds using the command, <code>request services security-intelligence download</code>. <p>To select a specific address or IP feed, select the addresses or IP feeds from the Available column and then click the right arrow to move it to the Selected column. You can select Exclude Selected to exclude only the selected address from the list.</p> <p>To create a new address, click +. For more information on fields, see Table 217 on page 741.</p> <ul style="list-style-type: none"> Dynamic applications—Select Any, Specific, or None. <p>NOTE: The Dynamic Applications option is not supported for tenants.</p> <p>To select a specific application, select the application from the Available column and then click the right arrow to move it to the Selected column.</p> <p>NOTE: The select all check box is only available when you search for specific dynamic applications.</p> |

Table 216: Fields on the Security Policies Page (Continued)

| Field | Action |
|--------|--|
| | <p>To create a new application, click +. The Create Application Signature page appears. For more information on fields, see "Add Application Signatures" on page 826 .</p> <p>NOTE: For logical systems, you cannot create a dynamic application inline.</p> <ul style="list-style-type: none"> • Services—Select Any, Specific, or None. <p>To select a specific service, select the service from the Available column and then click the right arrow to move it to the Selected column.</p> <p>To create a new service, click +. The Create Service page appears. For more information on fields, see Table 218 on page 742 .</p> <ul style="list-style-type: none"> • URL category—Select any, Specific, or None to match criteria for a web filtering category. <p>To select a specific URL category, select the URL category from the Available column and then click the right arrow to move it to the Selected column.</p> <p>NOTE: This option is not available for logical systems and tenants.</p> <ul style="list-style-type: none"> • Destination identity feed—You can select user identity threat feed to define the matching criteria for a policy. <p>Select the user identity threat feed from the Available column and then click the right arrow to move it to the Selected column.</p> <p>Maximum user identity threat feed count is 1024. That is, sum of source identity feed and destination identity feed per policy.</p> <p>NOTE: Feeds are only displayed if you have enrolled to Juniper ATP Cloud. You can also download the feeds using the command, <code>request services security-intelligence download</code>.</p> |
| Action | <p>Select an action to take when traffic matches the criteria:</p> <ul style="list-style-type: none"> • Permit—Allows packet to pass through the firewall. • Deny—Block and drop the packet, but do not send notification back to the source. • Reject—Block and drop the packet and send a notice to the source host. |

Table 216: Fields on the Security Policies Page (*Continued*)

| Field | Action |
|---|--|
| <p>Advanced Services Click +. The Select Advanced Services page appears.</p> | |
| <p>NOTE:</p> <ul style="list-style-type: none"> • When the action is Reject: <ul style="list-style-type: none"> • You can configure only the SSL Proxy and Redirect Profile options. • You can configure only the SSL Proxy option if the dynamic application is None. • Advanced Security option is not supported for logical systems and tenants. • When the action is Permit: <ul style="list-style-type: none"> • For logical systems, only IPS, IPS policy, Content Security, threat prevention policy, ICAP redirect profile, and AppQOS options are supported. • For tenant systems, only threat prevention policy and AppQOS are supported. | |
| SSL proxy | Select the SSL proxy policy to associate with this rule from the list. |
| Content Security | <p>Select the Content Security policy you want to associate with this rule from the list. The list displays all the Content Security policies available.</p> <p>If you want to create a new Content Security policy, click Add New. The Create a Content Security Policy page appears. For more information on creating a new Content Security policy, see "Create a Content Security Policy" on page 944 .</p> |
| IPS policy | Select the IPS policy from the list. |
| Threat prevention policy | Select the configured threat prevention policy from the list. |
| ICAP redirect profile | Select the configured ICAP redirect profile name from the list. |

Table 216: Fields on the Security Policies Page (Continued)

| Field | Action |
|-------------------------|--|
| AAMW | <p>Select an anti-malware profile from the list that you want to associate with the security policy.</p> <p>NOTE: Starting in Junos OS 22.2R1 Release, you can associate an anti-malware profile with the security policies.</p> |
| SecIntel profile group | <p>Select a SecIntel profile group from the list that you want to associate with the security policy.</p> <p>NOTE: Starting in Junos OS 22.2R1 Release, you can associate a SecIntel profile group with the security policies.</p> |
| IPsec VPN | <p>Select the IPsec VPN tunnel from the list.</p> <p>NOTE: If you select Dynamic applications in the destination, IPsec VPN option is not supported.</p> |
| Pair policy name | <p>Enter the name of the policy with the same IPsec VPN in the opposite direction to create a pair policy.</p> <p>NOTE: If you select Dynamic applications in the destination, Pair Policy Name option is not supported.</p> |
| Application QoS profile | <p>Select the configured AppQoS profile from the list.</p> <p>If you want to create a new AppQoS profile, click Add New. The Add AppQoS Profile page appears. For more information on creating a new AppQoS profile, see "Add an Application QoS Profile" on page 633 .</p> |

Table 216: Fields on the Security Policies Page (Continued)

| Field | Action |
|------------------|--|
| Threat profiling | <p>Starting in Junos OS Release 21.4R1, you can enable this option to generate threat profiling feeds.</p> <p>NOTE: Feeds are only displayed if you have enrolled to Juniper ATP Cloud. You can also download the feeds using the command, <code>request services security-intelligence download</code>.</p> <p>You can add source and destination addresses, and source and destination identities to the threat feeds. After the feeds are generated, you can configure other security policies to use the feeds to match designated traffic and perform policy actions.</p> <ul style="list-style-type: none"> • Add source IP to feed—Select the threat feed from the list to add it to the source IP address. • Add source identity to feed—Select the threat feed from the list to add it to the source user identity. • Add destination IP to feed—Select the threat feed from the list to add it to the destination IP address. • Add destination identity to feed—Select the threat feed from the list to add it to the destination user identity. |
| Packet capture | <p>Enable to capture unknown application traffic specific to a security policy rule.</p> <p>By default, this option is disabled. Once enabled, you can view the packet capture (PCAP) file details or download the PCAP file on the Monitor > Log > Sessions page.</p> |

Rule Options

Click on **Rule Options**. The SELECT RULE OPTIONS page appears.

Logging

| | |
|------------------|---|
| Session initiate | Enable this option to log an event when a session is created. |
| Session close | Enable this option to log an event when the session closes. |

Table 216: Fields on the Security Policies Page (Continued)

| Field | Action |
|---|--|
| Count | <p>Enable this option to collect statistics of the number of packets, bytes, and sessions that pass through the firewall with this policy.</p> <p>Specifies statistical counts. An alarm is triggered whenever traffic exceeds specified packet and byte thresholds.</p> <p>NOTE: Alarm threshold fields are disabled if Enable Count is not enabled.</p> |
| <p>Authentication</p> <p>NOTE:</p> <ul style="list-style-type: none"> • If you select Dynamic applications in the destination, Authentication option is not supported. • This option is not supported for logical systems and tenant systems. | |
| Push auth entry to JIMS | <p>Enable this option to push authentication entries from firewall authentication, that are in auth-success state, to Juniper Identity Management Server (JIMS). This will enable the SRX Series Firewall to query JIMS to get IP/user mapping and device information.</p> <p>This is not a mandatory option. You can select it when at least one domain is configured on local Active Directory or configure identity management.</p> |
| Type | Select the firewall authentication type from the list. The options available are: None, Pass-through, User-firewall, and Web-authentication. |
| Access profile | <p>Select an access profile from the list.</p> <p>NOTE: This option is not supported if you select the authentication type as Web-authentication.</p> |
| Client name | <p>Enter the client username or client user group name.</p> <p>NOTE: This option is not supported if you select the authentication type as User-firewall.</p> |
| Domain | <p>Select a domain name that must be in a client name from the list.</p> <p>NOTE: This option is supported only if you select the authentication type as User-firewall.</p> |

Table 216: Fields on the Security Policies Page (Continued)

| Field | Action |
|---------------------|--|
| Web redirect (http) | <p>Enable this option to redirect HTTP requests to the device's internal webserver by sending a redirect HTTP response to the client system to reconnect to the webserver for user authentication.</p> <p>NOTE: This option is not supported if you select the authentication type as Web-authentication.</p> |
| Captive portal | <p>Enable this option to redirect a client HTTP or HTTPS request to the internal HTTPS webserver of the device. The HTTPS client requests are redirected when SSL termination profile is configured.</p> <p>NOTE: This option is not supported if you select the authentication type as Web-authentication.</p> |
| Interface | <p>Select an interface for the webserver where the client HTTP or HTTPS request is redirected.</p> <p>NOTE: You cannot edit this once the policy is created. To edit the interface, go to Network > Connectivity > Interfaces.</p> |
| IPv4 address | <p>Enter IPv4 address of the webserver where the client HTTP or HTTPS request is redirected.</p> <p>NOTE: You cannot edit this once the policy is created. To edit the interface, go to Network > Connectivity > Interfaces.</p> |

Table 216: Fields on the Security Policies Page (Continued)

| Field | Action |
|---------------------------------|---|
| SSL termination profile | <p>Select an SSL termination profile from the list which contains the SSL terminated connection settings. SSL termination is a process where the SRX Series Firewall acts as an SSL proxy server, terminates the SSL session from the client.</p> <p>To add a new SSL termination profile:</p> <ol style="list-style-type: none"> 1. Click Add. The Create SSL Termination Profile page appears. 2. Enter the following details: <ul style="list-style-type: none"> • Name—Enter SSL termination profile name; 63-character maximum. • Server certificate—Select a server certificate from the list that is used to authenticate the server identity. <p>To add a certificate, click Add. For more information on adding a device certificate, see No Link Title.</p> <p>To import a certificate, click Import. For more information on importing a device certificate, see, No Link Title.</p> |
| Auth only browser | <p>Enable this option to drop non-browser HTTP traffic to allow for captive portal to be presented to unauthenticated users who request access using a browser.</p> <p>NOTE: This option is not supported if you select the authentication type as Web-authentication.</p> |
| User agents | <p>Enter a user-agent value which is used to verify that the user's browser traffic is HTTP/HTTPS traffic.</p> <p>NOTE: This option is not supported if you select the authentication type as Web-authentication.</p> |
| Advanced Settings | |
| Destination address translation | <p>Select the action to be taken on a destination address translation from the list. The options available are: None, Drop Translated, and Drop Untranslated.</p> |

Table 216: Fields on the Security Policies Page (Continued)

| Field | Action |
|----------------------------|---|
| Redirect options | Select a redirect action from the list. The options available are: None, Redirect Wx, and Reverse Redirect Wx. NOTE: This option is not supported for SRX5000 line of devices. |
| TCP Session Options | |
| Sequence number check | Enable or disable checking of sequence numbers in TCP segments during stateful inspections at policy rule level. By default, the check happens at the global level. To avoid commit failure, turn off Sequence number check under Global Options > Flow > TCP Session . |
| SYN flag check | Enable or disable the checking of the TCP SYN bit before creating a session at policy rule level. By default, the check happens at the global level. To avoid commit failure, turn off SYN flag check under Global Options > Flow > TCP Session . |
| Schedule | |
| Schedule | Click Schedule and select one of the configured schedules from the list. To add a new schedule, click Add New Schedule . The Add New Schedule page appears. For more information on creating a new schedule, see Table 219 on page 744 . |

Table 217: Fields on the Create Address Page

| Field | Action |
|--------------|--|
| Name | Enter a name for the address. The name must be a unique string that must begin with an alphanumeric character and can include colons, periods, dashes, and underscores; no spaces allowed; 63-character maximum. |
| IP type | Select IPv4 or IPv6 . |
| IPv4 | |
| IPv4 address | Enter a valid IPv4 address. |

Table 217: Fields on the Create Address Page (Continued)

| Field | Action |
|---------------|---|
| Subnet | Enter a subnet mask for the IPv4 address. |
| IPv6 | |
| IPv6 address | Enter a valid IPv6 address. |
| Subnet prefix | Enter a subnet prefix for the IPv6 address. |

Table 218: Fields on the Create Service Page

| Field | Action |
|------------------------|--|
| Global Settings | |
| Name | Enter a unique name for the application. |
| Description | Enter description of the 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. |

Table 218: Fields on the Create Service Page (Continued)

| Field | Action |
|--------------------------|--|
| RPC program numbers | Enter a value for RPC program numbers. The format of the value must be W or X-Y. Where, W, X, and Y are integers between 0 and 65535. |
| Inactivity timeout | Select an option from the list for application specific inactivity timeout. |
| UUID | Enter a value for DCE RPC objects. NOTE: The format of the value must be 12345678-1234-1234-1234-123456789012. |
| Custom application group | Select an application set name from the list. |

Terms

Click +. The Create Term page appears.

| | |
|-------------------|---|
| Name | Enter a name for the 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. |

Table 218: Fields on the Create Service Page (Continued)

| Field | Action |
|---------------------|---|
| RPC program numbers | Enter a value for RPC program numbers. NOTE: The format of the value must be W or X-Y. Where, W, X, and Y are integers between 0 and 65535. |
| Inactivity timeout | Select an option from the list for application specific inactivity timeout. |
| UUID | Enter a value for DCE RPC objects. NOTE: The format of the value must be 12345678-1234-1234-1234-123456789012. |

Table 219: Fields on the Add New Schedule Page

| Field | Action |
|-------------|---|
| Name | Enter the name for the schedule. |
| Description | Enter a description for the schedule. |
| Repeats | Select an option from the list to repeat the schedule: <ul style="list-style-type: none"> • Never • Daily • Weekly |
| All Day | Enable this option to schedule an event for an entire day. This option is available only for Never and Daily repeat type schedule. |
| Start date | Select the schedule start date in the YYYY-MM-DD format. This option is available only for Never repeat type schedule. |

Table 219: Fields on the Add New Schedule Page (Continued)

| Field | Action |
|------------|---|
| Stop date | <p>Select the schedule stop date in the YYYY-MM-DD format.</p> <p>This option is available only for Never repeat type schedule.</p> |
| Start time | <p>Enter the start time for the schedule in HH:MM:SS 24 hours format.</p> <p>This option is available only for Daily repeat type schedule.</p> |
| Stop time | <p>Enter the end time for the schedule in HH:MM:SS 24 hours format.</p> <p>This option is available only for Daily repeat type schedule.</p> |
| Repeat on | <p>Select the days and time on which you want to repeat the schedule.</p> <p>To set time for the selected day(s):</p> <ol style="list-style-type: none"> 1. Click Set Time or Set Time to Selected Days. <p>The Set Time to Selected Days page appears.</p> <ol style="list-style-type: none"> 2. Enter the following details: <ul style="list-style-type: none"> • Name—Displays the day(s) you have selected. • All day—Enable this option for the event to run for the entire day. • Start time—Enter the start time in HH:MM:SS 24 hours format. • Stop time—Enter the stop time in HH:MM:SS 24 hours format. 3. Click OK to save changes. <p>This option is available only for Weekly repeat type schedule.</p> |

Table 219: Fields on the Add New Schedule Page (Continued)

| Field | Action |
|-------------------|---|
| Schedule criteria | <p>Select any of the following options:</p> <ul style="list-style-type: none"> • Schedule Never Stops—Schedule can be active forever (recurrent), but only as specified by the daily or weekly schedule. • Schedule Specify Window—Schedule can be active during a single time slot, as specified by a start date and a stop date. <p>Enter the following details:</p> <ul style="list-style-type: none"> • Schedule starts—Enter the schedule start date in the YYYY-MM-DD format. • Schedule ends—Enter the schedule start date in the YYYY-MM-DD format. <p>This option is available only for Daily and Weekly repeat type schedule.</p> |

RELATED DOCUMENTATION

[Edit a Security Policy Rule | 747](#)

[Clone a Security Policy Rule | 746](#)

Clone a Security Policy Rule

You are here: **Security Policies & Objects > Security Policies.**

To clone a rule:

1. Select a rule that you want to clone on the Security Policies page.
2. Click **More > Clone** available on the upper right-side of the page.

The Security Policies page appears with inline editable fields. For more information on editing the fields, see "[Add a Rule to a Security Policy](#)" on page 729 .

3. Click **OK** to save the changes or click **Cancel** to discard the changes.

A cloned rule is created for the selected rule. By default, the name of the cloned rule is in the format: `<rule name>_clone`.

RELATED DOCUMENTATION

[Delete a Security Policy Rule | 747](#)

Edit a Security Policy Rule

You are here: **Security Policies & Objects** > **Security Policies**.

To edit a rule:

1. Select an existing rule configuration that you want to edit on the Security Policies page.
2. Click the pencil icon available on the upper right-side of the page.
The Security Policies page appears with inline editable fields. For more information on editing the fields, see "[Add a Rule to a Security Policy](#)" on page 729 .
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[Delete a Security Policy Rule | 747](#)

Delete a Security Policy Rule

You are here: **Security Policies & Objects** > **Security Policies**.

To delete a rule:

1. Select one or more rules that you want to delete on the Security Policies page.
2. Click the delete icon available on the upper-right corner of the page.
3. Click **Yes** to delete the rules or click **No** to retain the rules.

RELATED DOCUMENTATION

[About the Security Policies Page | 721](#)

Configure Captive Portal for Web Authentication and Firewall User Authentication

SUMMARY

Learn how to configure captive portal for Web authentication and firewall user authentication using J-Web.

IN THIS SECTION

- [Overview | 748](#)
- [Workflow | 749](#)
- [Step 1: Create a Logical Interface and Enable Web Authentication | 751](#)
- [Step 2: Create an Access Profile | 757](#)
- [Step 3: Configure Web Authentication Settings | 758](#)
- [Step 4: Create Security Zones and Assign Interfaces to the Zones | 760](#)
- [Step 5: Enable Web or Firewall User Authentication for Captive Portal in the Security Policy | 764](#)
- [Step 6: Verify the Web Authentication and User Authentication Configuration | 771](#)

Overview

What Is Captive Portal?

Captive portal is a method of authenticating devices that need to connect to a network. On an SRX Series Firewalls, you can enable captive portal to redirect Web browser requests to a login page that prompts you to enter your username and password. After successful authentication, you can proceed with the original page request and subsequent network access.

What Is Web Authentication?

With a Web authentication method, you point a browser to an IP address on a device that is enabled for Web authentication. This action initiates an HTTPS session on the IP address that hosts the Web authentication feature on the device. The device then prompts you to enter your username and password, and the result is cached on the device. When the traffic later encounters a Web authentication policy, your access is allowed or denied based on the previous Web authentication results.

You can use other authentication methods as well, but we will not cover those methods in this document. However, we describe each of those methods in brief:

- **Pass-through authentication**—Pass-through user authentication is a form of active authentication. In this method, the device prompts you to enter a username and password. If authentication validates your identity, you are allowed to pass through the firewall and access the requested resources.
- **Pass-through with web-redirect**—When using this authentication method for HTTPS client requests, you can use the web-redirect feature to direct your requests to the device's internal webserver. The webserver sends a redirect HTTPS response to the client system, directing it to reconnect to the webserver for user authentication. The interface that the client's request arrives at is the interface on which the redirect response is sent.

What Is Firewall User Authentication?

A firewall user is a network user who must provide a username and password for authentication when initiating a connection across the firewall. Junos OS enables administrators to restrict or to permit firewall users' access to protected resources (in different zones) behind a firewall based on their source IP address and other credentials. After defining the firewall users, you can create a policy that requires the users to authenticate using one of the three authentication methods (Web, pass-through, or pass-through with web-redirect).

Workflow

IN THIS SECTION

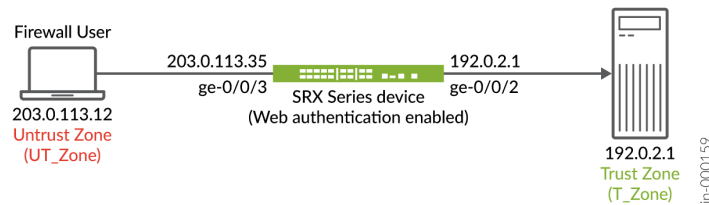
- [Scope | 749](#)
- [Before You Begin | 751](#)

Scope

Here's a sample topology (see [Figure 19 on page 750](#)), which comprises:

- A firewall user's device that acts as a client.
- An SRX Series Firewall that has access to the Internet.
- A network device that acts as an HTTPS server.

Figure 19: Sample Topology



In this sample topology, you'll use J-Web on the SRX Series Firewall to do the following tasks:

NOTE: The values used to configure the sample topology are only examples.

| Step | Action |
|------|--|
| 1 | <p>Create a logical interface on ge-0/0/3, assign it the IP address 203.0.113.35, and enable Web authentication.</p> <p>NOTE: In this example, the firewall user system IP address is 203.0.113.12, which is in the same subnet as 203.0.113.0/24.</p> <p>Create a logical interface on ge-0/0/2 and assign it the IP address 192.0.2.1.</p> <p>NOTE: In this example, the HTTPS server IP address is 192.0.2.1.</p> |
| 2 | Create an access profile (FWAUTH) and define local authentication services. |
| 3 | Configure Web authentication settings to display the successful login message. |
| 4 | Create an untrust (UT_ZONE) and a trust (T_ZONE) zones and assign the ge-0/0/3 and ge-0/0/2 interfaces, respectively. |
| 5 | Configure captive portal for Web authentication and firewall user authentication in the security policy rules (FWAUTH-RULE). |

(Continued)

| Step | Action |
|------|---|
| 6 | Verify that the configured values work for a firewall user: <ul style="list-style-type: none"> • For Web authentication, you'll successfully authenticate using <code>https://203.0.113.35</code>. • For firewall user authentication, you'll successfully authenticate using <code>https://203.0.113.35</code> and then get redirected to <code>https://192.0.2.1</code> for accessing the HTTPS server. |

Before You Begin

- The values used to configure the sample topology are only examples. You can change any details necessary to match your network configuration.
- Ensure that the SRX Series Firewall you use in this example runs Junos OS Release 21.4R1 or later.
- Ensure that your device has the required certificates installed to allow authentication. In this example, we'll use `cert1`, a self-signed certificate.

Step 1: Create a Logical Interface and Enable Web Authentication

In this step, you'll do the following tasks:

- For the `ge-0/0/3` interface on the SRX Series Firewall:
 1. Create a logical interface for an untrust zone.
 2. Assign the IPv4 address `203.0.113.35` to the interface.

NOTE: You'll use the same IP address for enabling captive portal.

3. Enable HTTPS on the interface for Web authentication.
- For the `ge-0/0/2` interface on the SRX Series Firewall:
 1. Create a logical interface for a trust zone.
 2. Assign the IPv4 address `192.0.2.1` to the interface.

You are here (in the J-Web UI): **Network > Connectivity > Interfaces**

To create a logical interface for an untrust zone and to enable Web authentication:

1. Select **ge-0/0/3** and then select **Create > Logical Interface** on the upper-right corner of the Interfaces page.

The Add Logical Interface for ge-0/0/3.0 page appears.

NOTE: You cannot configure captive portal on the fxp0 interface.

2. Specify the following details:

| Field | Action |
|---|--|
| Logical unit number | Type 0 . |
| Description | Type UT_Zone Interface . |
| VLAN ID | This field is not editable. |
| Multi tenancy type | Select None from the list. |
| Logical system | This field is not editable. |
| Zone | Select None from the list. In a later step, we'll create an untrust zone (UT_ZONE) and assign the ge-0/0/3 interface to it. See " Step 4: Create Security Zones and Assign Interfaces to the Zones " on page 760 . |
| Protocol (family) - IPv4 Address | |
| IPv4 Address / DHCP | Select the check box to enable the IPv4 Address/ DHCP configuration. |

(Continued)

| Field | Action |
|--------------|--|
| IPv4 Address | <p>Select IPv4 Address. Then, click + and enter the following details:</p> <ul style="list-style-type: none">• IPv4 Address—Type 203.0.113.35 for Web authentication. <p>NOTE: The captive portal configuration uses the same IPv4 address.</p> <ul style="list-style-type: none">• Subnet—Select 24 using the up or down arrow.• Web Auth:<ul style="list-style-type: none">a. Click Configure.The Web Authentication page appears.b. Select Enable Https dedicated to captive portal.c. Click OK to save changes. |

Add Logical Interface for ge-0/0/3.0

Logical unit number:

Description:

VLAN ID:

Multi tenancy type:

Logical system:

Zone:

Protocol (family):

IPv4 Address

IPv6 Address

Ethernet S...

IPv4 Address / DHCP

DHCP

IPv4 Address

Web Authentication

Enable Http:

Enable Hhttps:

Redirect to Hhttps:

| | IPv4 Address | Subnet | Web Auth | ARP |
|-------------------------------------|--------------|--------|---------------------------|----------------------|
| <input checked="" type="checkbox"/> | 203.0.113.35 | 24 | Configure | Edit |

3. Click **OK** to save the changes.

Good job! You've created a logical interface on ge-0/0/3 with IP address 203.0.113.35 (Web authentication enabled) for your system.

To create a logical interface for a trust zone:

1. Select **ge-0/0/2** and then select **Create > Logical Interface** on the upper-right corner of the Interfaces page.

The Add Logical Interface for ge-0/0/2.0 page appears.

2. Specify the following details:

| Field | Action |
|---|--|
| Logical unit number | Type 0 . |
| Description | Type T_Zone Interface . |
| VLAN ID | This field is not editable. |
| Multi tenancy type | Select None from the list. |
| Logical system | This field is not editable. |
| Zone | Select None from the list. In a later step, we'll create a trust zone (T_ZONE) and assign the ge-0/0/2 interface to it. See " Step 4: Create Security Zones and Assign Interfaces to the Zones " on page 760 . |
| VLAN ID | This field is not editable. |
| Protocol (family) - IPv4 Address | |
| IPv4 Address / DHCP | Select the check box to enable the IPv4 Address/ DHCP configuration. |
| IPv4 Address | <ol style="list-style-type: none"> a. Select IPv4 Address. b. Click +. c. IPv4 Address—Type 192.0.2.1 (HTTPS server). d. Subnet—Select 24 using the up or down arrow. e. Web Auth—Leave as is. f. ARP—Leave as is. |

Add Logical Interface for ge-0/0/2.0

Logical unit number: 0

Description: T_Zone Interface

VLAN ID:

Multi tenancy type: None

Logical system: None

Zone: None

Protocol (family):

IPv4 Address | IPv6 Address | Ethernet Switching

IPv4 Address / DHCP

DHCP

IPv4 Address

| | IPv4 Address | Subnet | Web Auth | ARP |
|-------------------------------------|--------------|--------|---------------------------|----------------------|
| <input checked="" type="checkbox"/> | 192.0.2.1 | 24 | Configure | Edit |

Cancel OK

3. Click **OK** to save the changes.

Good job! You've created a logical interface on ge-0/0/2 with IP address 192.0.2.1 for the HTTPS server.

4. Click **Commit** (at the right-side of the top banner) and select **Commit configuration** to commit the changes now.

The successful-commit message appears.

You can also choose to commit all configuration changes at once, at the end of "[Step 5: Enable Web or Firewall User Authentication for Captive Portal in the Security Policy](#)" on page 764 .

Step 2: Create an Access Profile

Let's create an access profile to define local authentication services. You will use this access profile in Web authentication settings and security policies.

You are here (in the J-Web UI): **Security Services > Firewall Authentication > Access Profile**

To create an access profile:

1. Click the add icon (+) on the upper-right corner of the Access Profile page.

The Create Access Profile page appears.

2. Specify the following details:

| Field | Action |
|-----------------------------|--|
| Name | Type FWAUTH . |
| Address Assignment | (Optional) Select None from the list. You can select an address pool from the list. You can also add a new address pool by clicking Create Address Pool and providing the required values. |
| Authentication | |
| Local | <ol style="list-style-type: none"> a. Select Local to configure the local authentication services. b. Click + and enter the following details on the Create Local Authentication User page: <ol style="list-style-type: none"> i. Username—Type FWClient1. This is the username of the user requesting access. ii. Password—Type \$ABC123. iii. XAUTH IP Address—Leave as is. iv. Group—Leave as is. v. Click OK to save the changes. |
| Authentication Order | |
| Order 1 | Select Local from the list. |

(Continued)

| Field | Action |
|---------|---|
| Order 2 | By default, None is selected. Leave as is. |

The screenshot shows the 'Create Access Profile' configuration interface. The 'Name' field is set to 'FWAUTH'. The 'Address Assignment' is set to 'None'. Under the 'Authentication' section, the 'Local' checkbox is checked. A modal window titled 'Create Local Authentication User' is open, showing fields for 'Username' (FWClient1), 'Password' (masked with asterisks), 'XAUTH IP Address', and 'Group'. The 'Authentication Order' section shows 'Order 1' set to 'Local' and 'Order 2' set to 'None'.

3. Click **OK** to save the changes.

*Good job! You've created the **FWAUTH** access profile.*

4. Click **Commit** (at the right-side of the top banner) and select **Commit configuration** to commit the changes now.

The successful-commit message appears.

You can also choose to commit all configuration changes at once, at the end of "[Step 5: Enable Web or Firewall User Authentication for Captive Portal in the Security Policy](#)" on page 764 .

Step 3: Configure Web Authentication Settings

We'll now assign the created access profile, define a successful-login message, and upload the logo image. You use this image for both Web authentication and captive portal.

You are here (in the J-Web UI): **Security Services > Firewall Authentication > Authentication Settings**

To configure Web authentication settings:

1. Click **Web Authentication Settings**.
2. Do the following:
 - **Default Profile**—Select **FWAUTH** from the list. The security policies use this profile to authenticate users.
 - **Success**—Type **Authentication Success** as the message to be displayed for users who log in successfully.
3. (Optional) To upload a customized logo:
 - a. Click **Logo Image Upload**.
 - b. Click **Browse** for uploading a logo file.
 - c. Select a logo image and then click **OK**.

NOTE: For a good logo, the image must be in the **.gif** format and the resolution must be 172x65.

- d. Click **Sync** to apply the logo.

The uploaded image will now appear on the captive portal login page or the Web authentication login page.

Authentication Settings ⓘ

Warning: To edit this page, atleast one access profile to be configured under "Security Services / Firewall Authentication / Access Profile" ↗️ ⌂ Cancel Save

> Pass Through Settings ⓘ ⚙️

Pass-through firewall authentication settings

▼ Web Authentication Settings

Default Profile ⓘ

Success ⓘ
max char 250

▼ Logo Image Upload

To achieve good look and feel, it is better that the image size is 172 * 65

Logo File

4. Click **Save** on the upper-right corner of the Authentication Settings page to save the changes.
Congratulations! You've successfully saved your Web authentication settings.
5. Click **Commit** (at the right-side of the top banner) and select **Commit configuration** to commit the changes now.

The successful-commit message appears.

You can also choose to commit all configuration changes at once, at the end of "[Step 5: Enable Web or Firewall User Authentication for Captive Portal in the Security Policy](#)" on page 764 .

Step 4: Create Security Zones and Assign Interfaces to the Zones

You create a security zone to define one or more network segments that regulate inbound and outbound traffic through policies.

We'll now separately create:

- An untrust zone (UT_ZONE) and assign the ge-0/0/3 interface to it.
- A trust zone (T_ZONE) and assign the ge-0/0/2 interface to it.

You are here (in the J-Web UI): **Security Policies & Objects > Zones/Screens**

To create UT_ZONE (untrust zone) and T_ZONE (trust zone) and to assign the defined interfaces to the zones:

1. Click the add icon (+) on the upper-right corner of the Zone List page.

The Add Zone page appears.

2. Specify the following details:

| Field | Action |
|----------------------|--|
| Main | |
| Zone name | <ul style="list-style-type: none"> • Type UT_ZONE for an untrust zone. • Type T_ZONE for a trust zone. |
| Zone description | <ul style="list-style-type: none"> • Type untrust zone for UT_ZONE. • Type trust zone for T_ZONE. |
| Zone type | Select Security . |
| Application Tracking | Leave as is. |
| Source Identity Log | Leave as is. |

(Continued)

| Field | Action |
|-------------------------|---|
| Traffic Control Options | Leave as is. |
| Interfaces | <ul style="list-style-type: none"> For UT_ZONE, select ge-0/0/3.0 from the Available column and click the right arrow to move it to the Selected column. For T_ZONE, select ge-0/0/2.0 from the Available column and click the right arrow to move it to the Selected column. |

Add Zone

Main | Host Inbound Traffic - Zone | Host Inbound Traffic - Interface

Zone Name *

Zone Description

Zone Type * Security Functional

Application Tracking

Source Identity Log

Traffic Control Options

Send RST for Non Matching Session

Binding Screen

Interfaces

| Available | | Selected |
|----------------------|--------|------------|
| ge-0/0/2.0 fxp0.0 | > < | ge-0/0/3.0 |

Cancel OK

Add Zone

Main
Host Inbound Traffic - Zone
Host Inbound Traffic - Interface

Zone Name *

Zone Description

Zone Type *

Security
 Functional

Application Tracking

Source Identity Log

Traffic Control Options

Send RST for Non Matching Session

Binding Screen

Interfaces

| Available | | Selected |
|------------|---|------------|
| ge-0/0/3.0 | > | ge-0/0/2.0 |
| fxp0.0 | < | |

Cancel
OK

| Field | Action (Sample Value) |
|-----------------------------|-----------------------|
| Host Inbound Traffic - Zone | Leave as is. |

Host Inbound Traffic - Interface

| | |
|---------------------|---|
| Selected Interfaces | <ul style="list-style-type: none"> For UT_ZONE, select ge-0/0/3.0. For T_ZONE, select ge-0/0/2.0. |
| Available Services | Select all from the Available Services column and click the right arrow to move it to the Selected column. |

(Continued)

| Field | Action (Sample Value) |
|---------------------|--|
| Available Protocols | Select all from the Available Protocols column and click the right arrow to move it to the Selected column. |

Add Zone

Main | Host Inbound Traffic - Zone | Host Inbound Traffic - Interface

Selected Interfaces

ge-0/0/3.0

Available Services

- all
- bootp
- dhcp
- dhcpv6
- dns
- finger
- ftp
- ident-reset

>

Selected

- all

<

Available Protocols

- all
- bfd
- bgp
- dvmp
- igmp
- ldp
- msdp
- nhrp

>

Selected

- all

<

Cancel | OK

Add Zone

The screenshot shows the 'Add Zone' configuration window. The 'Host Inbound Traffic - Interface' tab is selected. The 'Selected Interfaces' list contains 'ge-0/0/2.0'. The 'Available Services' list includes 'all', 'bootp', 'dhcp', 'dhcpv6', 'dns', 'finger', 'ftp', and 'ident-reset'. The 'Selected' list for services contains 'all'. The 'Available Protocols' list includes 'all', 'bfd', 'bgp', 'dvmrp', 'igmp', 'ldp', 'msdp', and 'nhp'. The 'Selected' list for protocols contains 'all'. The 'OK' button is highlighted in blue.

3. Click **OK** to save the changes.

Good job! You have assigned the ge-0/0/3 interface to UT_ZONE and ge-0/0/2 to T_ZONE.

4. Click **Commit** (at the right-side of the top banner) and select **Commit configuration** to commit the changes now.

The successful-commit message appears.

You can also choose to commit all configuration changes at once, at the end of "[Step 5: Enable Web or Firewall User Authentication for Captive Portal in the Security Policy](#)" on page 764 .

Step 5: Enable Web or Firewall User Authentication for Captive Portal in the Security Policy

We'll now enable captive portal in the security policy rules to redirect a client HTTPS request to the internal HTTPS server of the device.

You are here (in the J-Web UI): **Security Policies & Objects > Security Policies**

To configure security policy rule for captive portal:

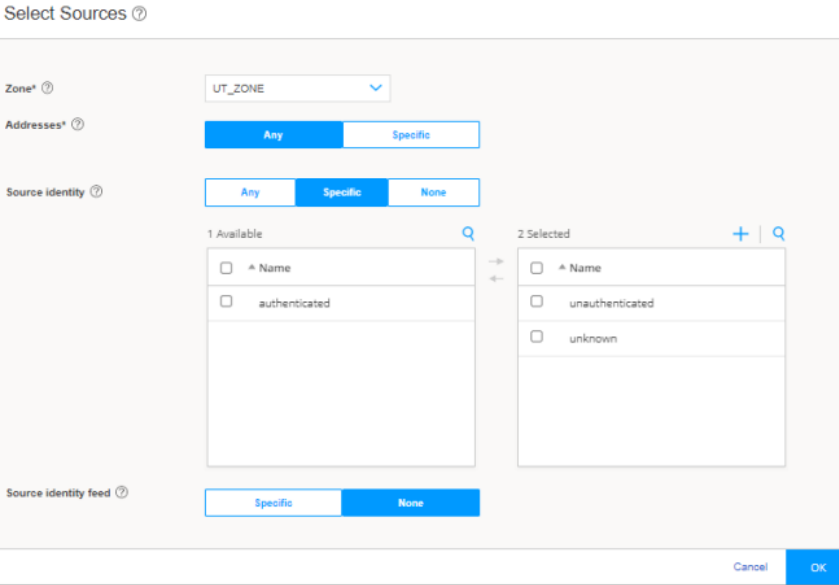
1. Click the add icon (+) on the upper-right corner of the Security Policies page.

The inline editable fields appear.

2. Specify the following details:

| Field | Action |
|--------------------|--|
| Rule Name | |
| Name | Type FWAUTH-RULE . |
| Description | Type Test rule . |
| Source Zone | |
| + | Click + to add a source zone. The Select Sources page appears. |

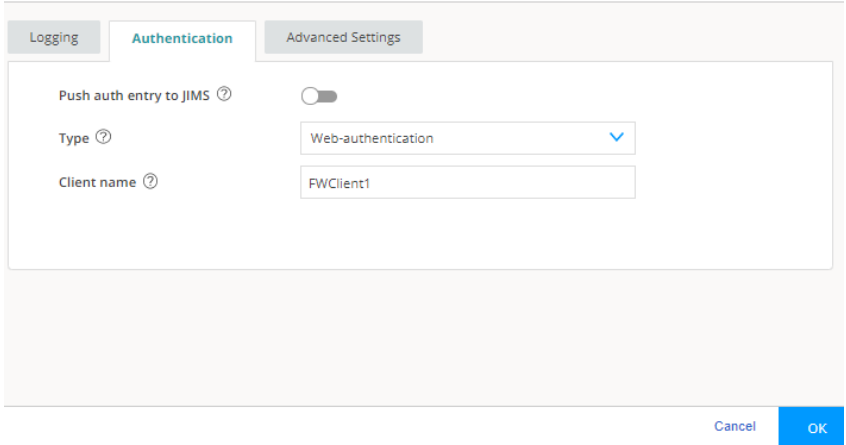
(Continued)

| Field | Action |
|-------------------------|---|
| Select Sources | <p>Specify the following details:</p> <ol style="list-style-type: none"> Zone—Select UT_ZONE from the list to which you want the rule to be associated. Addresses—By default, Any is selected. Leave as is. Source identity: <ul style="list-style-type: none"> For Web authentication, select None. For firewall user authentication, select Specific. Then select unauthenticated and unknown from the Available column and click the right arrow to move these values to the Selected column. Source identity feed—Select None.  <ol style="list-style-type: none"> Click OK to save the changes. |
| Destination Zone | |
| + | <p>Click + to add a destination zone.</p> <p>The Select Destination page appears.</p> |

(Continued)

| Field | Action |
|---------------------|--|
| Select Destination | <p>Specify the following details:</p> <ul style="list-style-type: none"> a. Zone—Select T_ZONE from the list to which you want the rule to be associated. b. Addresses—By default, Any is selected. Leave as is. c. Dynamic applications—Select None. <p>NOTE: You cannot configure dynamic applications with Web authentication.</p> <ul style="list-style-type: none"> d. Services—Select Any. e. URL category—Select None. f. Destination identity feed—Select None. <div data-bbox="581 856 1421 1276" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Select Destination ?</p> <p>Zone* ? <input type="text" value="T_ZONE"/></p> <p>Addresses* ? <input checked="" type="radio"/> Any <input type="radio"/> Specific</p> <p>Dynamic applications ? <input type="radio"/> Any <input type="radio"/> Specific <input checked="" type="radio"/> None</p> <p>Services ? <input checked="" type="radio"/> Any <input type="radio"/> Specific <input type="radio"/> None</p> <p>URL category ? <input type="radio"/> Any <input type="radio"/> Specific <input checked="" type="radio"/> None</p> <p>Destination identity feed ? <input type="radio"/> Specific <input checked="" type="radio"/> None</p> <p style="text-align: right;"><input type="button" value="Cancel"/> <input checked="" type="button" value="OK"/></p> </div> <ul style="list-style-type: none"> g. Click OK to save the changes. |
| Action | Select Permit . |
| Advanced Services | Leave as is. |
| Rule Options | |
| + | <p>Click + to select rule options.</p> <p>The Select Rule Options page appears.</p> |

(Continued)

| Field | Action |
|--|--|
| Logging | Leave as is. |
| <p>Authentication</p> <p>NOTE: Use this configuration for <i>Web authentication</i> only.</p> | <p>Specify the following details:</p> <ul style="list-style-type: none"> • Push auth entry to JIMS—By default, this option is disabled. Leave as is. • Type—Select Web-authentication from the list. • Client name—Type FWClient1. • Click OK to save the changes. <p>Select Rule Options ?</p>  |

(Continued)

| Field | Action |
|--|--|
| <p>Authentication</p> <p>NOTE: Use this configuration for <i>firewall user authentication</i> only.</p> | <p>Specify the following details:</p> <ul style="list-style-type: none"> • Push auth entry to JIMS—By default, this option is disabled. Leave as is. • Type—Select User-firewall from the list. • Access profile—Select FWAUTH from the list. • Domain—Leave as is. • Web redirect (http)—By default, this option is disabled. Leave as is. • Captive Portal—Enable to redirect a client HTTPS request to the webserver for user authentication. <ul style="list-style-type: none"> • Interface—Select ge-0/0/3.0 (203.0.113.35/24) from the list for the webserver where the client HTTPS request is redirected. This is the same interface that you configured while enabling Web authentication. • IP address—Type 203.0.113.35 for the webserver where the client HTTPS request is redirected. This is the same IPv4 address that you configured while enabling Web authentication on the ge-0/0/3 Interface. • SSL Termination Profile—Select SSL_termination (cert1) from the list for SSL termination support service. Acting as an SSL proxy server, the SRX Series Firewall uses the SSL termination process to terminate the client's SSL session. • Auth only browser—By default, this option is disabled. Leave as is. • User agents—Leave as is. • Click OK to save the changes. |

(Continued)

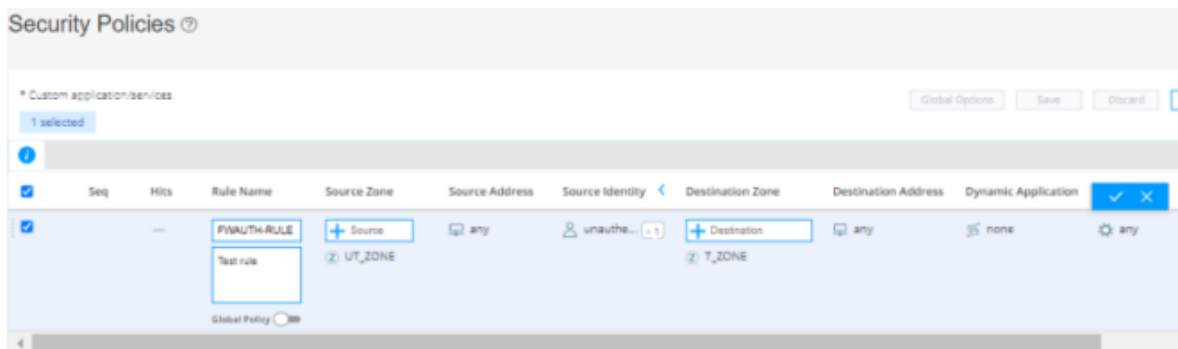
| Field | Action |
|-------|---|
| | <div data-bbox="581 359 1419 1199"> <p>Select Rule Options ⓘ</p> <p>Logging Authentication Advanced Settings</p> <p>Push auth entry to IIMS ⓘ <input type="checkbox"/></p> <p>Type ⓘ User-firewall <input type="text"/></p> <p>Access Profile** ⓘ PWAUTH <input type="text"/> Add</p> <p>Domain ⓘ Domain <input type="text"/></p> <p>Web redirect (http) ⓘ <input type="checkbox"/></p> <p>Captive Portal ⓘ <input checked="" type="checkbox"/></p> <p>Interface* ⓘ ge-0/0/3.0 (203.0.113.35/24) <input type="text"/></p> <p>IPv4 Address* ⓘ 203.0.113.35 <input type="text"/></p> <p>SSL Termination Profile SSL_termination (cert1) <input type="text"/> Add</p> <p>Auth only browser ⓘ <input type="checkbox"/></p> <p>User agents ⓘ <input type="text"/> +</p> <p><input type="text"/> X</p> <p>Cancel <input type="button" value="OK"/></p> </div> |

3. Click the tick icon

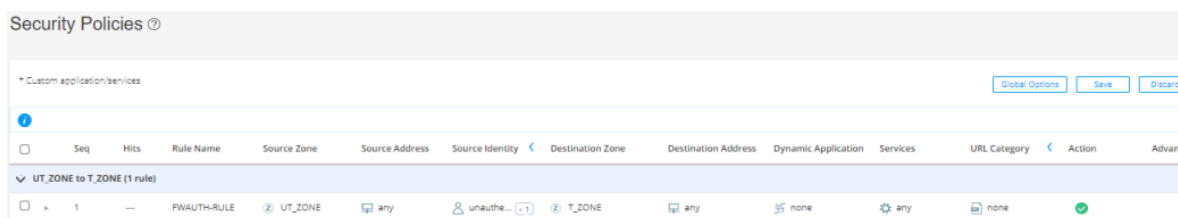


on the right-side of the row after you're done with the configuration.

NOTE: Slide the horizontal bar backward if the inline tick and cancel icons are not available when creating a new rule.



- Click **Save** on the upper-right corner of the Security Policies page to save changes.



- Click **Commit** (at the right side of the top banner) and select **Commit configuration**.

The successful-commit message appears.

Congratulations! You've successfully committed your configuration changes. You are all set with the Web or firewall user authentication policy.

Step 6: Verify the Web Authentication and User Authentication Configuration

IN THIS SECTION

- Purpose | 771
- Action | 772
- What's Next | 774

Purpose

The final step! Let's see whether your configuration works for a firewall user:

- For Web authentication, you'll successfully authenticate using <https://203.0.113.35>. This is the same IPv4 address that you configured in "[Step 1: Create a Logical Interface and Enable Web Authentication](#)" on page 751 .
- For firewall user authentication, you'll successfully authenticate using <https://203.0.113.35> and then get redirected to <https://192.0.2.1> for accessing the HTTPS server. These are the same IPv4

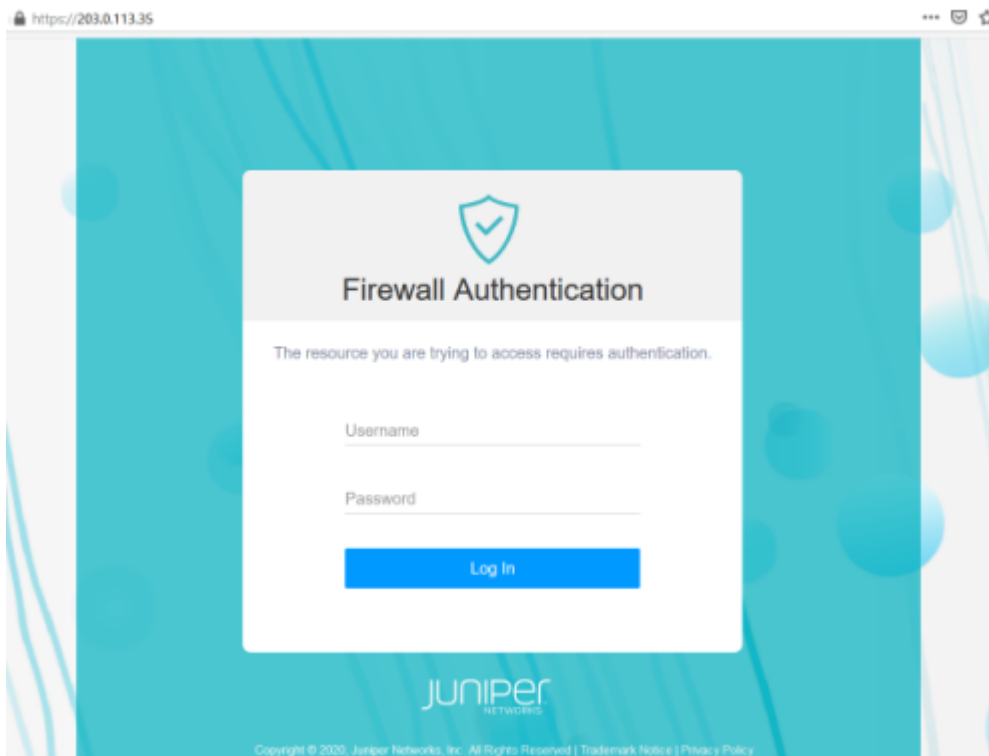
addresses that you configured in ["Step 1: Create a Logical Interface and Enable Web Authentication"](#) on page 751 .

Action

To verify the Web authentication configuration:

1. Type **https://203.0.113.35** in your Web browser.

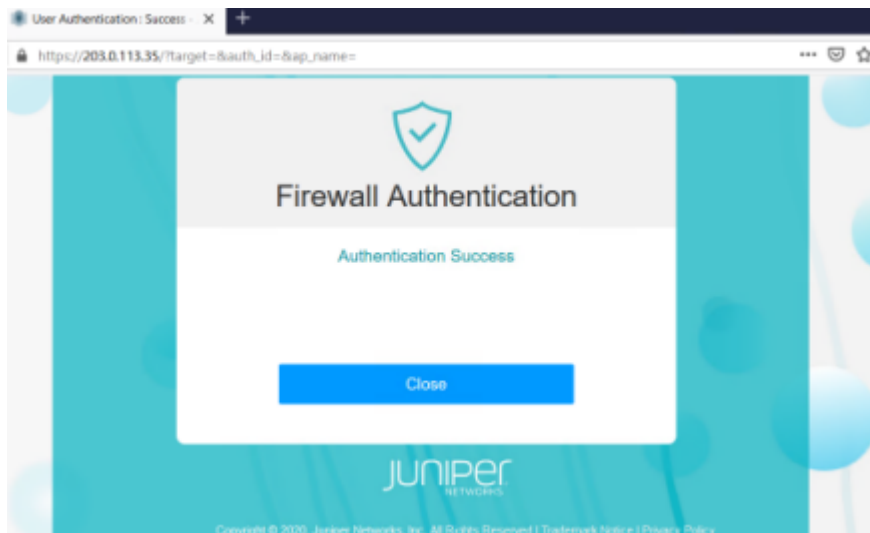
The Firewall Authentication login page appears.



2. Type the following credentials, and then click **Log In**.

- Username—**FWClient1**
- Password—**\$ABC123**

Congratulations! You are successfully authenticated. You can also see the success message *Authentication Success* that you configured.

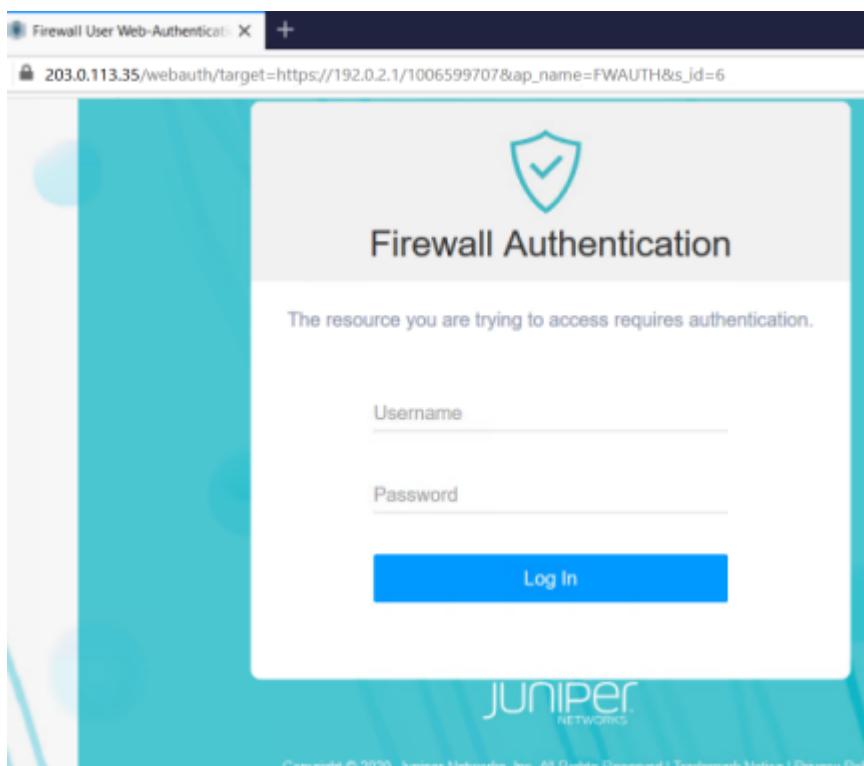


3. Click **Close**.

To verify firewall user authentication:

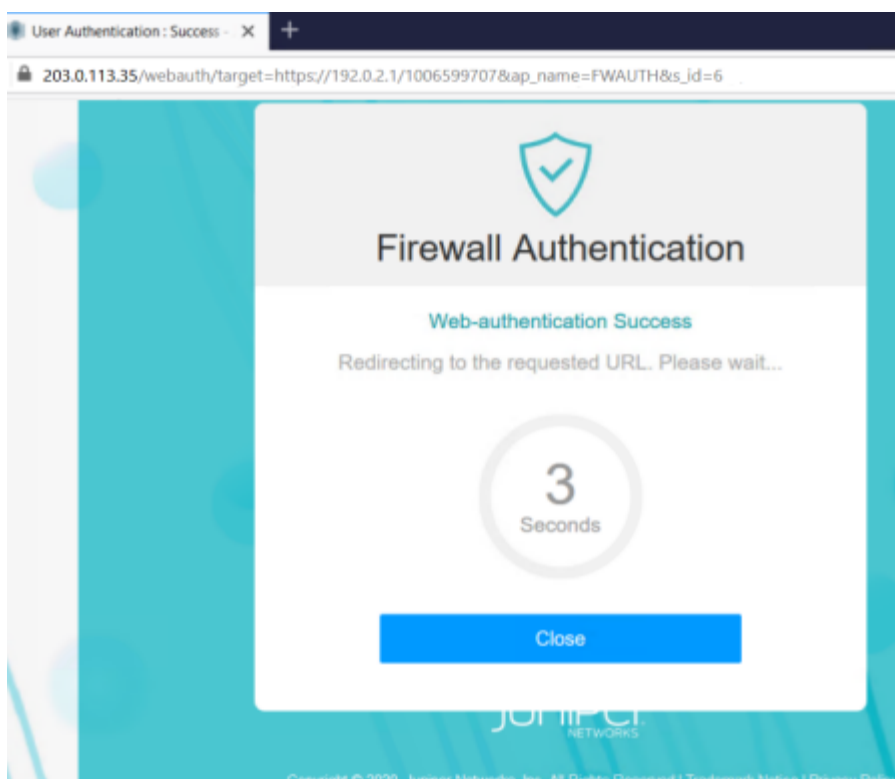
1. Type **https://192.0.2.1** in your Web browser.

You are redirected to **https://203.0.113.35** for Web authentication.



2. Type the following credentials, and then click **Log In**.

- Username—FWClient1
- Password—\$ABC123



Congratulations! You are successfully authenticated. Soon, you'll be redirected to <https://192.0.2.1>, and you'll be able to access the HTTPS server.

What's Next

To keep going, visit the [J-Web for SRX Series Documentation](#) page in the Juniper TechLibrary.

Metadata Streaming Policy

IN THIS CHAPTER

- [About the Metadata Streaming Policy Page | 775](#)
- [Create a Metadata Streaming Policy | 777](#)
- [Edit a Metadata Streaming Policy | 778](#)
- [Delete a Metadata Streaming Policy | 779](#)

About the Metadata Streaming Policy Page

IN THIS SECTION

- [Benefits of Metadata Streaming | 776](#)
- [Tasks You Can Perform | 776](#)
- [Field Descriptions | 777](#)

You are here: **Security Policies & Objects > Metadata Streaming Policy.**

Configure a security metadata streaming policy on SRX Series Firewalls to send a network traffic metadata and connection patterns to Juniper ATP Cloud. Using DNS, a metadata streaming profile protects and defends your network from advanced threats. You must assign the metadata streaming profile to the metadata streaming policy. For more information on the metadata streaming profile, see ["About the Metadata Streaming Profile Page" on page 1020](#) . After configuring the metadata streaming policy, assign it to the security policy at zone-level.

Domain Name System (DNS) Domain Generation Algorithm (DGA) generates seemingly random domain names that are used as rendezvous points with potential C&C servers. DNS DGA detection uses machine learning models as well as known pre-computed DGA domain names to provides domain verdicts, which helps in-line DNS query blocking and sinkholing on SRX Series Firewalls.

Encrypted Traffic Insights (ETI) detects malicious threats that are hidden in encrypted traffic without intercepting and decrypting the traffic.

Benefits of Metadata Streaming

- Provide all SRX Series Firewalls with a SaaS-based, high-performance, and low-overhead solution.
- Deploy easily to existing SRX environments.
- SRX can detect and act on Domain Name System (DNS) without any sensors.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a metadata streaming policy. See ["Create a Metadata Streaming Policy" on page 777](#) .
- Edit a metadata streaming policy. See ["Edit a Metadata Streaming Policy" on page 778](#) .
- Delete a metadata streaming policy. See ["Delete a Metadata Streaming Policy" on page 779](#) .
- Show or hide columns in the Metadata Streaming Policy table. To do this, use the Show Hide Columns icon in the upper-right corner of the page and select the options to show or deselect to hide options on the page.
- Advanced search for metadata streaming policies. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

For an advanced search:

1. Enter the search string in the text box.

Based on your input, a list of items from the filter context menu appears.

2. Select a value from the list and then select a valid operator to perform the advanced search operation.

NOTE: Press Spacebar to add an AND operator or an OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.

3. Press Enter to display the search results in the grid.

Field Descriptions

Table 220 on page 777 describes the fields on the Metadata Streaming Policy page.

Table 220: Fields on the Metadata Streaming Policy Page

| Field | Description |
|----------------------------|--|
| Source Zone | Displays the name of the source zone associated with the metadata streaming policy. |
| Destination Zone | Displays the name of the destination zone associated with the metadata streaming policy. |
| Metadata Streaming Profile | Displays the name of the metadata streaming profile associated with the metadata streaming policy. |

RELATED DOCUMENTATION

[Create a Metadata Streaming Policy | 777](#)

Create a Metadata Streaming Policy

You are here: **Security Policies & Objects > Metadata Streaming Policy.**

Create a metadata streaming policy to associate a metadata streaming profile with the zone-level.

To create a metadata streaming policy:

1. Click + available on the upper-right corner of the Metadata Streaming Policy page.
The inline editable fields will appear.
2. Complete the configuration according to the guidelines provided in [Table 221 on page 778](#).
3. Click the tick icon on the upper right of the row once done with the configuration.

Table 221: Fields on the Metadata Streaming Policy Page

| Field | Action |
|----------------------------|---|
| Source Zone | Select a source zone from the list to associate it with the metadata streaming policy. |
| Destination Zone | Select a destination zone from the list to associate it with the metadata streaming policy. |
| Metadata Streaming Profile | <p>Select a metadata streaming profile from the list to associate it with the zone-level.</p> <p>To create a metadata streaming profile inline, click Create Metadata Streaming Profile available in the list. For information on creating the profile, see "Create a Metadata Streaming Profile" on page 1023 .</p> |

RELATED DOCUMENTATION

[About the Metadata Streaming Policy Page | 775](#)

[Edit a Metadata Streaming Policy | 778](#)

[Delete a Metadata Streaming Policy | 779](#)

Edit a Metadata Streaming Policy

You are here: **Security Policies & Objects > Metadata Streaming Policy.**

To edit a metadata streaming policy:

1. Select an existing policy configuration to edit on the Metadata Streaming Policy page.
2. Click the pencil icon available on the upper-right corner of the page.

The Metadata Streaming Policy page opens with inline editable fields. For more information on editing the fields, see ["Create a Metadata Streaming Policy" on page 777](#) .

3. Click the tick icon on the upper right of the row to save the edited configuration.

RELATED DOCUMENTATION

[About the Metadata Streaming Policy Page | 775](#)

[Create a Metadata Streaming Policy | 777](#)

[Delete a Metadata Streaming Policy | 779](#)

Delete a Metadata Streaming Policy

You are here: **Security Policies & Objects** > **Metadata Streaming Policy**.

To delete metadata streaming policies:

1. Select one or more policy configuration to delete on the Metadata Streaming Policy page.
2. Click the delete icon available on the upper-right corner of the page.
3. Click **Yes** to delete the policy configuration or click **No** to retain the policy configuration.

RELATED DOCUMENTATION

[About the Metadata Streaming Policy Page | 775](#)

[Create a Metadata Streaming Policy | 777](#)

[Edit a Metadata Streaming Policy | 778](#)

Zones/Screens

IN THIS CHAPTER

- [About the Zones/Screens Page | 780](#)
- [Add a Zone | 782](#)
- [Edit a Zone | 785](#)
- [Delete a Zone | 785](#)
- [Add a Screen | 785](#)
- [Edit a Screen | 796](#)
- [Delete a Screen | 797](#)

About the Zones/Screens Page

IN THIS SECTION

- [Tasks You Can Perform | 780](#)
- [Field Descriptions | 781](#)

You are here: **Security Policies & Objects > Zones/Screens.**

Use this page to configure zones and screens.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a Zone. See ["Add a Zone" on page 782](#) .
- Edit a Zone. See ["Edit a Zone" on page 785](#) .

- Delete Zone. See ["Delete a Zone" on page 785](#) .
- Add a Screen. See ["Add a Screen" on page 785](#) .
- Edit a Screen. See ["Edit a Screen" on page 796](#) .
- Delete Screen. See ["Delete a Screen" on page 797](#) .

Field Descriptions

[Table 222 on page 781](#) describes the fields on Zones/Screens page.

Table 222: Fields on Zones/Screens Page

| Field | Description |
|------------------------|--|
| Zone List | |
| Zone name | Displays the name of the zone. |
| Type | Displays the type of zone. |
| Host-inbound Services | Displays the services that permit inbound traffic. |
| Host-inbound Protocols | Displays the protocol that permit inbound 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. |

Table 222: Fields on Zones/Screens Page (Continued)

| Field | Description |
|-------------|---------------------------------------|
| Description | Displays a description of the screen. |

RELATED DOCUMENTATION

[Add a Zone](#) | 782

Add a Zone

You are here: **Security Policies & Objects > Zones/Screens.**

To add a zone:

1. Click **+** available on the upper-right corner of the Zone List page.
The Add Zone page appears.
2. Complete the configuration according to the guidelines provided in [Table 223 on page 782](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 223: Fields on the Add Zone page

| Field | Action |
|----------------------|---|
| Main | |
| Zone name | Enter a name for the zone. |
| Zone description | Enter a description for the zone. |
| Zone type | Select a zone type: Security or Functional. |
| Application Tracking | Select the check box to enable application tracking support for the zone. |

Table 223: Fields on the Add Zone page (*Continued*)

| Field | Action |
|------------------------------------|---|
| Source Identity Log | Select the check box to enable it to trigger user identity logging when that zone is used as the source zone (from-zone) in a security policy. |
| Traffic Control Options | <p>Enter the following details:</p> <ul style="list-style-type: none"> Send RST for Non Matching Session—Select the check box to enable this option. 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. Binding Screen—Select a binding screen from the list. NOTE: If you have already configured screens, the list shows the screen names and allows you to select or delete a screen. |
| Interfaces | <p>Select interfaces from the Available column and move it to the Selected column using the arrow to include in the security zone.</p> <p>Starting in Junos OS Release 19.4R1, J-Web supports Wi-Fi Mini-PIM for SRX320, SRX340, SRX345, and SRX550M devices. The physical interface for the Wi-Fi Mini-PIM uses the name wl-x/0/0, where x identifies the slot on the services gateway where the Mini-PIM is installed.</p> |
| Host inbound traffic - Zone | |
| Protocols | <p>Specifies the protocols that permit inbound traffic of the selected type to be transmitted to hosts within the zone.</p> <p>Select the protocols from the Available column and move it to the Selected column using the right arrow.</p> <p>Select all to permit all protocols.</p> <p>NOTE: 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 223: Fields on the Add Zone page (Continued)

| Field | Action |
|---|--|
| Services | <p>Specifies the interface services that permit inbound traffic of the selected type to be transmitted to hosts within the zone.</p> <p>Select the services from the Available column and move it to the Selected column using the right arrow.</p> <p>Select all to permit all services.</p> <p>NOTE: To deselect services, select the services in the Selected column and then use the left arrow to move them to the Available column.</p> |
| Host inbound traffic - Interface | |
| Selected Interfaces | Displays the list of selected interfaces. |
| Interface Services | <p>Specifies the interfaced services that permit inbound traffic from the selected interface to be transmitted to hosts within the zone.</p> <p>Select the interface services from the Available column and move it to the Selected column using the right arrow. Select all to permit all interface services.</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 | <p>Specifies the interfaced protocols that permit inbound traffic from the selected interface to be transmitted to hosts within the zone.</p> <p>Select the interface protocols from the Available column and move it to the Selected column using the right arrow. Select all to permit all interface protocols.</p> |

RELATED DOCUMENTATION

[Edit a Zone](#) | 785

Edit a Zone

You are here: **Security Policies & Objects > Zones/Screens.**

To edit a zone:

1. Select an existing zone configuration that you want to edit on the Zones/Screens page.
2. Click the pencil icon available on the upper-right corner of the Zone List page.

The Edit Zone page appears with editable fields. For more information on the options, see "[Add a Zone](#)" on page 782 .

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

| [Delete a Zone](#) | 785

Delete a Zone

You are here: **Security Policies & Objects > Zones/Screens.**

To delete a zone:

1. Select a zone that you want to delete on the Zones/Screens page.
2. Click the delete icon available on the upper-right corner of the Zone List page.

A confirmation window appears.

3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

| [Add a Screen](#) | 785

Add a Screen

You are here: **Security Policies & Objects > Zones/Screens.**

To add a screen:

1. Click **+** available on the upper-right corner of the Screen List page.
The Add Screen page appears.
2. Complete the configuration according to the guidelines provided in [Table 224 on page 786](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

[Table 224 on page 786](#) describes the fields on the Add Screen page.

Table 224: Fields on the Add Screen Page

| Field | Action |
|---|---|
| Main | |
| Screen name | Enter a name for the screen object. |
| Screen description | Enter a description for the screen object. |
| Generate alarms without dropping packet | Select the check box to enable this feature. |
| IP spoofing | Select the check box to enable this feature. 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. |
| IP sweep | Select the check box to enable this feature. Specifies the number of ICMP address sweeps. An IP address sweep can occur with the intent of triggering responses from active hosts. |
| Threshold | 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. Range: 1000 through 1000000 microseconds. The default value is 5000 microseconds. |

Table 224: Fields on the Add Screen Page (Continued)

| Field | Action |
|----------------------------|---|
| Port scan | <p>Select the check box to enable this feature.</p> <p>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.</p> |
| Threshold | <p>Enter the time interval for a TCP port scan.</p> <p>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.</p> <p>Range: 1000 through 1000000 microseconds. The default value is 5000 microseconds.</p> |
| MS-Windows Defense | <p>WinNuke attack protection—Select the check box to enable this feature.</p> <p>NOTE: WinNuke is a DoS attack targeting any computer on the Internet running Windows operating system.</p> |
| IPv6 Check | <p>Enter the following details:</p> <ul style="list-style-type: none"> • Malformed IPv6—Select this check box to enable the IPv6 malformed header intrusion detection service (IDS) option. • Malformed ICMPv6—Select this check box to enable the ICMPv6 malformed IDS option. |
| Denial of Service | |
| Land attack protection | <p>Select the check box to enable this feature.</p> <p>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.</p> |
| Teardrop attack protection | <p>Select the check box to enable this feature.</p> <p>NOTE: Teardrop attacks exploit the reassembly of fragmented IP packets.</p> |
| ICMP fragment protection | <p>Select the check box to enable this feature.</p> <p>NOTE: ICMP packets contain very short messages. There is no legitimate reason for ICMP packets to be fragmented.</p> |

Table 224: Fields on the Add Screen Page *(Continued)*

| Field | Action |
|-----------------------------------|--|
| Ping of death attack protection | <p>Select the check box to enable this feature.</p> <p>NOTE: A ping of death occurs when IP packets are sent that exceed the maximum legal length (65,535 bytes).</p> |
| Large size ICMP packet protection | <p>Select the check box to enable this feature.</p> |
| Block fragment traffic | <p>Select the check box to enable this feature.</p> |
| SYN-ACK-ACK proxy protection | <p>Select the check box to enable this feature.</p> |
| Threshold | <p>Enter the threshold value for SYN-ACK-ACK proxy protection.</p> <p>NOTE: The range is from 1 through 250000 sessions. The default value is 512 sessions.</p> |
| Anomalies | |

Table 224: Fields on the Add Screen Page *(Continued)*

| Field | Action |
|-------|--|
| IP | <p>Enter the following details:</p> <ul style="list-style-type: none"> • Bad option—Select the check box to specify the number of bad options counter. • Security—Select the check box to enable the method for hosts to send security. • Unknown protocol—Select the check box to enable the IP address with security option. • Strict source route—Select the check box to enable the complete route list for a packet to take on its journey from source to destination. • Source route—Select the check box to enable this feature. <p>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.</p> <ul style="list-style-type: none"> • Timestamp—Select the check box to enable the time recorded (in UTC) when each network device receives the packet during its trip from the point of origin to its destination. • Stream—Select the check box to enable a method for the 16-bit SATNET stream identifier to be carried through networks that do not support streaming. • Loose source route—Select the check box to enable a partial route list for a packet to take on its journey from source to destination. • Record route—Select the check box to enable that IP addresses of network devices along the path that the IP packet travels can be recorded. |

Table 224: Fields on the Add Screen Page (Continued)

| Field | Action |
|--|---|
| TCP | <p>Enter the following details:</p> <ul style="list-style-type: none"> • SYN Fragment Protection—Select the check box to enable the number of TCP SYN fragments. • SYN and FIN Flags Set Protection—Select the check box to enable the number of TCP SYN and FIN flags. <p>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.</p> <ul style="list-style-type: none"> • FIN Flag Without ACK Flag Set Protection—Select the check box to enable the number of TCP FIN flags set without an ACK flag set. • TCP Packet Without Flag Set Protection—Select the check box to enable the number of TCP headers without flags set. <p>NOTE: A normal TCP segment header has at least one flag control set.</p> |
| Flood Defense | |
| Limit sessions from the same source | <p>Enter the range within which the sessions are limited from the same source IP.</p> <p>Range: 1 through 50000 sessions.</p> |
| Limit sessions from the same destination | <p>Enter the range within which the sessions are limited from the same destination IP. The range is from 1 through 50000 sessions.</p> <p>Range: 1 through 8000000 sessions per second. The default value is 128 sessions.</p> |
| ICMP flood protection | <p>Select the check box to enable the Internet Control Message Protocol (ICMP) flood counter.</p> <p>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.</p> |
| Threshold | <p>Enter the threshold value for ICMP flood protection.</p> <p>NOTE: Range: 1 through 4000000 ICMP pps.</p> |

Table 224: Fields on the Add Screen Page *(Continued)*

| Field | Action |
|----------------------|---|
| UDP flood protection | Select the check box to enable the User Datagram Protocol (UDP) flood counter. 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. |
| Threshold | Enter the threshold value for UDP flood protection. NOTE: Range: 1 through 100000 session. The default value is 1000 sessions. |

Table 224: Fields on the Add Screen Page *(Continued)*

| Field | Action |
|----------------------|--|
| UDP allowlist | <ol style="list-style-type: none"> 1. Click Select. The UDP Allowlist window appears. 2. Click + to add IP addresses that you wish to allowlist. The Add Allowlist window appears. 3. Enter the following details: <ul style="list-style-type: none"> • Name—Enter a Name to identify the group of IP addresses. • IPv4/IPv6 Address—Enter IPv4 or IPv6 address. • IPv4/IPv6 Address(es)—Lists the address that you have entered. <p>NOTE: You can select the IP address and click X to delete it.</p> 4. Click OK to save the changes. 5. Select the allowlist name in the UDP Allowlist page that you associated with the group of IP addresses that you entered in the Add Allowlist window from the Available column and move it to the Selected column using the right arrow. 6. Click OK to save the changes. <p>NOTE:</p> <ul style="list-style-type: none"> • The UDP Allowlist option is enabled only if you select UDP flood protection. • The allowlist that you created in the UDP Allowlist window will be available in the TCP Allowlist window also for selection. <p>To edit an allowlist in the UDP Allowlist page, select the allowlist name and click on the pencil icon.</p> <p>To delete an allowlist in the UDP Allowlist page, select the allowlist name and click on the delete icon.</p> |
| SYN flood protection | <p>Select the check box to enable all the threshold and ager timeout options.</p> <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> |

Table 224: Fields on the Add Screen Page *(Continued)*

| Field | Action |
|------------------|--|
| TCP allowlist | <ol style="list-style-type: none"> 1. Click Select. The TCP Allowlist window appears. 2. Click + to add IP addresses that you wish to allowlist. The Add Allowlist window appears. 3. Enter the following details: <ul style="list-style-type: none"> • Name—Enter a Name to identify the group of IP addresses. • IPv4/IPv6 Address—Enter IPv4 or IPv6 address. • IPv4/IPv6 Address(es)—Lists the address that you have entered. <p>NOTE: You can select the IP address and click X to delete it.</p> 4. Click OK to save the changes. 5. Select the allowlist name in the TCP Allowlist page that you associated with the group of IP addresses that you entered in the Add Allowlist window from the Available column and move it to the Selected column using the right arrow. 6. Click OK to save the changes. <p>NOTE:</p> <ul style="list-style-type: none"> • The TCP Allowlist option is enabled only if you select SYN flood protection. • The allowlist that you created in the TCP allowlist window will be available in the UDP Allowlist window also for selection. <p>To edit a allowlist in the TCP Allowlist page, select the allowlist name and click on the pencil icon.</p> <p>To delete a allowlist in the TCP Allowlist page, select the allowlist name and click on the delete icon.</p> |
| Attack threshold | <p>Enter a value to specify the number of SYN packets per second required to trigger the SYN proxy mechanism.</p> <p>NOTE: Range: 1 through 1000000 proxied requests per second. The default attack threshold value is 625 pps.</p> |

Table 224: Fields on the Add Screen Page (Continued)

| Field | Action |
|-----------------------|--|
| Alarm threshold | <p>Enter a value to specify the number of half-complete proxy connections per second at which the device makes entries in the event alarm log.</p> <p>NOTE: Range: 1 through 1000000 segments per second. The default alarm threshold value is 250 pps.</p> |
| Source threshold | <p>Enter a value to specify 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> <p>NOTE: Range: 4 through 1000000 segments per second. The default source threshold value is 25 pps.</p> |
| Destination threshold | <p>Enter a value to specify 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> <p>NOTE: Range: 4 through 1000000 segments per second. The default destination threshold value is 0 pps.</p> |
| Ager timeout | <p>Enter a value to specify 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> <p>Range: 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> |

IPv6 EXT Header

Table 224: Fields on the Add Screen Page (Continued)

| Field | Action |
|------------------------------|--|
| Predefined Header Type | <p>Configure the following screen options:</p> <ul style="list-style-type: none"> • Hop-by-Hop header—Select an option from the list and enter the value and click + to add it. To delete, select one or more headers and click X. • Destination header—Select an option from the list and enter the value and click + to add it. To delete, select one or more headers and click X. |
| Routing header | Select the check box to enable the IPv6 routing header screen option. |
| ESP header | Select the check box to enable the IPv6 Encapsulating Security Payload header screen option. |
| No-Next header | Select the check box to enable the IPv6 no next header screen option. |
| Mobility header | Select the check box to enable the IPv6 mobility header screen option. |
| Fragment header | Select the check box to enable the IPv6 fragment header screen option. |
| AH header | Select the check box to enable the IPv6 Authentication Header screen option. |
| Shim6 header | Select the check box to enable the IPv6 shim header screen option. |
| HIP header | Select the check box to enable the IPv6 Host Identify Protocol header screen option. |
| Customer Defined Header Type | <p>Enter a value to define the type of header range and click + to add it. Range: 0 through 255. To delete, select one or more header types and click X.</p> |

Table 224: Fields on the Add Screen Page *(Continued)*

| Field | Action |
|-----------------------|---|
| IPv6 ext header limit | Enter a value to set the number of IPv6 extension headers that can pass through the screen. Range: 0 through 32. |
| Apply to Zones | |
| Apply to Zones | Select zones from the Available column and move them to the Selected column using the right arrow. |

RELATED DOCUMENTATION

[Edit a Screen](#) | 796

Edit a Screen

You are here: **Security Policies & Objects > Zones/Screens.**

To edit a screen:

1. Select an existing screen that you want to edit on the Zones/Screens page.
2. Click the pencil icon available on the upper-right corner of the Screen List page.
The Edit Screen page appears with editable fields. For more information on the options, see "[Add a Screen](#)" on page 785 .
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[Delete a Screen](#) | 797

Delete a Screen

You are here: **Security Policies & Objects** > **Zones/Screens**.

To delete a screen:

1. Select a screen that you want to delete on the Zones/Screens page.
2. Click the delete icon available on the upper-right corner of the Screen List page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the Zones/Screens Page](#) | 780

Zone Addresses

IN THIS CHAPTER

- [About the Zone Addresses Page | 798](#)
- [Add Zone Addresses | 800](#)
- [Clone Zone Addresses | 802](#)
- [Edit Zone Addresses | 803](#)
- [Delete Zone Addresses | 803](#)
- [Search Text in a Zone Addresses Table | 803](#)

About the Zone Addresses Page

IN THIS SECTION

- [Tasks You Can Perform | 798](#)
- [Field Descriptions | 799](#)

You are here: **Security Policies & Objects > Zone Addresses.**

Use this page to configure zone address or address set.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add addresses or address sets. See ["Add Zone Addresses" on page 800](#) .
- Edit addresses or address sets. See ["Edit Zone Addresses" on page 803](#) .
- Delete addresses or address sets. See ["Delete Zone Addresses" on page 803](#) .

- Clone addresses or address sets. See ["Clone Zone Addresses" on page 802](#) .
- View the details of addresses or address sets—To do this, select the address or address set for which you want to view the details and follow the available options:
 - Click **More** and select **Detailed View**.
 - Click the detailed view icon available to the left of the selected address or address set.
- Deselect the selected address or address set. To do this, click **More** and select **Clear All Selections**.
- Search text in the Addresses table. See ["Search Text in a Zone Addresses Table" on page 803](#) .
- Show or hide columns in the Web filtering profiles table. To do this, click the Show Hide Columns icon in the upper-right corner of the Web filtering profiles table and select the options you want to view or deselect the options you want to hide on the page.

Field Descriptions

[Table 225 on page 799](#) describes the fields on the Zone Addresses page.

Table 225: Fields on the Zone Addresses Page

| Field | Description |
|---------------------|---|
| Addresses | |
| Zone | Displays the zone name to which the address is applied. |
| Name | Displays the address name. |
| Type | Displays the selected address type. |
| IP Address | Displays the IP address of the zone address. |
| Description | Displays the description of the address. |
| Address Sets | |
| Zone | Displays the zone name to which the address set is applied. |

Table 225: Fields on the Zone Addresses Page (Continued)

| Field | Description |
|------------------|--|
| Name | Displays the address sets name. |
| Type | Displays the selected address type. |
| Address List | Displays the preexisting addresses that should be included from the address set. |
| Address Set List | Displays the preexisting addresses that should be included from the list. |
| Description | Displays the description of the address set. |

RELATED DOCUMENTATION

| [Add Zone Addresses](#) | 800

Add Zone Addresses

You are here: **Security Policies & Objects** > **Zone Addresses**.

To create a zone address or address set:

1. Click **+** available on the upper-right corner of the Zone Addresses page.
The Create Addresses page appears.
2. Complete the configuration according to the guidelines provided in [Table 226 on page 800](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 226: Fields on the Create Addresses Page

| Field | Action |
|-------------|---|
| Object Type | Select an option from the list: Address or Address Group. |

Table 226: Fields on the Create Addresses Page (*Continued*)

| Field | Action |
|----------------------------------|---|
| Addresses or Address Sets | |
| Zone | Select a zone from the list to which the address is applied. |
| Name | Enter the address name. |
| Description | Enter the description for the address. |
| Type | Select an option from the list: Host, Range, or DNS host. |
| Host IP | Enter the IPv4 or IPv6 address. NOTE: This option is available if you have selected Host type. |
| Start Address | Enter the start IPv4 or IPv6 address. NOTE: This option is available if you have selected Range type. |
| End Address | Enter the end IPv4 or IPv6 address. NOTE: This option is available if you have selected Range type. |
| DNS Name | Enter a domain hostname. The string must include alphanumeric characters, periods, dashes, no spaces are allowed and must end with an alphanumeric character. NOTE: This option is available if you have selected DNS Host type. |
| Address Sets | Displays the address set name. Select the address set. |
| Create Address Set | Enter the address set name and click + to add the address set in the Address Sets. |
| Address Set Name | Enter a name for address set. NOTE: This option is available if you have selected Address Group for Object type. |

Table 226: Fields on the Create Addresses Page (*Continued*)

| Field | Action |
|--------------|---|
| Description | <p>Enter a description for address set.</p> <p>NOTE: This option is available if you have selected Address Group for Object type.</p> |
| Address List | <p>Specifies which of the preexisting addresses should be included or excluded from the address set.</p> <p>Select the addresses from the list in the Available column and then click the right arrow to move it to the Selected column.</p> <p>NOTE: This option is available if you have selected Address Group for Object type.</p> |

RELATED DOCUMENTATION

[Edit Zone Addresses](#) | 803

Clone Zone Addresses

You are here: **Security Policies & Objects** > **Zone Addresses**.

To clone a zone address or address set:

1. Select an existing zone address or address set that you want to clone and select **Clone** from the More link.
2. Click the pencil icon available on the upper-right corner of the Zone Addresses page.
The Clone Addresses page appears with editable fields. For more information on the options, see ["Add Zone Addresses" on page 800](#).
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[Delete Zone Addresses](#) | 803

Edit Zone Addresses

You are here: **Security Policies & Objects > Zone Addresses.**

To edit a zone address or address set:

1. Select an existing zone address or address set that you want to edit on the Zone Addresses page.
2. Click the pencil icon available on the upper-right corner of the Zone Addresses page.

The Edit Addresses page appears with editable fields. For more information on the options, see "[Add Zone Addresses](#)" on page 800 .

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

| [Delete Zone Addresses](#) | 803

Delete Zone Addresses

You are here: **Security Policies & Objects > Zone Addresses.**

To delete a zone address or address set:

1. Select a zone address or address set that you want to delete on the Zone Addresses page.
2. Click the delete icon available on the upper-right corner of the Zone Addresses page.

A confirmation window appears.

3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

| [Search Text in a Zone Addresses Table](#) | 803

Search Text in a Zone Addresses Table

You are here: **Security Policies & Objects > Zone Addresses.**

You can use the search icon in the upper-right corner of the Zone Addresses page to search for text containing letters and special characters on that page.

To search for text:

1. Click the search icon and enter partial text or full text of the keyword in the search bar.
The search results are displayed.
2. Click **X** next to a search keyword or click **Clear All** to clear the search results.

RELATED DOCUMENTATION

| [About the Zone Addresses Page | 798](#)

Global Addresses

IN THIS CHAPTER

- [About the Global Addresses Page | 805](#)
- [Add an Address Book | 806](#)
- [Edit an Address Book | 810](#)
- [Delete an Address Book | 810](#)

About the Global Addresses Page

IN THIS SECTION

- [Tasks You Can Perform | 805](#)
- [Field Descriptions | 806](#)

You are here: **Security Policies & Objects > Global Addresses.**

Use this page to configure global address books for security policies.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add an Address Book. See "[Add an Address Book](#)" on page 806 .
- Edit an Address Book. See "[Edit an Address Book](#)" on page 810 .
- Delete an Address Book. See "[Delete an Address Book](#)" on page 810 .

- Upgrade the old zone-based address book to global address books. To do this, click **Upgrade** available on the right-side corner of the Global Addresses table. Click **Yes** to proceed with the upgrade to global address books and click **OK**.

Field Descriptions

Table 227 on page 806 describes the fields on the Global Addresses Page.

Table 227: Fields on the Global Addresses Page

| Field | Description |
|--------------------------|---|
| 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. |

RELATED DOCUMENTATION

| [Add an Address Book | 806](#)

Add an Address Book

You are here: **Security Policies & Objects > Global Addresses.**

To add an address book:

1. Click **+** available on the upper-right corner of the Global Addresses page.
The Add Address Book page appears.
2. Complete the configuration according to the guidelines provided in [Table 228 on page 807](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 228: Fields on the Global Addresses Page

| Field | Action |
|--------------------------|---|
| Address Book Name | Enter a name for the address book. |
| Address Book Description | Enter a description for the address book. |
| Attach Zones | <p>You can select more than one zone from the list for one address book.</p> <p>NOTE: Ensure 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> |
| Addresses | |

Table 228: Fields on the Global Addresses Page *(Continued)*

| Field | Action |
|--------|--|
| + | <p>To add an address:</p> <ol style="list-style-type: none"> Click + available on the upper-right corner of the Addresses table. The Add Address page appears. Enter the following details: <ul style="list-style-type: none"> Address Name—Enter a name for the address. Description—Enter a description for the address. Address Type—Select one of the following address types from the list: <ul style="list-style-type: none"> IP Address Wildcard Address Domain Name Ranged Address Value—Enter an address that matches the selected address type. Click OK to save the changes. |
| Edit | <p>To edit an address:</p> <ol style="list-style-type: none"> Select an existing address and click the pencil icon available on the upper-right corner of the Addresses table. The Add Address page appears with editable fields. Click OK to save the changes. |
| Delete | <p>Select an existing address and click the delete icon available on the upper-right corner of the Addresses table to delete it.</p> |

Address Set

Table 228: Fields on the Global Addresses Page *(Continued)*

| Field | Action |
|--------|---|
| + | <p>To add an address set:</p> <ol style="list-style-type: none"> Click + available on the upper-right corner of the Addresses table. The Add Address Set page appears. Enter the following details: <ul style="list-style-type: none"> Address Set Name—Enter a name for the address set. Description—Enter a description for the address set. Address List—Select the address from the list in the Available column and then click the right arrow to move it to the Selected column. Specifies which of the preexisting addresses should be included or excluded from the address set. Address Set List—Select the address sets from the list in the Available column and then click the right arrow to move it to the Selected column. Specifies which of the preexisting address sets should be included or excluded from the list. Click OK to save the changes. |
| Edit | <p>To edit an address set:</p> <ol style="list-style-type: none"> Select an existing address and click the pencil icon available on the upper-right corner of the Address Set table. The Add Address Set page appears with editable fields. Click OK to save the changes. |
| Delete | <p>Select an existing address set and click the delete icon available on the upper-right corner of the Address Set table to delete it.</p> |

RELATED DOCUMENTATION

[Edit an Address Book](#) | 810

Edit an Address Book

You are here: **Security Policies & Objects > Global Addresses.**

To edit an address book:

1. Select an existing address book that you want to edit on the Global Addresses page.
2. Click the pencil icon available on the upper-right corner of the Global Addresses page.

The Edit Address Book page appears with editable fields. For more information on the options, see ["Add an Address Book" on page 806](#) .

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

| [Delete an Address Book | 810](#)

Delete an Address Book

You are here: **Security Policies & Objects > Global Addresses.**

To delete an address book:

1. Select an existing address book that you want to delete on the Global Addresses page.
2. Click the delete icon available on the upper-right corner of the Global Addresses page.

A confirmation window appears.

3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

| [About the Global Addresses Page | 805](#)

Services

IN THIS CHAPTER

- [About the Services Page | 811](#)
- [Add a Custom Application | 813](#)
- [Edit a Custom Application | 816](#)
- [Delete Custom Application | 816](#)
- [Add an Application Group | 817](#)
- [Edit an Application Group | 818](#)
- [Delete an Application Group | 819](#)

About the Services Page

IN THIS SECTION

- [Tasks You Can Perform | 811](#)
- [Field Descriptions | 812](#)

You are here: **Security Policies & Objects > Services.**

Use services in policies to manage applications across devices.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a custom application. See ["Add a Custom Application" on page 813](#) .
- Edit a custom application. See ["Edit a Custom Application" on page 816](#) .

- Delete custom application. See ["Delete Custom Application" on page 816](#) .
- Add an application group. See ["Add an Application Group" on page 817](#) .
- Edit an application group. See ["Edit an Application Group" on page 818](#) .
- Delete an application group. See ["Delete an Application Group" on page 819](#) .

Field Descriptions

[Table 229 on page 812](#) describes the fields on the Services Page.

Table 229: Fields on the Services Page

| Field | Description |
|---------------------------------|---|
| 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 229: Fields on the Services Page (Continued)

| Field | Description |
|--------------------------|--|
| Source-Port | Displays the predefined source port identifier. |
| Destination-Port | Displays the predefined destination port identifier. |
| Application Group | |
| Application Group Name | Displays the application group name. |
| Members | Displays members in the set. |
| Description | Displays a description of the application group. |

RELATED DOCUMENTATION

| [Add a Custom Application](#) | 813

Add a Custom Application

You are here: **Security Policies & Objects > Services.**

To add a custom application:

1. Click the **Custom-Applications** tab.
2. Click + available on the upper-right corner of the Services page.
The Add an Application page appears.
3. Complete the configuration according to the guidelines provided in [Table 230 on page 814](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 230: Fields on the Add an Application Page

| Field | Action |
|-------------------------|--|
| Global | |
| Application Name | Enter a custom application name. |
| Application Description | Enter a description for the custom application. |
| Application-protocol | Select a custom application protocol from the list. |
| Match IP protocol | Select a custom network protocol from the list. |
| Destination Port | Select a custom destination port identifier from the list. |
| Source Port | Select a custom source port identifier from the list. |
| Inactivity-timeout | Enter a value from 4 through 86400. Specifies the length of time (in seconds) that the application is inactive before it times out. |
| RPC-program-number | Enter a remote procedure call value from 0 through 65535. |
| Match ICMP message code | Select an Internet Control Message Protocol (ICMP) message code value from the list. |
| Match ICMP message type | Select an Internet Control Message Protocol message type value from the list. |
| UUID | Enter a universal unique identifier (UUID). |
| Application Group | Select an option from the list. Specifies the set to which this application belongs. |
| Terms | |

Table 230: Fields on the Add an Application Page (Continued)

| Field | Action |
|-------------------------|--|
| Add | Click +. The Add new term page appears. |
| Term Name | Enter an application term name. |
| ALG | Select an option from the list. Specifies the Application Layer Gateway (ALG) for the application protocol. |
| Match IP protocol | Select a network protocol from the list. |
| Destination Port | Enter the destination port identifier. |
| Source Port | Specifies the source port identifier. |
| Inactivity-timeout | Enter a value from 4 through 86400. Specifies the length of time (in seconds) that the application is inactive before it times out. |
| RPC-program-number | Enter a remote procedure call value from 0 through 65535. |
| Match ICMP message code | Select an ICMP message code value from the list. |
| Match ICMP message type | Select an ICMP message type value from the list. |
| UUID | Select an option from the list. Specifies the set to which this application belongs. |
| Edit | Select a term and click the pencil icon at the right corner of the table to modify the configuration. |

Table 230: Fields on the Add an Application Page *(Continued)*

| Field | Action |
|--------|---|
| Delete | Select a term and click the delete (X) icon at the right corner of the table to delete the selected term. |

RELATED DOCUMENTATION

[Edit a Custom Application](#) | 816

Edit a Custom Application

You are here: **Security Policies & Objects** > **Services**.

To edit a custom application:

1. Click the **Custom-Applications** tab.
2. Select an existing application that you want to edit on the Services page.
3. Click the pencil icon available on the upper-right corner of the Services page.

The Edit an Application page appears with editable fields. For more information on the options, see ["Add a Custom Application" on page 813](#).

4. Click **OK** to save the changes.

RELATED DOCUMENTATION

[Delete Custom Application](#) | 816

Delete Custom Application

You are here: **Security Policies & Objects** > **Services**.

To delete a custom application:

1. Click the **Custom-Applications** tab.

2. Select an application that you want to delete on the Services page.
3. Click the delete icon available on the upper-right corner of the Services page.
A confirmation message window appears.
4. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[Add a Custom Application | 813](#)

[Add an Application Group | 817](#)

Add an Application Group

You are here: **Security Policies & Objects > Services.**

To add an application group:

1. Click the **Application Group** tab.
2. Click + available on the upper-right corner of the Application Group page.
The Add New Application Set page appears.
3. Complete the configuration according to the guidelines provided in [Table 231 on page 817](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 231: Fields on the Add New Application Set Page

| Field | Action |
|------------------------|--|
| Application Group Name | Enter a name for application group. |
| Description | Enter a description for application group. |

Table 231: Fields on the Add New Application Set Page (Continued)

| Field | Action |
|-------------------|--|
| Application | <p>Using the right arrow, select values from Applications out of this set and move them to Applications in this set.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • Enter the application name in the search box and press Enter to search for the required application. • Click Clear to remove the selected applications from the list of Applications in this set column. |
| Application Group | <p>Using the right arrow, select values from Application groups out of this group and move them to Application groups in this group.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • Enter the application name in the search box and press Enter to search for the required application. • Click Clear to remove the selected applications from the list of Application groups in this group column. |

RELATED DOCUMENTATION

[Edit an Application Group](#) | 818

Edit an Application Group

You are here: **Security Policies & Objects** > **Services**.

To edit an application group:

1. Click the **Application Group** tab.
2. Select an existing application group that you want to edit on the Services page.
3. Click the pencil icon available on the upper-right corner of the Services page.

The Edit Application Set page appears with editable fields. For more information on the options, see ["Add an Application Group" on page 817](#).

4. Click **OK** to save the changes.

RELATED DOCUMENTATION

| [Delete an Application Group](#) | 819

Delete an Application Group

You are here: **Security Policies & Objects** > **Services**.

To delete an application group:

1. Click the **Application Group** tab.
2. Select an application group name that you want to delete on the Services page.
3. Click the delete icon available on the upper-right corner of the Services page.
A confirmation message window appears.
4. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

| [About the Services Page](#) | 811

Dynamic Applications

IN THIS CHAPTER

- [About the Dynamic Applications Page | 820](#)
- [Global Settings | 823](#)
- [Add Application Signatures | 826](#)
- [Clone Application Signatures | 831](#)
- [Add Application Signatures Group | 832](#)
- [Edit Application Signatures | 833](#)
- [Delete Application Signatures | 833](#)
- [Search Text in an Application Signatures Table | 834](#)

About the Dynamic Applications Page

IN THIS SECTION

- [Tasks You Can Perform | 821](#)
- [Field Descriptions | 822](#)

You are here: **Security Policies & Objects > Dynamic Applications.**

Use this page to create, modify, clone, and delete application signature groups. You can view the details of predefined application signatures that are already downloaded.

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 3207 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.

Tasks You Can Perform

You can perform the following tasks from this page:

- Global Settings. See ["Global Settings" on page 823](#) .
- Create application signatures. See ["Add Application Signatures" on page 826](#) .
- Create application signatures group. See ["Add Application Signatures Group" on page 832](#) .
- Edit application signatures. See ["Edit Application Signatures" on page 833](#) .
- Delete application signatures. See ["Delete Application Signatures" on page 833](#) .
- Clone application signatures. See ["Clone Application Signatures" on page 831](#) .
- Search text in an application signature. See ["Search Text in an Application Signatures Table" on page 834](#) .
- View the details of application signatures—To do this, select the application signature for which you want to view the details and follow the available options:
 - Click **More** and select **Detailed View**.
 - Right-click on the selected application signature profile and select **Detailed View**.
 - Mouse over to the left of the selected application signature and click **Detailed View**.
- Filter the application signatures based on select criteria. To do this, select the filter icon at the upper-right corner of the application signatures 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 application signature profiles table. To do this, click the Show Hide Columns icon in the upper-right corner of the application signatures table and select the options you want to view or deselect the options you want to hide on the page.
- **More**—Clone an existing application signature package, create group, or configure the page to show a detailed view.
- **Create Group**—Create a new application signature or application signatures group.

Field Descriptions

Table 232 on page 822 describes the fields on the Application Signatures page.

Table 232: Fields on the Application Signatures Page

| Field | Description |
|----------------------|---|
| Name | Displays the application signature name. |
| Object Type | Displays the application signature object type. |
| Category | Specifies the category of the application signature. |
| Subcategory | Specifies the subcategory of the application signature. |
| Risk | Displays the risk as critical, high, moderate, low, or unsafe. |
| Characteristic | Specifies the characteristic of the application signature. |
| Predefined or Custom | Displays the predefined or custom application signatures and settings that are configured on your device. |
| Status | Displays the status of the application signature. |

RELATED DOCUMENTATION

[Global Settings](#) | 823

[Add Application Signatures | 826](#)

[Add Application Signatures Group | 832](#)

[Edit Application Signatures | 833](#)

[Delete Application Signatures | 833](#)

[Clone Application Signatures | 831](#)

[Search Text in an Application Signatures Table | 834](#)

Global Settings

You are here: **Security Policies & Objects > Dynamic Applications.**

To add global settings:

1. Click the **Global Settings** on the upper-right corner of the Application Signatures page.
The Global Settings page appears.
2. Complete the configuration according to the guidelines provided in [Table 233 on page 823](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 233: Fields on the Global Settings Option Page

| Field | Action |
|--|--|
| General | |
| Custom Application Byte Limit | Select the byte limit in the range 0 through 10000. This helps in understanding when to stop the identification of custom applications. |
| Micro Applications | Enable micro-application detection in application identification and then use them as matching criteria in a security policy. |
| Application System Cache | |
| 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. | |
| Application Cache | Enable this option to save the mapping between an application type and the corresponding destination IP address, destination port, protocol type, and service. |

Table 233: Fields on the Global Settings Option Page (Continued)

| Field | Action |
|------------------------------|---|
| Security Services | Enable this option for security services, such as security policies, application firewall (AppFW), Juniper ATP Cloud, IDP, and Content Security. |
| Miscellaneous Services | Enable this option for miscellaneous services, such as APBR and AppTrack. |
| Cache entry timeout | Enter the timeout value in seconds for the application system cache (ASC) entries. Range: 0 through 1000000 seconds. Default is 3600 seconds. |
| Packet Capture | |
| Global packet capture | Enable packet capture globally to capture all unknown application traffic. You can also enable this option specific to a security policy at the rule level. For more information, see "Add a Rule to a Security Policy" on page 729 . |
| Aggressive mode | Enable to capture all traffic before AppID classifies the applications. In this mode, the system captures all application traffic regardless of the application system cache (ASC) entry. Packet capture starts for the first packet of the first session. |
| Exclude inconclusive traffic | Disable packet capture of inconclusive traffic. This option is available when you enable the Aggressive mode option. This option disables the packet capture for the following sessions: <ul style="list-style-type: none"> • Sessions closed before the application identification or classification completes. • Sessions not classified even though they reach the maximum packet capture limit. <p>If you do not configure this option, by default, the system captures packets for inconclusive sessions.</p> |
| Advanced | |
| Maximum packets | Maximum number of UDP packets per session. Range: 1 through 1000. Default is 10 packets. |

Table 233: Fields on the Global Settings Option Page *(Continued)*

| Field | Action |
|-------------------------|--|
| Maximum bytes | <p>Maximum number of TCP bytes per session. For TCP sessions, the count includes the actual payload data length and excludes IP/TCP headers for the maximum bytes limit.</p> <p>Range: 40 through 1,073,741,824. Default is 6000 bytes.</p> |
| Maximum files | <p>Maximum number of unique packet capture files to create before the oldest file is overwritten by a new file created.</p> <p>Range: 1 through 2500. Default is 100.</p> |
| Maximum storage | <p>Maximum disk space (bytes) that can be used in the Routing Engine for packet capture files.</p> <p>Range: 1 through 4096 MB. Default is 50 MB.</p> |
| Maximum memory | <p>Maximum memory limit for deep packet inspection (DPI).</p> <p>Range: 1 KB through maximum bytes (depending on the available space on the device).</p> |
| Packet capture interval | <p>Timeout value in minutes to avoid repetitive capture of same traffic. After this interval, the system continues to capture newer packet details for unknown applications until the capture limit is reached.</p> <p>Range: 1 through 525,600 minutes. Default is 1440 minutes (24 hours).</p> |
| Repeat traffic capture | <p>Number of repetitive captures of same traffic. Use this option to limit the number of times the same traffic can be repeatedly captured before the cache entry times out.</p> <p>Range: 1 through 1000. Default is 5.</p> |

RELATED DOCUMENTATION

[About the Dynamic Applications Page | 820](#)

[Add Application Signatures | 826](#)

[Add Application Signatures Group | 832](#)

[Edit Application Signatures | 833](#)

[Delete Application Signatures | 833](#)

[Clone Application Signatures | 831](#)

[Search Text in an Application Signatures Table | 834](#)

Add Application Signatures

You are here: **Security Policies & Objects > Dynamic Applications.**

To add an application signature:

1. Click **Create > Signature** on the upper-right corner of the Dynamic Applications page.
The Create Application Signatures page appears.
2. Complete the configuration according to the guidelines provided in [Table 234 on page 826](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 234: Fields on the Add Application Signatures Page

| Field | Action |
|-------------|--|
| Name | Enter the application signature name. |
| Description | Enter the application signature description. |
| Order | Enter the order of the custom application. Lower order has higher priority. The range is 1 through 50,000. |

Table 234: Fields on the Add Application Signatures Page (Continued)

| Field | Action |
|---|--|
| Priority | <p>Enter the priority over other signature applications.</p> <p>Select an option from the list:</p> <ul style="list-style-type: none"> • High • Low <p>By default, the priority for the custom application is set to Low. This allows a predefined application to take precedence. If you want to override a predefined application, you must set the priority to High.</p> |
| Risk | <p>Enter the risk as critical, high, moderate, low, or unsafe.</p> |
| Application Identification match criteria | <p>Select one or more options from the list:</p> <ul style="list-style-type: none"> • ICMP Mapping • IP Protocol Mapping • Address Mapping • L7 Signature |
| ICMP Mapping | <p>Select a value from the list.</p> <ul style="list-style-type: none"> • ICMP Type—Select the numeric value of an ICMP type. The type identifies the ICMP message, such as Unassigned or Destination Unreachable. The range is from 0 through 254. • Select the numeric value of an ICMP code. The code field provides further information (such as RFCs) about the associated type field. The range is from 0 through 254. |
| IP Protocol Mapping | <p>Select the numeric value of an ICMP type. The type identifies the ICMP message, such as Unassigned or Destination Unreachable. The range is from 0 through 254.</p> |

Table 234: Fields on the Add Application Signatures Page (Continued)

| Field | Action |
|---------------------|---|
| Address Mapping | <p>To add a new address mapping:</p> <ol style="list-style-type: none"> 1. Click Add. The Add Address Mapping page appears. Enter the following details: <ul style="list-style-type: none"> • Name—Enter the name of the address mapping. • IP Address—Enter an IPv4 or IPv6 address. • CIDR Range—Enter an IPv4 or IPV6 address prefix for classless IP addressing. • TCP Port range—Enter the TCP port range for the application. • UDP Port Range—Enter the UDP port range for the application. 2. Click the pencil icon at the upper-right corner of the Address Mapping table. Then, edit the address mapping and click OK. 3. To delete an existing Address Mapping, select it and click the delete icon or right-click on it and click Delete. |
| L7 Signature | |
| Cacheable | Set this option to True only when L7 signatures are configured in a custom signature. This option is not supported for address-based, IP protocol-based, and ICMP-based custom application signatures. |
| Add L7 Signature | <p>Click Add L7 Signature list and select an option from the following:</p> <ul style="list-style-type: none"> • Over HTTP • Over SSL • Over TCP • Over UDP <p>The Add Signature page appears.</p> |

Table 234: Fields on the Add Application Signatures Page (Continued)

| Field | Action |
|--|--|
| Add Signature | |
| Over Protocol | Displays the signature that matches the application protocol. Example: HTTP |
| Signature Name | Enter a unique name that is a string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 63 characters. |
| Port Range | Enter the port range for the application. Range is 0-65535. |
| Add Members | |
| Custom signatures can contain multiple members that define attributes of an application. The supported member name range is m01 through m15. | |
| + | Click + to create a member. |
| Context (Over HTTP) | Select the service-specific context from the following list: <ul style="list-style-type: none"> • http-get-url-parsed-param-parsed • http-header-content-type • http-header-cookie • http-header-host • http-header-user-agent • http-post-url-parsed-param-parsed • http-post-variable-parsed • http-url-parsed • http-url-parsed-param-parsed |

Table 234: Fields on the Add Application Signatures Page (Continued)

| Field | Action |
|--------------------|---|
| Context (Over SSL) | Select the service-specific context as ssl-server-name. |
| Context (Over TCP) | Select the service-specific context as stream. |
| Context (Over UDP) | Select the service-specific context as stream. |
| Direction | <p>Select the direction of the packet flow to match the signature:</p> <ul style="list-style-type: none"> any—The direction of the packet flow can either be from the client-side to the server-side or from the server-side to the client-side. client-to-server—The direction of packet flow is from the client-side to the server-side. server-to-client—The direction of packet flow is from the server-side to the client-side. |
| Depth | <p>Enter the maximum number of bytes to check for context match. Use the byte limit for AppID to identify custom application pattern for applications running over TCP or UDP or Layer 7 applications.</p> <p>Range is 1 through 8000. The Depth is set to 1000 by default, if not explicitly configured.</p> <p>NOTE: Starting in Junos OS Release 20.2R1, Depth option is supported.</p> |
| Pattern | Enter the deterministic finite automaton (DFA) pattern matched the context. The DFA pattern specifies the pattern to be matched for the signature. The maximum length is 128. |

Change History Table

Feature support is determined by the platform and release you are using. Use [Feature Explorer](#) to determine if a feature is supported on your platform.

| Release | Description |
|---------|---|
| 20.2R1 | Starting in Junos OS Release 20.2R1, Depth option is supported. |

RELATED DOCUMENTATION

- [About the Dynamic Applications Page | 820](#)
- [Global Settings | 823](#)
- [Add Application Signatures Group | 832](#)
- [Edit Application Signatures | 833](#)
- [Delete Application Signatures | 833](#)
- [Clone Application Signatures | 831](#)
- [Search Text in an Application Signatures Table | 834](#)

Clone Application Signatures

You are here: **Security Policies & Objects > Dynamic Applications.**

To clone an application signature:

1. Select the application signature profile that you want to clone and select **Clone** from the More link.

NOTE: Alternatively, you can right-click on the selected application signature profile and select **Clone**.

The Clone Application Signature page appears with editable fields. For more information on the fields, see "[Add Application Signatures](#)" on page 826 .

2. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

RELATED DOCUMENTATION

- [About the Dynamic Applications Page | 820](#)
- [Global Settings | 823](#)
- [Add Application Signatures | 826](#)
- [Add Application Signatures Group | 832](#)
- [Edit Application Signatures | 833](#)
- [Delete Application Signatures | 833](#)
- [Search Text in an Application Signatures Table | 834](#)

Add Application Signatures Group

You are here: **Security Policies & Objects** > **Dynamic Applications**.

To add an application signature group:

1. Click **Create** > **Signature Group** on the upper-right corner of the Dynamic Applications page. You can also click **More** and select **Create Group**.

The Create Application Signature Group page appears.

2. Complete the configuration according to the guidelines provided in [Table 235 on page 832](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 235: Fields on the Add Application Signature Group Page

| Field | Action |
|---------------|--|
| Name | Enter the application signature group name. |
| Group Members | <p>Enter the add or remove applications associated with the application signature group.</p> <p>Click one of the following options:</p> <ul style="list-style-type: none"> • Add—Click + to create an application signature group. • Delete—Select an existing application signature group that you want to delete and click the delete icon available at the upper right of the application signature group table. • Detailed View—Hover over the application signature group name and click the Detailed View icon to view the signature group. <p>You can also click More and select Detailed View for the selected signature group.</p> |

RELATED DOCUMENTATION

[About the Dynamic Applications Page | 820](#)

[Edit Application Signatures | 833](#)

[Delete Application Signatures | 833](#)

[Clone Application Signatures | 831](#)

[Search Text in an Application Signatures Table | 834](#)

Edit Application Signatures

You are here: **Security Policies & Objects** > **Dynamic Applications**.

To edit an application signature:

1. Select an existing application signature that you want to edit on the Dynamic Applications page.
2. Click the pencil icon available on the upper-right corner of the page.

The Edit Application Signatures page appears with editable fields. For more information on the options, see ["Add Application Signatures" on page 826](#) .

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[About the Dynamic Applications Page | 820](#)

[Global Settings | 823](#)

[Add Application Signatures | 826](#)

[Add Application Signatures Group | 832](#)

[Add Application Signatures Group | 832](#)

[Delete Application Signatures | 833](#)

[Clone Application Signatures | 831](#)

[Search Text in an Application Signatures Table | 834](#)

Delete Application Signatures

You are here: **Security Policies & Objects** > **Dynamic Applications**.

To delete application signatures:

1. Select an application signature that you want to delete on the Dynamic Applications page.
2. Click the delete icon available on the upper-right corner of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the Dynamic Applications Page | 820](#)

[Global Settings | 823](#)

[Add Application Signatures | 826](#)

[Add Application Signatures Group | 832](#)

[Edit Application Signatures | 833](#)

[Clone Application Signatures | 831](#)

[Search Text in an Application Signatures Table | 834](#)

Search Text in an Application Signatures Table

You are here: **Security Policies & Objects** > **Dynamic Applications**.

You can use the search icon in the upper-right corner of the Dynamic Applications page to search for text containing letters and special characters on that page.

To search for text:

1. Click the search icon and enter partial text or full text of the keyword in the search bar.

The search results are displayed.

2. Click **X** next to a search keyword or click **Clear All** to clear the search results.

RELATED DOCUMENTATION

[About the Dynamic Applications Page | 820](#)

[Global Settings | 823](#)

[Add Application Signatures | 826](#)

[Add Application Signatures Group | 832](#)

[Edit Application Signatures | 833](#)

[Delete Application Signatures | 833](#)

[Clone Application Signatures | 831](#)

Application Tracking

IN THIS CHAPTER

- [About the Application Tracking Page | 835](#)

About the Application Tracking Page

IN THIS SECTION

- [Field Description | 835](#)

You are here: **Security Policies & Objects** > **Application Tracking**.

Use this page to configure application tracking.

Field Description

To configure application tracking:

1. Complete the configuration according to the guidelines provided in [Table 236 on page 835](#) .
2. Click **Save** to save the changes.

[Table 236 on page 835](#) describes the fields on the Application Tracking page.

Table 236: Fields on the Application Tracking Page

| Field | Description |
|----------------------|--|
| Application tracking | Select this option to enable application tracking. |

Table 236: Fields on the Application Tracking Page *(Continued)*

| Field | Description |
|-------------------------------|--|
| Logging Type | <p>Select an option:</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—Enables you to specify the length of time that must pass before the first log message is created. The default is 1 minute. |
| First Update Interval (min) | Use the up/down arrow to set the interval time. |
| Session Update Interval (min) | Use the up/down arrow to set the interval time. |
| Application Tracking By Zone | <p>Lists the available zones.</p> <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. |

RELATED DOCUMENTATION

[About the Address Pools Page](#) | 1087

Schedules

IN THIS CHAPTER

- [About the Schedules Page | 837](#)
- [Add a Schedule | 839](#)
- [Clone a Schedule | 841](#)
- [Edit a Schedule | 841](#)
- [Delete a Schedule | 842](#)
- [Search Text in Schedules Table | 842](#)

About the Schedules Page

IN THIS SECTION

- [Tasks You Can Perform | 837](#)
- [Field Descriptions | 838](#)

You are here: **Security Policies & Objects > Schedules.**

Use this page to configure security policy schedules.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a schedule. See ["Add a Schedule" on page 839](#) .
- Clone a schedule. See ["Clone a Schedule" on page 841](#) .
- Edit a schedule. See ["Edit a Schedule" on page 841](#) .

- Delete a schedule. See ["Delete a Schedule" on page 842](#) .
- View the details of schedules—To do this, select the schedule for which you want to view the details and follow the available options:
 - Click **More** and select **Detailed View**.
 - Right-click on the selected custom object and select **Detailed View**.
 - Mouse over to the left of the selected custom object and click **Detailed View**.
- Deselect the selected schedules. To do this, click **More** and select **Clear All Selections**.
- Search text in the Schedules table. See ["Search Text in Schedules Table" on page 842](#) .
- Show or hide columns in the Schedules table. To do this, click the Show Hide Columns icon in the upper-right corner of the Schedules table and select the options you want to view or deselect the options you want to hide on the page.

Field Descriptions

[Table 237 on page 838](#) describes the fields on the Schedules Page.

Table 237: Fields on the Schedules Page

| Field | Description |
|-------------------|---|
| Name | Displays the name of the policy schedule. |
| Description | Displays a description of the policy schedule. |
| 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. |

RELATED DOCUMENTATION

| [Add a Schedule](#) | 839

Add a Schedule

You are here: **Security Policies & Objects** > **Schedules**.

To add a schedule:

1. Click **+** available on the upper-right corner of the Schedules page.
The Create Schedule page appears.
2. Complete the configuration according to the guidelines provided in [Table 238 on page 839](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 238: Fields on the Create Schedule Page

| Field | Action |
|-------------------|--|
| General | |
| Name | Enter the name of the scheduler. |
| Description | Enter a description for the scheduler. |
| Dates | |
| Start Date | Select the start date for the first day from the calendar and select the time in AM, PM, or 24 ours format. |
| Stop Date | Select the stop date for the first day from the calendar and select the time in AM, PM, or 24 ours format. |
| Second Start Date | Select the start date for the second day from the calendar and select the time in AM, PM, or 24 ours format. |
| Second End Date | Select the stop date for the second day from the calendar and select the time in AM, PM, or 24 ours format. |

Table 238: Fields on the Create Schedule Page (Continued)

| Field | Action |
|--------------------|--|
| Time Ranges | |
| Time Ranges | Select the check box to specify the time range. |
| Daily Options | <ol style="list-style-type: none"> 1. Click on the day to specify the time for a particular day. The Specify Time for <Selected Day> page appears. NOTE: Click Specify the same time for all days to configure the same time options to all days. 2. Select an option for time: <ul style="list-style-type: none"> • All Day—Specifies time options for an entire day. • Exclude Day—Excludes a specific day. • Time Ranges—Enter time ranges for the selected day: <ul style="list-style-type: none"> • Start Time—Enter the first day start time in HH:MM:SS and select AM, PM, or 24 hours format. • End Time—Enter the first day end time first day in HH:MM:SS and select AM, PM, or 24 hours format. • Second Start Time—Click + and enter the second day start time in HH:MM:SS, and then select AM, PM, or 24 hours format. • Second End Time—Enter the second day end time in HH:MM:SS and select AM, PM, or 24 hours format. <p>NOTE: Click X to delete the second day start and end time.</p> 3. Click OK to save changes. |

RELATED DOCUMENTATION

| [Edit a Schedule](#) | 841

Clone a Schedule

You are here: **Security Policies & Objects** > **Schedules**.

To clone a schedule:

1. Select a schedule that you want to clone and select **Clone** from the More link.

The Clone Schedule page appears with editable fields. For more information on the fields, see ["Add a Schedule" on page 839](#) .

NOTE: Alternatively, you can right-click on the selected schedule and select **Clone**.

2. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

RELATED DOCUMENTATION

| [Edit a Schedule](#) | 841

Edit a Schedule

You are here: **Security Policies & Objects** > **Schedules**.

To edit a schedule:

1. Select an existing schedule that you want to edit on the Schedules page.
2. Click the pencil icon available on the upper-right corner of the Schedules page.

The Edit Schedules page appears with editable fields. For more information on the options, see ["Add a Schedule" on page 839](#) .

3. Click **OK** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

| [Delete a Schedule](#) | 842

Delete a Schedule

You are here: **Security Policies & Objects > Schedules.**

To delete a schedule:

1. Select a schedule that you want to delete on the Schedules page.
2. Click the delete icon available on the upper-right corner of the Schedules page.
A confirmation window appears.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

| [Search Text in Schedules Table](#) | 842

Search Text in Schedules Table

You are here: **Security Policies & Objects > Schedules.**

You can use the search icon in the upper-right corner of the Schedules page to search for text containing letters and special characters on that page.

To search for text:

1. Click the search icon and enter partial text or full text of the keyword in the search bar.
The search results are displayed.
2. Click **X** next to a search keyword or click **Clear All** to clear the search results.

RELATED DOCUMENTATION

| [About the Schedules Page](#) | 837

Proxy Profiles

IN THIS CHAPTER

- [About the Proxy Profiles Page | 843](#)
- [Add a Proxy Profile | 845](#)
- [Edit a Proxy Profile | 846](#)
- [Delete a Proxy Profile | 846](#)

About the Proxy Profiles Page

IN THIS SECTION

- [Tasks You Can Perform | 843](#)
- [Field Descriptions | 844](#)

You are here: **Security Policies & Objects > Proxy Profiles.**

Use this page to configure the proxy profiles.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a proxy profile. See ["Add a Proxy Profile" on page 845](#) .
- Edit a proxy profile. See ["Edit a Proxy Profile" on page 846](#) .
- Delete a proxy profile. See ["Delete a Proxy Profile" on page 846](#) .

- Filter the proxy profile based on select criteria. To do this, select the filter icon at the upper-right corner of the Proxy Profiles 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 Proxy Profiles table. To do this, click the Show Hide Columns icon in the upper-right corner of the Proxy Profiles table and select the options you want to view or deselect the options you want to hide on the page.
- Advanced search for proxy profiles. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

For an advanced search:

1. Enter the search string in the text box.

Based on your input, a list of items from the filter context menu appears.

2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.

3. Press Enter to display the search results in the grid.

Field Descriptions

[Table 239 on page 844](#) describes the fields on the Proxy Profiles Page.

Table 239: Fields on the Proxy Profiles Page

| Field | Description |
|-----------------------|---|
| 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. |

RELATED DOCUMENTATION

[Add a Proxy Profile | 845](#)

Add a Proxy Profile

You are here: **Security Policies & Objects > Proxy Profiles.**

To add a proxy profile:

1. Click **+** available on the upper-right corner of the Proxy Profiles page.
The Create Proxy Profile page appears.
2. Complete the configuration according to the guidelines provided in [Table 240 on page 845](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

[Table 240 on page 845](#) describes the fields on the Create Proxy Profile Page.

Table 240: Fields on the Create Proxy Profile Page

| Field | Action |
|-----------------|--|
| Profile Name | Enter a name of the proxy profile. |
| Connection Type | Select the type of connection used by the proxy profile: <ul style="list-style-type: none"> • Server IP—Enter the server IP address. • Host Name—Enter a hostname. |
| Port Number | Enter the port number used by the proxy profile. Range: 0 through 65535. |

RELATED DOCUMENTATION

[Edit a Proxy Profile | 846](#)

Edit a Proxy Profile

You are here: **Security Policies & Objects > Proxy Profiles.**

To edit a proxy profile:

1. Select an existing proxy profile that you want to edit on the Proxy Profiles page.
2. Click the pencil icon available on the upper-right corner of the Proxy Profiles page.

The Edit Proxy Profile page appears with editable fields. For more information on the options, see ["Add a Proxy Profile" on page 845](#).

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[Delete a Proxy Profile | 846](#)

Delete a Proxy Profile

You are here: **Security Policies & Objects > Proxy Profiles.**

To delete a proxy profile:

1. Select a proxy profile that you want to delete on the Proxy Profiles page.
2. Click the delete icon available on the upper-right corner of the Proxy Profiles page.

A confirmation window appears.

3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[Add a Proxy Profile | 845](#)

[Edit a Proxy Profile | 846](#)



Security Services

[Content Security Default Configuration | 849](#)

[Content Security Antivirus Profiles | 853](#)

[Content Security Web Filtering Profiles | 884](#)

[Content Security Antispam Profiles | 914](#)

[Content Security Content Filtering Profiles | 920](#)

[Content Security Custom Objects | 929](#)

[Content Security Policies | 942](#)

[IPS Policies | 950](#)

[IPS Signatures | 967](#)

[IPS Sensor | 1001](#)

[ALG | 1009](#)

[Metadata Streaming Profile | 1020](#)

[ATP Anti-malware | 1027](#)

[ATP SecIntel Profiles | 1037](#)

[ATP SecIntel Profile Groups | 1052](#)

[SSL Initiation Profiles | 1057](#)

[SSL Proxy Profiles | 1064](#)

[Firewall Authentication—Access Profile | 1076](#)

[Firewall Authentication—Address Pools | 1087](#)

[Firewall Authentication Settings | 1095](#)

Firewall Authentication—UAC Settings | 1098

Firewall Authentication—Active Directory | 1102

Firewall Authentication—Local Authentication | 1108

Firewall Authentication—Authentication Priority | 1111

Firewall Authentication—JIMS | 1113

ICAP Redirect | 1120

Content Security Default Configuration

IN THIS CHAPTER

- [About the Default Configuration Page | 849](#)
- [Edit a Default Configuration | 851](#)
- [Delete a Default Configuration | 851](#)

About the Default Configuration Page

IN THIS SECTION

- [Tasks You Can Perform | 850](#)
- [Field Descriptions | 850](#)

You are here: **Security Services > Content Security > Default Configuration.**

The Default Configuration page describes the security features of Content Security.

This default configuration will be used, if there are multiple Content Security 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 Content Security default configuration:

- **Antivirus**—Antivirus is an in-the-cloud antivirus solution. The virus pattern and malware database are 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.

Tasks You Can Perform

You can perform the following tasks from this page:

- View the collapsed or expanded details of the Content Security default configuration options. To do this, select any one of the Content Security default configurations and click **Expand All** or **Collapse All** available on the upper-right corner of the page.
- Edit a default configuration. See "[Edit a Default Configuration](#)" on page 851 .
- Delete a default configuration. See "[Delete a Default Configuration](#)" on page 851 .

Field Descriptions

[Table 241 on page 850](#) describes the fields on the Default Configuration page.

Table 241: Fields on the Default Configuration Page

| Field | Function |
|-------------------|--|
| Anti-Virus | Displays the configured antivirus. You can edit the configured antivirus. |
| Web Filtering | Displays the configured Web filtering. You can edit the configured web filtering. NOTE: Starting in Junos OS 23.4R1 Release, J-Web supports Juniper NextGen Web Filtering. |
| Anti-Spam | Displays the configured antispam. You can edit the configured antispam. |
| Content Filtering | Displays the configured content filtering. You can edit the configured content filtering. |

RELATED DOCUMENTATION

[Edit a Default Configuration | 851](#)

[Delete a Default Configuration | 851](#)

Edit a Default Configuration

You are here: **Security Services > Content Security > Default Configuration.**

You can edit all of the following Content Security default configurations:

- Antivirus
- Web filtering
- Antispam
- Content filtering

NOTE: Starting in Junos OS 23.4R1 Release, J-Web supports Juniper NextGen Web Filtering.

To edit a default configuration:

1. Select any of the existing Content Security default configurations that you want to edit on the Default Configuration page.
2. Click the pencil icon available on the upper-right corner of the page.

The edit page for the selected default configuration appears with editable fields. You can modify any previous changes done to Antivirus, Web Filtering, Antispam, and Content Filtering.

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[About the Default Configuration Page | 849](#)

[Delete a Default Configuration | 851](#)

Delete a Default Configuration

You are here: **Security Services > Content Security > Default Configuration.**

You can delete all of the following Content Security default configurations:

- Antivirus
- Web filtering
- Antispam
- Content filtering

To delete an individual default configuration:

1. Select any of the existing Content Security default configurations that you want to delete on the Default Configuration page.
2. Click the delete icon available on the upper-right corner of the page.
The Confirm Delete window appears.

NOTE: You can only delete the configured data and not the junos-default configuration.

3. Click **Yes** to delete or click **No** to retain the profile.

To delete all the default configuration at the same time:

1. Click **Delete All Default Configurations** available on the upper-right corner of the page.
The Confirm Delete window appears.

NOTE: You can only delete the configured data and not the junos-default configuration.

2. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the Default Configuration Page | 849](#)

[Edit a Default Configuration | 851](#)

Content Security Antivirus Profiles

IN THIS CHAPTER

- [About the Antivirus Profiles Page | 853](#)
- [Add an Antivirus Profile | 855](#)
- [Clone an Antivirus Profile | 861](#)
- [Edit an Antivirus Profile | 861](#)
- [Delete an Antivirus Profile | 862](#)
- [Prevent Virus Attacks by Using J-Web Content Security Antivirus | 862](#)

About the Antivirus Profiles Page

IN THIS SECTION

- [Tasks You Can Perform | 853](#)
- [Field Descriptions | 854](#)

You are here: **Security Services > Content Security > Antivirus Profiles.**

Use this page to configure antivirus.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add an antivirus profile. See ["Add an Antivirus Profile" on page 855](#) .
- Clone an antivirus profile. See ["Clone an Antivirus Profile" on page 861](#) .
- Edit an antivirus profile. See ["Edit an Antivirus Profile" on page 861](#) .

- Delete antivirus profile. See ["Delete an Antivirus Profile" on page 862](#) .
- View the details of an antivirus profile—To do this, select the antivirus profile for which you want to view the details and follow the available options:
 - Click **More** and select **Detailed View**.
 - Right-click on the selected antivirus profile and select **Detailed View**.
 - Mouse over to the left of the selected antivirus profile and click **Detailed View**.
- Advanced search for antivirus profiles. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

For an advanced search:

1. Enter the search string in the text box.

Based on your input, a list of items from the filter context menu appears.

2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.

3. Press Enter to display the search results in the grid.
- Filter the antivirus profiles based on select criteria. To do this, select the filter icon at the upper-right corner of the antivirus profiles 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 antivirus profiles table. To do this, click the Show Hide Columns icon in the upper-right corner of the antivirus profiles table and select the options you want to view or deselect the options you want to hide on the page.

Field Descriptions

[Table 242 on page 855](#) describes the fields on the Antivirus Profiles page.

Table 242: Fields on the Antivirus Profiles Page

| Field | Function |
|----------------|---|
| Name | Displays the unique name of the antispam profile. |
| URL Allowlist | Specifies a unique customized list of all URLs or IP addresses for a given category that are to be bypassed for scanning. |
| Default Action | Displays the default fallback action taken when the antivirus system encounters errors. |

RELATED DOCUMENTATION

[Add an Antivirus Profile | 855](#)

[Edit an Antivirus Profile | 861](#)

[Delete an Antivirus Profile | 862](#)

Add an Antivirus Profile

You are here: **Security Services > Content Security > Antivirus Profiles.**

To add an antivirus profile:

1. Click **+** available on the upper-right corner of the Antivirus Profiles page.
The Create Antivirus Profiles wizard appears, displaying brief instructions about creating an antivirus profile.
2. Click **Next** to navigate to the next page.
3. Complete the configuration according to the guidelines provided in [Table 243 on page 856](#).
4. Click **Finish**.
The Summary page is displayed with the configurations you have made.
5. Review the settings, and if you need to make any modifications, click the **Edit** link or the **Back** button.
6. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.
A new antivirus profile is created. You can assign this antivirus profile to a Content Security policy. Within the Content Security policy, you can apply either the same or different antivirus profiles to the Web, file transfer and E-mail traffic.

Table 243: Fields on the Create Antivirus Profile Page

| Field | Function |
|-----------------------|---|
| General | |
| Name | Enter a unique name for the antivirus profile. The maximum length is 29 characters. |
| URL Allowlist | Select the customized object from the list for a given category that are to be bypassed for scanning. |
| MIME Allowlist | |

Table 243: Fields on the Create Antivirus Profile Page (Continued)

| Field | Function |
|--------------------------|--|
| MIME Allowlist | <p>Select a MIME allowlist from the list.</p> <p>To create a MIME list inline and add it to the MIME allowlist:</p> <ol style="list-style-type: none"> 1. Click Create New MIME List. <p>The Add MIME Pattern List window appears.</p> <ol style="list-style-type: none"> 2. Enter the following details: <ul style="list-style-type: none"> • Name—Enter a unique name for the MIME pattern list. <p>You can use a string beginning with an alphabet or underscore and consisting of alphanumeric characters, special characters such as dashes and underscores. The maximum length is 40 characters.</p> <ul style="list-style-type: none"> • Values—Click + and enter a value in the value list and click the tick mark. <p>NOTE: Value must be two strings separated by slash(/):</p> <ul style="list-style-type: none"> • The first string beginning with a letter or number and consisting of alphanumeric characters, underscores and dashes. Dashes cannot be used consecutively in the string. • The second string can be null or begin with a letter or number and consisting of alphanumeric characters, underscores, dashes, dots and pluses. Dashes, dots, and pluses cannot be used consecutively in the string. <p>If you want to delete any MIME pattern values, select the value and click the delete icon.</p> 3. Click OK. <p>A new MIME list is created and added to the MIME allowlist.</p> |
| Exception MIME Allowlist | <p>Select an exception MIME allowlist from the list.</p> <p>Click Create New MIME list to create and add a MIME pattern list inline.</p> |

Table 243: Fields on the Create Antivirus Profile Page (Continued)

| Field | Function |
|--|--|
| Fallback Options | |
| Fallback options are used when the antivirus system experiences errors and must fall back to one of the previously configured actions to either deny (block) or permit the object. | |
| Content Size | <p>Select Block or Log and Permit.</p> <p>If the content size exceeds a set limit, the content is either passed or blocked. The default action is Block.</p> |
| Engine Error | <p>Select Block or Log and Permit to specify whether the scan engine should be blocked (default) or logged and permitted if it is not ready during certain processes. For example, while the signature database is loading.</p> |
| Trickling Timeout | <p>Select Block or Log and Permit to specify whether the time taken to scan should be blocked (default) or logged and permitted if the scan process exceeds the timeout setting in the antivirus profile.</p> |
| Out of Resources | <p>Select Block or Log and Permit to specify whether the resource constraints should be blocked (default) or logged and permitted if the error is received during virus scanning.</p> |
| Decompress Layer | <p>Select Block or Log and Permit to specify whether the number of layers of nested compressed files that the internal antivirus scanner can decompress before the execution of the virus scan. The default action is Block.</p> |
| Too many Requests | <p>Select an option to specify whether the number of messages should be blocked (default) or logged and permitted if the messages received concurrently exceeds the device limits.</p> |
| Default Action | <p>Select a default action to take when an error occurs; Block or Log and Permit.</p> |

Table 243: Fields on the Create Antivirus Profile Page *(Continued)*

| Field | Function |
|---|---|
| Notification Options | |
| Use the notification options to configure a method of notifying the user when a fallback occurs or a virus is detected. | |
| Fallback Deny | |
| Notify Mail Sender | Select this option to configure e-mail notifications to notify the administrator about the errors returned by either the scan engine or the scan manager when a fallback action occurs. |
| Notification Type | Select None , Protocol , or Message from the list to specify the type of notification sent when a fallback option of deny is triggered. |
| Custom Message Subject | Enter the subject line text for your custom message for the fallback deny notification. The maximum character length is 255. |
| Custom Message | Enter the customized message text for the fallback deny notification. The maximum character length is 512. |
| Fallback Non-Deny | |
| Notify Mail Recipient | Select this option to configure E-mail notifications to notify the recipient when a fallback e-mail option without a deny action is triggered. |
| Custom Message Subject | Enter the subject line for your custom message for the fallback non-deny notification. The maximum character length is 255. |

Table 243: Fields on the Create Antivirus Profile Page *(Continued)*

| Field | Function |
|------------------------|--|
| Custom Message | Enter the customized message text for the fallback non-deny notification. The maximum character length is 512. |
| Virus Detection | |
| Notify Mail Sender | Select this option to configure E-mail notifications to notify the administrator when a virus is detected. |
| Notification Type | Specifies the type of notification to be sent when a virus is detected. Select None , Protocol , or Message from the list to specify the type of notification sent when a virus is detected. |
| Custom Message Subject | Enter the subject line text for your custom message for the virus detection notification. The maximum character length is 255. |
| Custom Message | Enter the customized message text for the virus detection notification. The maximum character length is 512. |

RELATED DOCUMENTATION

[About the Antivirus Profiles Page | 853](#)

[Edit an Antivirus Profile | 861](#)

[Delete an Antivirus Profile | 862](#)

Clone an Antivirus Profile

You are here: **Security Services** > **Content Security** > **Antivirus Profiles**.

To clone an antivirus profile:

1. Select an antivirus profile that you want to clone and select **Clone** from the More link.

NOTE: Alternatively, you can right-click on the selected antivirus profile and select **Clone**.

The Clone Antivirus Profiles page appears with editable fields. For more information on the options, see "[Add an Antivirus Profile](#)" on page 855 .

2. Click **OK** to save the changes.

A cloned antivirus profile is created for the selected antivirus profile. By default, the name of the cloned antivirus profile is in the format: *<Antivirus profile name>_clone*.

RELATED DOCUMENTATION

[About the Antivirus Profiles Page](#) | 853

[Edit an Antivirus Profile](#) | 861

[Delete an Antivirus Profile](#) | 862

Edit an Antivirus Profile

You are here: **Security Services** > **Content Security** > **Antivirus Profiles**.

To edit an antivirus profile:

1. Select an existing antivirus profile that you want to edit on the Antivirus Profiles page.
2. Click the pencil icon available on the upper-right corner of the page.

The Edit Antivirus Profiles page appears with editable fields. For more information on the options, see "[Add an Antivirus Profile](#)" on page 855 .

NOTE: Alternatively, you can right-click on the selected antivirus profile and select **Edit Antivirus Profiles**.

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[About the Antivirus Profiles Page | 853](#)

[Edit an Antivirus Profile | 861](#)

[Delete an Antivirus Profile | 862](#)

Delete an Antivirus Profile

You are here: [Security Services](#) > [Content Security](#) > [Antivirus Profiles](#).

To delete an antivirus profile:

1. Select an antivirus profile that you want to delete on the Antivirus Profiles page.
2. Click the delete icon available on the upper-right corner of the page.

NOTE: Alternatively, you can right-click on the selected antivirus profile and select **Delete Antivirus Profiles**.

3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the Antivirus Profiles Page | 853](#)

[Add an Antivirus Profile | 855](#)

[Edit an Antivirus Profile | 861](#)

Prevent Virus Attacks by Using J-Web Content Security Antivirus

SUMMARY

Learn about Content Security antivirus protection and how to configure Content Security antivirus to prevent virus attacks on SRX Series Firewalls by using J-Web. The Content Security antivirus feature on the SRX Series Firewall scans network traffic to

IN THIS SECTION

- [Content Security Antivirus Overview | 863](#)
- [Benefits of Content Security Antivirus | 864](#)

protect your network from virus attacks and to prevent virus spread.

- [Antivirus Workflow | 865](#)
- [Step 1: Update Default Configuration for Antivirus | 867](#)
- [Step 2: Configure Antivirus Custom Object | 869](#)
- [Step 3: Create Antivirus Profile | 873](#)
- [Step 4: Apply the Antivirus Profile to a Content Security Policy | 875](#)
- [Step 5: Assign the Content Security Policy to a Security Firewall Policy | 876](#)
- [Step 6: Verify That Content Security Antivirus Is Working | 879](#)
- [What's Next? | 881](#)
- [Sample Configuration Output | 881](#)

Content Security Antivirus Overview

In today's world, where cyber security threats are evolving and getting more sophisticated, protecting your network from virus attacks is extremely critical. The viruses, worms, and malware perform unwanted and malicious acts, such as damaging or deleting files, hacking personal data, affecting system performance, reformatting the hard disk, or using your computer to transmit viruses to other computers. The Content Security antivirus software acts like a first line of defense against such security threats and prevents the spread of viruses into your network. It protects your network from virus attacks, unwanted computer malwares, spywares, rootkits, worms, phishing attacks, spam attacks, trojan horses, and so on.

You must always ensure that the antivirus software and virus pattern database are up to date.

NOTE: Starting in Junos OS 22.2R1:

- In the J-Web GUI, UTM term is replaced with Content Security.
- In Junos CLI commands, we continue to use the legacy term UTM for content security.

Juniper Networks offers the following Content Security antivirus solutions:

- On-device antivirus protection

The on-device antivirus is an on-box solution. The on-device antivirus scan engine scans the data by accessing the virus pattern database that is locally stored on the device. It provides a full file-based antivirus scanning function that is available through a separately licensed subscription service.

NOTE:

- The on-device Express or Kaspersky scan engine is not supported from Junos OS Release 15.1X49-D10 onwards; however, it is still applicable for Junos OS Release 12.3X48.
- Starting in Junos OS Release 18.4R1, SRX Series Firewalls support the Avira on-device antivirus scanning engine.
- Avira on-device antivirus scanning engine is not supported on SRX300, SRX320, SRX340, SRX345, SRX380, and SRX550 HM devices.

- Sophos antivirus protection

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. The Sophos antivirus scanner also uses a local internal cache to maintain query responses from the external list server. We offer the Sophos antivirus scanning as a less CPU-intensive alternative to the full file-based antivirus feature.

Benefits of Content Security Antivirus

- The on-device antivirus solution:
 - Scans the application traffic locally without connecting to the Internet server to query whether the application traffic has virus.
 - Minimizes processing delays because the pattern database is locally stored and the scan engine is on-device.
- The Sophos antivirus solution:
 - Avoids downloading and maintaining large pattern databases on the Juniper device because the virus pattern and malware database is located on external servers maintained by Sophos.
 - Improves lookup performance because the Sophos antivirus scanner uses a local internal cache to maintain query responses from the external list server.
 - Effectively prevents malicious content from reaching the endpoint client or server through the use of the Uniform Resource Identifier (URI) checking functionality.

Antivirus Workflow

IN THIS SECTION

- [Scope | 865](#)
- [Before You Begin | 865](#)
- [Topology | 866](#)
- [Video | 866](#)
- [Sneak Peek – J-Web Content Security Antivirus Configuration Steps | 866](#)

Scope

Juniper Web (J-Web) Device Manager supports the Content Security antivirus solution on SRX Series Firewalls. In this example, you'll use Sophos antivirus protection to do the following:

1. Scan HTTP and FTP traffic from a server (10.102.70.89) to your computer for virus attacks.
2. Define a custom message **Virus Found!** to be displayed when a virus is found while scanning the traffic.
3. Create Allowlist URLs (<http://10.102.70.89>) where AV scanning is skipped.

NOTE: Assumption is that you must be able to route to the example URLs.

Before You Begin

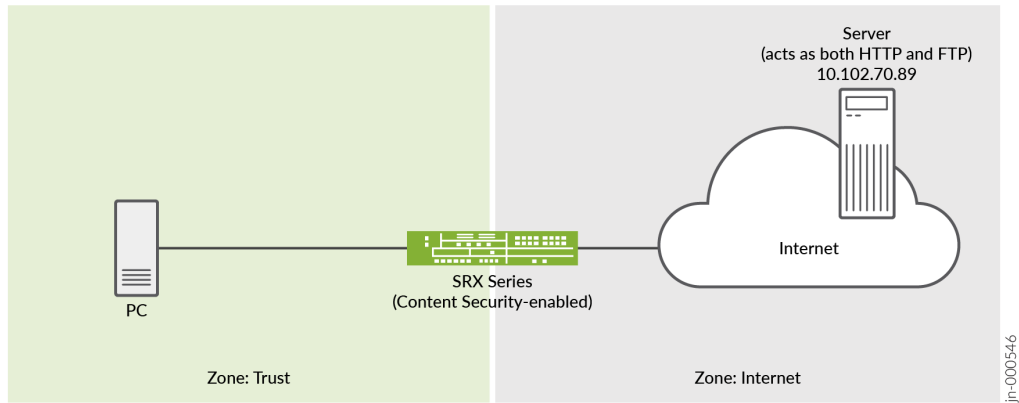
- Install a Sophos antivirus license. See the [Installation and Upgrade Guide](#), [Licensing Administration Guide](#), and [Licensing Guide](#).
- Ensure that the SRX Series Firewall you use in this example runs Junos OS Release 22.2R1.

NOTE: Starting in Junos OS 22.2R1:

- In the J-Web GUI, UTM term is replaced with Content Security.
- In Junos CLI commands, we continue to use the legacy term UTM for content security.

Topology

The topology used in this example comprises a PC connected to a Content Security-enabled SRX Series Firewall that has access to the Internet and a server. You'll use J-Web to scan the HTTP and FTP requests sent to the server with this simple setup. You'll then use Sophos antivirus protection to prevent virus attacks from the Internet to your PC.



Video

See the following video to learn how to configure Content Security antivirus using J-Web.



Video: [Configure Content Security Antivirus Using J-Web](#)

Sneak Peek – J-Web Content Security Antivirus Configuration Steps



| Step | Action |
|--------|--|
| Step 1 | Configure the Sophos engine in Default Configuration. Here, you first define the default engine as Sophos in Default Configuration. |

(Continued)

| Step | Action |
|--------|--|
| Step 2 | <p>Configure antivirus custom object.</p> <p>Here, you define the URL pattern list (allowlist) of URLs or addresses that will be bypassed by antivirus scanning. After you create the URL pattern list, you will create a custom URL category list and add the pattern list to it.</p> |
| Step 3 | <p>Configure an antivirus feature profile using the Sophos engine.</p> <p>After the default configuration, you define the parameters that will be used for virus scanning in the feature profile.</p> <p>NOTE: You must configure DNS servers before creating the antivirus profiles. To configure DNS servers, go to Device Administration > Basic Settings > System Identity > DNS servers.</p> |
| Step 4 | <p>Create a Content Security policy for Sophos antivirus and apply the antivirus feature profile to the Content Security policy.</p> <p>Here, you use a Content Security policy to bind a set of protocols (for example, HTTP) to the Sophos Content Security feature profile. You can scan other protocols as well by creating different profiles or adding other protocols to the profile, such as imap-profile, pop3-profile, and smtp-profile.</p> |
| Step 5 | <p>Create a security policy for Sophos antivirus and assign the Content Security policy to the security policy.</p> <p>Here, you use the security firewall and feature profile settings to scan the traffic from the trust zone (trust) to the untrust zone (Internet).</p> |
| Step 6 | <p>Access a URL from the allowlist URL (http://10.102.70.89) and try to download a test virus file (eicar.txt) which is made available on the 10.102.70.89 server.</p> |

Step 1: Update Default Configuration for Antivirus

You are here (in the J-Web UI): **Security Services > Content Security > Default Configuration**.

In this step, you'll set up **Sophos Engine** as the default engine type.

To update the default antivirus profile:

1. On the Anti-Virus tab, click the edit icon (pencil) to edit the default configuration.
The Anti Virus page appears. See .
2. Complete the tasks listed in the Action column in [Table 244 on page 868](#) .

Table 244: Default Configuration Settings

| Field | Action |
|-----------------------|---|
| Type | Select the Sophos Engine type for the antivirus. |
| URL Whitelist | Select None . |
| MIME Whitelist | |
| List | Select None . |
| Exception | Select None . |

Figure 20: Default Antivirus Configuration

Anti Virus ⓘ

Type ⓘ ▼

URL Whitelist ⓘ ▼

MIME Whitelist
Anti-virus MIME whitelist

List ⓘ ▼

Exception ⓘ ▼

mime-pattern can be defined under, 'Configure / Security / UTM / Custom Objects / MIME Pattern List'

3. Click **OK** to save the new default configuration.

Step 2: Configure Antivirus Custom Object

IN THIS SECTION

- [Step 2a: Configure a URL Pattern List That You Want to Bypass | 869](#)
- [Step 2b: Categorize the URLs That You Want to Allow | 871](#)

Step 2a: Configure a URL Pattern List That You Want to Bypass

In this step, you define a URL pattern list (safelist) of URLs or addresses that will be bypassed by antivirus scanning.

You are here (in the J-Web UI): **Security Services > Content Security > Custom Objects.**

To configure the safelist of URLs:

1. Click the **URL Pattern List** tab.
2. Click the add icon (+) to add a URL pattern list.
The Add URL Pattern List page appears. See [Figure 21 on page 870](#).
3. Complete the tasks listed in the Action column in [Table 245 on page 869](#).

Table 245: URL Pattern List Settings


| Field | Action |
|-------|---|
| Name | Type av-url-pattern . NOTE: Use a string beginning with a letter or underscore and consisting of alphanumeric characters and special characters such as dashes and underscores. You can use a maximum of 29 characters. |
| Value | <ol style="list-style-type: none"> a. Click + to add a URL pattern value. b. Type http://10.102.70.89. c. Click the tick icon  |

Figure 21: Add URL Pattern List

Add URL Pattern List ?

Name* ?

Values* ?

1 selected + 🗑️

| | |
|-------------------------------------|---------------------|
| <input checked="" type="checkbox"/> | Value List |
| <input checked="" type="checkbox"/> | http://10.102.70.89 |

1 items

Cancel Ok

4. Click **OK** to save the URL pattern list configuration.

Good job! Here's the result of your configuration:

 URL pattern list name: av-url-pattern
URLs allowed: http://10.102.70.89 jp-000549

Security Services / Content Security / Custom Objects

Custom Objects ?

MIME Pattern | File Extension | Protocol Command | **URL Pattern** | URL Category | Custom Message

| | | |
|--------------------------|----------------|---------------------|
| i | | |
| <input type="checkbox"/> | Name | Value |
| <input type="checkbox"/> | av-url-pattern | http://10.102.70.89 |

1 items

Step 2b: Categorize the URLs That You Want to Allow

You'll now assign the created URL pattern to a URL category list. The category list defines the action of mapping. For example, the *Safelist* category should be permitted.

You are here: **Security Services > Content Security > Custom Objects.**

To categorize URLs:

1. Click the **URL Category List** tab.
2. Click the add icon (+) to add a URL category list.
The Add URL Category List page appears. See [Figure 22 on page 872](#) .
3. Complete the tasks listed in the Action column in [Table 246 on page 871](#) .

Table 246: URL Category List Settings

| Field | Action |
|--------------|--|
| Name | Type av-url as the URL category list name for the safelisted URL pattern. NOTE: Use a string beginning with a letter or underscore and consisting of alphanumeric characters and special characters such as dashes and underscores. You can use a maximum of 59 characters. |
| URL Patterns | Select the URL pattern value av-url-pattern from the Available column and click the right arrow to move the URL pattern values to the Selected column. By doing this, you associate the URL pattern value av-url-pattern with the URL category list av-url . |

Figure 22: Add URL Category List

Add URL Category List ?

Name* ?

URL Patterns* ?

0 Available ?

| <input type="checkbox"/> | Name |
|--------------------------|------|
| No available items | |

1 Selected ?

| <input type="checkbox"/> | Name |
|--------------------------|----------------|
| <input type="checkbox"/> | av-url-pattern |

[Create New URL Pattern](#)

[Cancel](#) [Ok](#)

4. Click **OK** to save the category list configuration.

Good job! Here's the result of your configuration:

 URL category name: av-url
URL pattern list name: av-url-pattern

Security Services / Content Security / Custom Objects

Custom Objects ?

MIME Pattern | File Extension | Protocol Command | URL Pattern | **URL Category** | Custom Message

| <input type="checkbox"/> | Name | Value |
|--------------------------|--------|----------------|
| <input type="checkbox"/> | av-url | av-url-pattern |

1 Items

Step 3: Create Antivirus Profile

You are here: **Security Services > Content Security > Antivirus Profiles.**

In this step, you'll create a new Content Security antivirus profile, refer the created URL objects (patterns and categories) to the profile, and specify the notification details.

To create the new antivirus profile:

1. Click the add icon (+) to add a new antivirus profile.
The Create Antivirus Profiles page appears. See [Figure 23 on page 874](#).
2. Complete the tasks listed in the Action column in [Table 247 on page 873](#).

Table 247: Antivirus Profile Settings

| Field | Action |
|-----------------------------|---|
| General | |
| Name | Type av-profile for the new antivirus profile. NOTE: You can use a maximum of 29 characters. |
| URL Allowlist | Select av-url from the list. |
| Fallback Options | |
| Content Size | Select Log and Permit . |
| Default Action | Select Log and Permit . |
| Notification Options | |
| Virus Detection | Select Notify Mail Sender . |
| Notification Type | Select Message . |
| Custom Message Subject | Type ***Antivirus Alert*** . |

Table 247: Antivirus Profile Settings (Continued)

| Field | Action |
|----------------|-----------------------------|
| Custom Message | Type Virus Found ! . |

Figure 23: Create Antivirus Profile General Settings

Create Antivirus Profiles ?

General Fallback Options Notification Options

General Information

Name* ?

URL Whitelist ? ▼

MIME Whitelist

Anti-virus MIME whitelist

MIME Whitelist ? ▼ [Create New MIME list](#)

Exception MIME Whitelist ? ▼ [Create New MIME list](#)

Figure 24: Create Antivirus Profile Notification Settings

Create Antivirus Profiles ?

General Fallback Options **Notification Options**

Notification Options

Use notification options to specify how users are notified when a fallback occurs or a virus is detected.

Fallback Deny ? Notify Mail Sender

Fallback Non-Deny ? Notify Mail Recipient

Virus Detection ? Notify Mail Sender

Notification Type

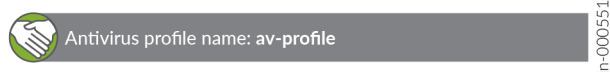
Custom Message Subject
255 characters maximum

Custom Message
512 characters maximum

Cancel Back Finish

3. Click **Finish**. Review the summary of the configuration and click **OK** to save your configuration.
4. Click **Close** after you see a successful-configuration message.

Good job! Here's the result of your configuration:



Step 4: Apply the Antivirus Profile to a Content Security Policy

After you've created the antivirus feature profile, you configure a Content Security policy for an antivirus scanning protocol and attach this policy to the antivirus profile created in "[Step 3: Create Antivirus Profile](#)" on page 873 . In this example, you'll scan HTTP and FTP traffic for viruses.

You are here: **Security Services > Content Security > Content Security Policies.**

To create a Content Security policy:

1. Click the add icon (+).

The Create Content Security Policies page appears.

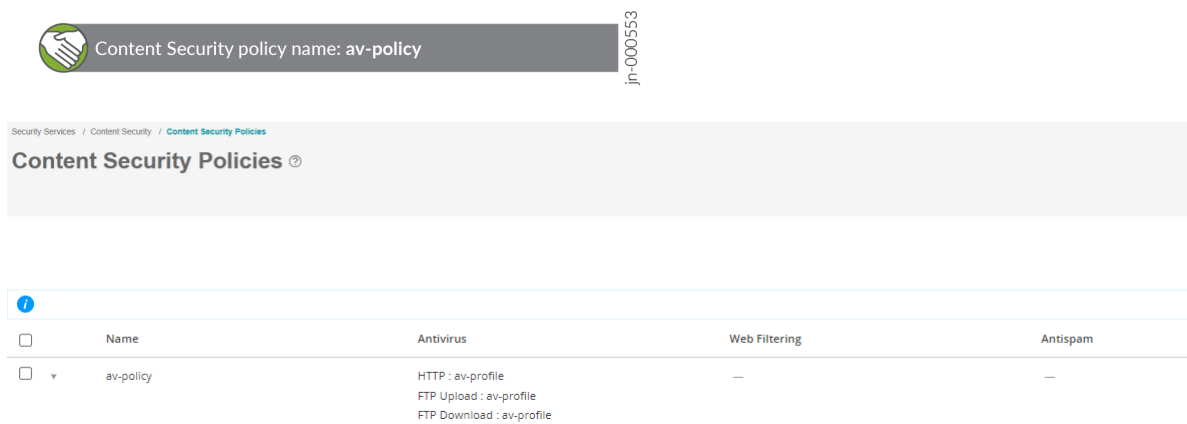
2. Complete the tasks listed in the Action column in [Table 248 on page 876](#) :

Table 248: Create Content Security Policies Settings

| Field | Action |
|------------------|--|
| General | |
| Name | Type av-policy as the name of the Content Security policy and click Next . NOTE: You can use a maximum of 29 characters. |
| Antivirus | |
| HTTP | Select av-profile from the list and click OK . |
| FTP Upload | Select av-profile from the list. |
| FTP Download | Select av-profile from the list and click Next till end of the page. |

3. Click **Finish**. Review the summary of the configuration and click **OK** to save the changes.
4. Click **Close** after you see a successful-configuration message.

Almost there! Here's the result of your configuration:



Content Security policy name: av-policy

jn-000553

Security Services / Content Security / Content Security Policies

Content Security Policies ⓘ

| | Name | Antivirus | Web Filtering | Antispam |
|--------------------------|-----------|---|---------------|----------|
| <input type="checkbox"/> | av-policy | HTTP : av-profile FTP Upload : av-profile FTP Download : av-profile | — | — |

Step 5: Assign the Content Security Policy to a Security Firewall Policy

In this step, you create a firewall security policy that will cause traffic passing from the trust zone (trust) to the untrust zone (Internet) to be scanned by Sophos antivirus using the antivirus profile settings.

You haven't yet assigned the Content Security configurations to the security policy from the trust zone to the Internet zone. Filtering actions are taken only after you assign the Content Security policy to security policy rules that act as the match criteria.

NOTE: When the security policy rules are permitted, the SRX Series Firewall:

1. Intercepts an HTTP connection and extracts each URL (in the HTTP request) or IP address.

NOTE: For an HTTPS connection, antivirus is supported through SSL forward proxy.

2. Searches for URLs in the user-configured safelist under Antivirus (**Security Services > Content Security > Default Configuration**). Then, if the URL is in the user-configured safelist, the device permits the URL.
3. Allows or blocks the URL (if a category is not configured) based on the default action configured in the antivirus profile.

You are here: **Security Policies & Objects > Security Policies.**

To create security policy rules for the Content Security policy:

1. Click the add icon (+).
2. Complete the tasks listed in the Action column in [Table 249 on page 877](#) :

Table 249: Rule Settings

| Field | Action |
|------------------|---|
| General | |
| Rule Name | Type av-security-policy as the security policy rule name. This rule allows the URLs in the av-url category list. |
| Rule Description | Enter a description for the security policy rule and click Next . |

Table 249: Rule Settings (*Continued*)

| Field | Action |
|-------------------|---|
| Source Zone | <ol style="list-style-type: none"> a. Click +. The Select Sources page appears. b. Zone—Select trust from the list. c. Addresses—Leave this field with the default value any. d. Click OK |
| Destination Zone | <ol style="list-style-type: none"> a. Click +. The Select Destination page appears. b. Zone—Select internet from the list. c. Addresses—Leave this field with the default value any. d. Services—Leave this field with the default value any. e. Click OK |
| Action | Select Permit from the list. |
| Advanced Security | <ol style="list-style-type: none"> a. Click +. The Select Advanced Security page appears. b. Content Security—Select av-policy from the list. c. Click OK |

NOTE: Navigate to **Security Policies & Objects > Zones/Screens** to create zones. Creating zones is outside the scope of this documentation.

3. Click the tick icon



to save changes.

Good job! Here's the result of your configuration:

Security Policies & Objects / Security Policies

Security Policies

* Custom application/services

Global Options Save Discard More +

| Seq | Hits | Rule Name | Source Zone | Source Address | Source Identity | Destination Zone | Destination Address | Dynamic Application | Services | URL Category | Action | Advanced Security | Rule |
|----------------------------|------|--------------------|-------------|----------------|-----------------|------------------|---------------------|---------------------|----------|--------------|------------------|-------------------|------|
| trust to trust (1 rule) | | | | | | | | | | | | | |
| trust to internet (1 rule) | | | | | | | | | | | | | |
| 1 | 4302 | av-security-policy | trust | any | — | internet | any | any | any | none | Content Security | | |



Content Security policy name: av-policy
 Security policy name: av-security-policy
 Security policy from zone: trust
 Security policy to zone: internet
 Source address: any
 Destination address: any
 Services: any
 Rule action: permit

JN-000555

- Click the commit icon (at the right side of the top banner) and select **Commit**.

The successful-commit message appears.

Congratulations! We're now ready to scan the traffic for virus attacks.

Step 6: Verify That Content Security Antivirus Is Working

IN THIS SECTION

- Purpose | 879
- Action | 879

Purpose

Verify that your configured Content Security antivirus is preventing virus attacks from the Internet server and allowing traffic from the Allowlist server.

Action

- Using the PC, send a HTTP request to `http://10.102.70.89`.

Good job! You can access the `http://10.102.70.89` server.

- Using the PC, send a FTP request to the `10.102.70.89` server to download the `ecar.txt` file. The `ecar.txt` file is a test virus file which is made available on the `10.102.70.89` server.

Sorry! The SRX Series Firewall has blocked downloading the file and sent you a custom block message *****Antivirus Alert***- Virus Found!**.

Here is an example output when you try to download the eicar.txt file and the SRX Series Firewall sends a virus alert:

```
[centos-01 ~]$ ftp 10.102.70.89
Connected to 10.102.70.89 (10.102.70.89).
220 XX FTP server (Version 6.00LS) ready.
Name (10.102.70.89:lab): root
331 Password required for root.
Password:
230 User root logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get eicar.txt
local: eicar.txt remote: eicar.txt
227 Entering Passive Mode (10,102,70,89,197,55)
150 Opening BINARY mode data connection for 'eicar.txt' (70 bytes).
netin: Connection reset by peer
426 10.102.70.89:21->10.0.1.1:36240 ***Antivirus Alert***- Virus Found!
```

Here is an example of the anti-virus statistics output when you find a threat:

```
[edit]
root@srx> show security utm anti-virus statistics
UTM Anti Virus statistics:

Intelligent-prescreening passed:      0
MIME-whitelist passed:                0
URL-whitelist passed:                 1
Session abort:                        0
Scan Request:

Total          Clean          Threat-found  Fallback
-----
          2          0          1          0

Fallback:

Log-and-Permit  Block          Permit
-----
Engine not ready:      0          0          0
Out of resources:     0          0          0
Timeout:              0          0          0
```

| | | | |
|-----------------------|---|---|---|
| Maximum content size: | 0 | 0 | 0 |
| Too many requests: | 0 | 0 | 0 |
| Decompress error: | 0 | 0 | 0 |
| Others: | 0 | 0 | 0 |

What's Next?

| If you want to | Then |
|---|--|
| Monitor Content Security antivirus details and statistics | In J-Web, go to Monitor > Security Services > Content Security > Anti Virus . |
| Generate and view reports on URLs allowed and blocked | <p>To generate and view reports:</p> <ol style="list-style-type: none"> 1. Log in to J-Web UI and click Monitor > Reports. The Reports page appears. 2. Select any of the following predefined report name. <ul style="list-style-type: none"> • Threat Assessment Report • Viruses Blocked <p>NOTE: You can't generate more than one report at the same time.</p> 3. Click Generate Report. The Report Title page appears. 4. Enter the required information and click Save. A reported is generated. |
| Learn more about Content Security features | See Content Security User Guide |

Sample Configuration Output

In this section, we present samples of configurations that block virus attacks from the websites defined in this example.

You configure the following Content Security configurations at the [edit security utm] hierarchy level.

Creating custom objects at the [edit security utm] hierarchy level:

```

custom-objects {
  url-pattern {
    av-url-pattern {
      value http://10.102.70.89 ;
    }
  }
  custom-url-category {
    av-url {
      value av-url-pattern;
    }
  }
}

```

Creating the antivirus profile at the [edit security utm] hierarchy level:

```

default-configuration {
  anti-virus {
    type sophos-engine;
  }
}

```

```

feature-profile {
  anti-virus {
    profile UTM-LB-AV {
      notification-options {
        virus-detection {
          type message;
          notify-mail-sender;
          custom-message "Virus-Found!";
          custom-message-subject "***Antivirus Alert***";
        }
      }
    }
  }
}

```

Creating the Content Security policy:

```
utm-policy av-policy {
  anti-virus {
    http-profile av-profile;
    ftp {
      upload-profile av-profile;
      download-profile av-profile;
    }
  }
}
```

Creating rules for a security policy at the [edit security policies] hierarchy level.:

```
from-zone trust to-zone internet {
  policy av-security-policy {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      permit {
        application-services {
          utm-policy av-policy;
        }
      }
    }
  }
}
```

Content Security Web Filtering Profiles

IN THIS CHAPTER

- [About the Web Filtering Profiles Page | 884](#)
- [Add a Web Filtering Profile | 887](#)
- [Clone a Web Filtering Profile | 893](#)
- [Edit a Web Filtering Profile | 894](#)
- [Delete a Web Filtering Profile | 895](#)
- [Allow or Block Websites by Using J-Web Integrated Content Security Web Filtering | 895](#)

About the Web Filtering Profiles Page

IN THIS SECTION

- [Tasks You Can Perform | 885](#)
- [Field Descriptions | 886](#)

You are here: **Security Services > Content Security > Web Filtering Profiles.**

Use this page to manage Internet usage by preventing access to inappropriate Web content.

A Web filtering profile defines a set of permissions and actions to take based on Web connections predefined by website categories. In addition, you can create custom URL categories and URL pattern lists during this process.

For an example use case, see [Allow or Block Websites by Using J-Web Integrated Content Security Web Filtering](#).

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a Web filtering profile. See ["Add a Web Filtering Profile" on page 887](#) .
- Edit a Web filtering profile. See ["Edit a Web Filtering Profile" on page 894](#) .
- Clone a Web filtering profile. See ["Clone a Web Filtering Profile" on page 893](#) .
- Delete a Web filtering profile. See ["Delete a Web Filtering Profile" on page 895](#) .
- Filter the Web filtering profiles based on select criteria. To do this, select the filter icon at the upper-right corner of the Web filtering profiles 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 Web filtering profiles table. To do this, click the Show Hide Columns icon in the upper-right corner of the Web filtering profiles table and select the columns you want to view or deselect the columns you want to hide on the page.
- View the details of a Web filtering profile—To do this, select the Web filtering profile for which you want to view the details and follow the available options:
 - Click **More** and select **Detailed View**.
 - Right-click on the selected Web filtering profile and select **Detailed View**.
 - Mouse over to the left of the selected Web filtering profile and click **Detailed View**.
- Advanced search for Web filtering profiles. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. An example filter condition is displayed in the search text box when you hover over the Search icon. When you start entering the search string, the icon indicates whether the filter string is valid or not.

For an advanced search:

1. Enter the search string in the text box.

Based on your input, a list of items from the filter context menu appears.

2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace to delete a character of the search string.

3. Press Enter to display the search results in the grid.

- Migrate to Juniper NextGen—Click **Migrate to Juniper NextGen** to convert all user defined Juniper Enhanced profiles to Juniper NextGen profiles.

NOTE:

- You cannot migrate to Juniper NextGen when:
 - Web filtering profile type is not configured in the Default Configuration page. Profile type must be ng-juniper.
 - There are no user defined profile types in the Web Filtering Profiles page with Juniper Enhanced.
- On the Default Configuration page, your profile type is not ng-juniper (Juniper NextGen), and you have a Juniper Enhanced profile type on the Web Filtering profiles page. When you click **Migrate to Juniper NextGen**, the Web Filtering profile type is automatically changed to ng-juniper on the Default Configuration page.

Field Descriptions

Table 250 on page 886 describes the fields on the Web filtering page.

Table 250: Fields on the Web Filtering Page

| Field | Action |
|----------------|---|
| Name | Displays the name for the Web filtering profile. |
| Profile type | Displays the type of profile based on the filtering type selected. |
| Default action | Displays the default action to be taken for the web filtering profile. |
| Timeout | Displays the time interval to wait before the connection to the server is closed. |

RELATED DOCUMENTATION

[Add a Web Filtering Profile | 887](#)

[Edit a Web Filtering Profile | 894](#)

Add a Web Filtering Profile

You are here: **Security Services** > **Content Security** > **Web Filtering Profiles**.

To create a new web filtering profile:

1. Click **+** available on the upper-right corner of the Web Filtering Profiles page.
The Create Web Filtering Profiles page appears.
2. Complete the configuration according to the guidelines provided in [Table 251 on page 887](#) through [Table 253 on page 892](#).
3. Click **Finish** to save the changes or click **Back** to go to the previous tab. If you want to discard your changes, click **Cancel**.

If you click **Finish**, a new web filtering profile is created.

Table 251: Fields on the General tab

| Field | Action |
|---------|---|
| Name | Enter a name for the Web filtering profile. The maximum length is 29 characters. |
| Timeout | Enter a timeout value to wait for a response from the Websense server. The maximum value is 1800 seconds. Default value is 15 seconds. |

Table 251: Fields on the General tab (Continued)

| Field | Action |
|-------------|---|
| Engine type | <p>Select an engine type for Web filtering:</p> <p>The available options are</p> <ul style="list-style-type: none"> • Juniper NextGen—Intercepts the HTTP and HTTPS traffic and sends URL information or the destination IP address to the Juniper NextGen Web Filtering (NGWF) Cloud. The NGWF Cloud categorizes the URL and provides site reputation information. Based on this information, SRX Series Firewall takes the action on the traffic. • 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). • 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. • Local—Specifies that the Web filtering module intercepts URLs and makes a permit or deny decision locally. <p>NOTE: The default value is Juniper NextGen.</p> |
| Safe search | <p>Enable a safe search solution 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>NOTE: This option is available only for the Juniper Enhanced engine type. By default, this option is enabled.</p> |
| Account | <p>Enter the user account associated with the Websense Web filtering profile.</p> <p>NOTE: This option is available only for the Websense Redirect engine type.</p> |
| Server | <p>Enter the hostname or IP address for the Websense server.</p> <p>NOTE: This option is available only for the Websense Redirect engine type.</p> |

Table 251: Fields on the General tab (Continued)

| Field | Action |
|---------------------------|---|
| Port | <p>Enter the port number for communicating with the Websense server.</p> <p>The default port is 15868.</p> <p>NOTE: This option is available only for the Websense Redirect engine type.</p> |
| Sockets | <p>Enter the number of sockets used for communication between the client and the server.</p> <p>The default value is 8.</p> <p>NOTE: This option is available only for the Websense Redirect engine type.</p> |
| Custom Block Message/URL | <p>Specify the redirect URL or a custom message to be sent when HTTP requests are blocked.</p> <p>Maximum length is 512 characters.</p> |
| Custom Quarantine Message | <p>Define a custom message to allow or deny access to a blocked site based on a user response to the message.</p> <p>Maximum length is 512 characters.</p> <p>NOTE: This option is available only for the Juniper Enhanced, Juniper NextGen, and the Local engine types.</p> |
| Base Filter | <p>Select a predefined base filter, which has default actions for all categories, for Web filtering.</p> <p>Click Clear All to discard the changes.</p> <p>NOTE: This option is available only for the Juniper Enhanced and Juniper NextGen engine types.</p> |

Table 252: Fields on the URL Categories Tab

| Field | Action |
|---------------|--|
| Apply actions | <p>To apply actions that the device must take for the selected category:</p> <ol style="list-style-type: none"> 1. Click Apply Actions. <ul style="list-style-type: none"> The Apply Actions page appears. 2. Enter the following details: <ul style="list-style-type: none"> • Action—Select an action for the URL category from the list. The options are Permit, Log and Permit, Block or Quarantine. • Custom Message—Select a custom message for the URL category. <p>NOTE:</p> <ul style="list-style-type: none"> • This option is applicable only when the action is Block or Quarantine. • Click Clear all to clear the custom message. <p>To add a custom message list inline:</p> <ol style="list-style-type: none"> a. Click Create New. b. Enter the following details: <ul style="list-style-type: none"> • Name—Enter a unique name for the custom message list. <p>Special characters such as hyphen, underscore, !, @, \$, *, + are allowed. The maximum length is 29 characters.</p> • Type—Select an option from the list. The options are Redirect URL or User Message. • Content—Enter a content for the custom message list. The maximum length is 512 characters. c. Click OK to add a new custom message list. Else, click Cancel. 3. Click OK to apply actions for the category. Else, click Cancel. |

Table 252: Fields on the URL Categories Tab (*Continued*)

| Field | Action |
|---------------|---|
| Create | <p>To add a new URL category:</p> <ol style="list-style-type: none"> Click +. The Select URL Categories page appears. Select one or more predefined and custom URL categories to apply to the list. The Name column displays the list of URL categories to choose from. Click the search icon in the upper-right corner of the table to search for any particular URL category in the list. Enter the following details: <ul style="list-style-type: none"> Action—Select an action for the URL category from the list. The options available are Permit, Log and Permit, Block, and Quarantine. NOTE: The default action is Log and Permit. Custom Message—Select a custom message for the URL category. NOTE: <ul style="list-style-type: none"> This option is applicable only when the action is Block or Quarantine. Click Clear all to clear the custom message. Click Create New to add a custom message list inline. Click OK to save the changes. If you want to discard your changes, click Cancel. |
| Delete | Select a URL category that you want to delete and click the delete icon in the upper-right corner of the table |
| Search | Click the search icon in the upper-right corner of the table and the URL category you want to search. |
| Category name | <p>Displays the URL category names.</p> <p>Select one or more categories from the list.</p> |

Table 252: Fields on the URL Categories Tab (Continued)

| Field | Action |
|----------------|---|
| Action | Displays the action taken for the URL category. |
| Custom message | Displays the respective custom messages for the URL categories. |

Table 253: Fields on the Fallback Options Tab

| Field | Action |
|---------------------------|---|
| Global Reputation Actions | <p>Select to choose the action you want to take for each reputation level.</p> <p>URLs can be processed using their reputation score if there is no category available.</p> |
| Very Safe | <p>Select an option from the list for the device must take appropriate action if the site reputation reaches the % score that is defined by you.</p> <p>NOTE: If you have not defined the percentage, the default score is 90 through 100.</p> <p>The options are Permit, Log and Permit, Block, and Quarantine.</p> |
| Moderately Safe | <p>Select an option from the list for the device must take appropriate action if the site reputation reaches the % score that is defined by you.</p> <p>NOTE: If you have not defined the percentage, the default score is 80 through 89.</p> <p>The options are Permit, Log and Permit, Block, and Quarantine.</p> |
| Fairly Safe | <p>Select an option from the list for the device must take appropriate action if the site reputation reaches the % score that is defined by you.</p> <p>NOTE: If you have not defined the percentage, the default score is 70 through 79.</p> <p>The options are Permit, Log and Permit, Block, and Quarantine.</p> |

Table 253: Fields on the Fallback Options Tab *(Continued)*

| Field | Action |
|-----------------|--|
| Suspicious | <p>Select an option from the list for the device must take appropriate action if the site reputation reaches the % score that is defined by you.</p> <p>NOTE: If you have not defined the percentage, the default score is 60 through 69.</p> <p>The options are Permit, Log and Permit, Block, and Quarantine.</p> |
| Harmful | <p>Select an option from the list for the device must take appropriate action if the site reputation reaches the % score that is defined by you.</p> <p>NOTE: If you have not defined the percentage, the default score is 50 through 59.</p> <p>The options are Permit, Log and Permit, Block, and Quarantine.</p> |
| Default Action | <p>Select an option from the list for the actions to be taken for URL categories with no assigned action and for uncategorized URLs.</p> <p>The options are Permit, Log and Permit, Block, and Quarantine.</p> |
| Fallback Action | <p>Select an option from the list. The options are Log and Permit and Block.</p> <p>Use this option when the ThreatSeeker Websense Cloud servers are unreachable. A timeout occurs for requests to ThreatSeeker Cloud.</p> |

RELATED DOCUMENTATION

[About the Web Filtering Profiles Page | 884](#)

[Clone a Web Filtering Profile | 893](#)

[Edit a Web Filtering Profile | 894](#)

[Delete a Web Filtering Profile | 895](#)

Clone a Web Filtering Profile

You are here: **Security Services > Content Security > Web Filtering Profiles.**

To clone a Web filtering profile:

1. Select a Web filtering profile that you want to clone and select **Clone** from the More link.

NOTE: Alternatively, you can right-click on the selected Web filtering profile and select **Clone**.

The Clone Web Filtering Profiles page appears with editable fields. For more information on the options, see ["Add a Web Filtering Profile" on page 887](#) .

2. Click **OK** to save the changes.

A cloned Web filtering profile is created for the selected Web filtering profile. By default, the name of the cloned Web filtering profile is in the format: *<Web filtering profile name>_clone*.

RELATED DOCUMENTATION

[About the Web Filtering Profiles Page | 884](#)

[Add a Web Filtering Profile | 887](#)

[Edit a Web Filtering Profile | 894](#)

[Delete a Web Filtering Profile | 895](#)

Edit a Web Filtering Profile

You are here: **Security Services > Content Security > Web Filtering Profiles**.

To edit a Web filtering profile:

1. Select a Web filtering profile that you want to edit on the Web Filtering page.
2. Click the pencil icon available on the upper-right corner of the page.

The Edit Web Filtering Profiles page appears with editable fields. For more information on the options, see ["Add a Web Filtering Profile" on page 887](#) .

3. Click **OK** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

[About the Web Filtering Profiles Page | 884](#)

[Add a Web Filtering Profile | 887](#)

[Clone a Web Filtering Profile | 893](#)

[Delete a Web Filtering Profile | 895](#)

Delete a Web Filtering Profile

You are here: **Security Services** > **Content Security** > **Web Filtering Profiles**.

To delete Web filtering profiles:

1. Select one or more Web filtering profiles that you want to delete from the Web Filtering page.
2. Click the delete icon available on the upper-right corner of the page.
A confirmation window appears.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the Web Filtering Profiles Page | 884](#)

[Add a Web Filtering Profile | 887](#)

[Clone a Web Filtering Profile | 893](#)

[Edit a Web Filtering Profile | 894](#)

Allow or Block Websites by Using J-Web Integrated Content Security Web Filtering

SUMMARY

Learn about Web filtering and how to filter URLs on Content Security-enabled SRX Series Firewalls by using J-Web. Web filtering helps you to allow or block access to the Web and to monitor your network traffic.

IN THIS SECTION

- [Content Security URL Filtering Overview | 896](#)
- [Benefits of Content Security Web Filtering | 897](#)
- [Web Filtering Workflow | 897](#)
- [Step 1: List URLs That You Want to Allow or Block | 899](#)
- [Step 2: Categorize the URLs That You Want to Allow or Block | 901](#)
- [Step 3: Add a Web Filtering Profile | 903](#)

- [Step 4: Reference a Web Filtering Profile in a Content Security Policy | 904](#)
- [Step 5: Assign a Content Security Policy to a Security Policy | 907](#)
- [Step 6: Verify That the URLs Are Allowed or Blocked from the Server | 910](#)
- [What's Next | 911](#)
- [Sample Configuration Output | 911](#)

Content Security URL Filtering Overview

Today, most of us spend an amount of time on the Web. We surf our favorite sites, follow interesting links sent to us through E-mail, and use a variety of Web-based applications for our office network. This increased use of the network helps us both personally and professionally. However, it also exposes the organization to a variety of security and business risks, such as potential data loss, lack of compliance, and threats such as malware, viruses, and so on. In this environment of increased risk, it's wise for businesses to implement Web or URL filters to control network threats. You can use a Web or URL filter to categorize websites on the Internet and to either allow or block user access.

Here's an example of a typical situation where a user of office network has access to a website blocked:

On the Web browser, the user types **www.game.co.uk**, a popular gaming site. The user receives a message such as Access Denied or The Website is blocked. Display of such a message means that your organization has inserted a filter for the gaming websites, and you can't access the site from your workplace.

Juniper Web (J-Web) Device Manager supports Content Security Web filtering on SRX Series Firewalls.

NOTE: Starting in Junos OS 22.2R1:

- In the J-Web GUI, UTM term is replaced with Content Security.
- In Junos CLI commands, we continue to use the legacy term UTM for content security.

In J-Web, a Web filtering profile defines a set of permissions and actions based on Web connections predefined by website categories. You can also create custom URL categories and URL pattern lists for a Web filtering profile.

NOTE: You cannot inspect URLs within e-mails using J-Web Content Security Web filtering.

Benefits of Content Security Web Filtering

- Local Web filtering:
 - Doesn't require a license.
 - Enables you to define your own lists of allowed sites (allowlist) or blocked sites (blocklist) for which you want to enforce a policy.
- Enhanced Web filtering:
 - Is the most powerful integrated filtering method and includes a granular list of URL categories, support for Google Safe Search, and a reputation engine.
 - Doesn't require additional server components.
 - Provides real-time threat score for each URL.
 - Enables you to redirect users from a blocked URL to a user-defined URL rather than simply preventing user access to the blocked URL.
- Redirect Web filtering:
 - Tracks all queries locally, so you don't need an Internet connection.
 - Uses the logging and reporting features of a standalone Websense solution.

Web Filtering Workflow

IN THIS SECTION

- [Scope | 898](#)
- [Before You Begin | 898](#)
- [Topology | 899](#)
- [Sneak Peek – J-Web Content Security Web Filtering Steps | 899](#)

Scope

In this example, you'll:

1. Create your own custom URL pattern lists and URL categories.
2. Create a Web filtering profile using the Local engine type. Here, you define your own URL categories, which can be allowed sites (allowlist) or blocked sites (blocklist) that are evaluated on the SRX Series Firewall. All URLs added for blocked sites are denied, while all URLs added for allowed sites are permitted.
3. Block inappropriate gaming websites and allow suitable websites (for example, www.juniper.net).
4. Define a custom message to display when users attempt to access gaming websites.
5. Apply the Web filtering profile to a Content Security policy.
6. Assign the Content Security policy to a security policy rule.

NOTE: Web filtering and URL filtering have the same meaning. We'll use the term *Web filtering* throughout our example.

Before You Begin

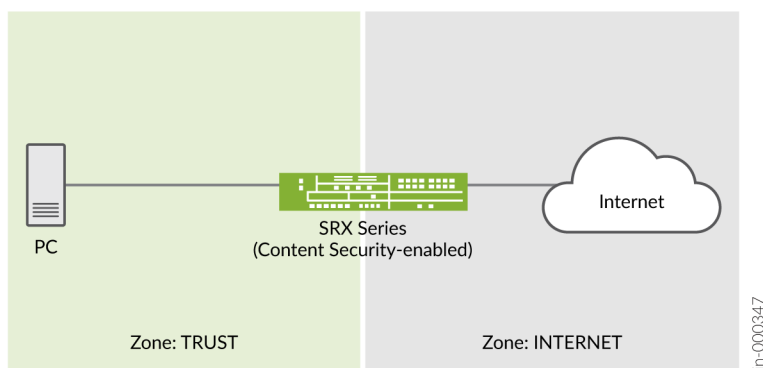
- We assume that your device is set with the basic configuration. If not, see [Configure Setup Wizard](#).
- You do not need a license to configure the Web filtering profile if you use the Local engine type. This is because you will be responsible for defining your own URL pattern lists and URL categories.
- You need a valid license (`wf_key_websense_ewf`) if you want to try the Juniper Enhanced engine type for the Web filtering profile. Redirect Web filtering does not need a license.
- Ensure that the SRX Series Firewall you use in this example runs Junos OS Release 22.2R1 and later.

NOTE: Starting in Junos OS 22.2R1:

- In the J-Web GUI, UTM term is replaced with Content Security.
- In Junos CLI commands, we continue to use the legacy term UTM for content security.

Topology

In this topology, we have a PC connected to a Content Security-enabled SRX Series Firewall that has access to the Internet. Let's use J-Web to filter the HTTP/HTTPS requests sent to the Internet using this simple setup.



Sneak Peek – J-Web Content Security Web Filtering Steps



Step 1: List URLs That You Want to Allow or Block

In this step, we define custom objects (URLs and patterns) to handle the URLs that you want to allow or block.

You are here (in the J-Web UI): **Security Services > Content Security > Custom Objects**.

To list URLs:

1. Click the URL Pattern List tab.
2. Click the add icon (+) to add a URL pattern list.
 - The Add URL Pattern List page appears. See [Figure 25 on page 900](#).
3. Complete the tasks listed in the Action column in the following table:


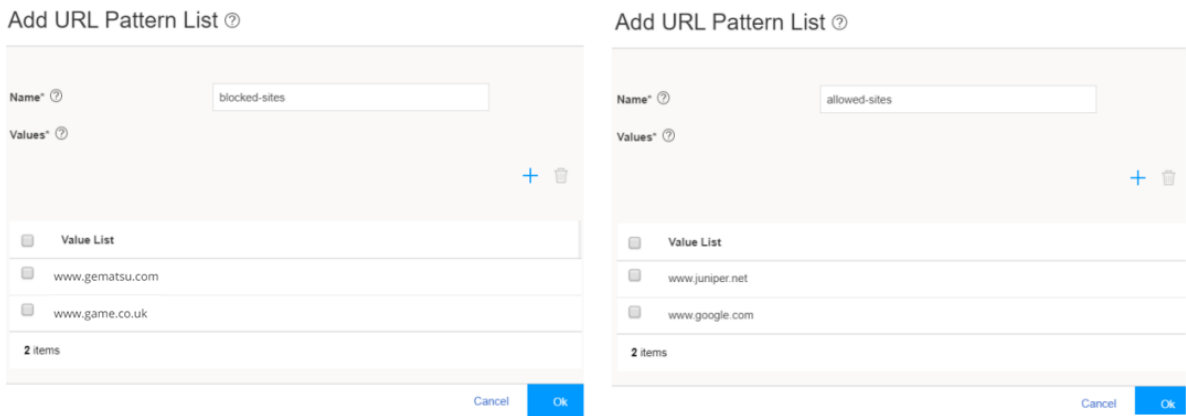

| Field | Action |
|-------|---|
| Name | Type allowed-sites or blocked-sites . NOTE: Use a string beginning with a letter or underscore and consisting of alphanumeric characters and special characters such as dashes and underscores. The maximum length is 29 characters. |
| Value | <p>a. Click + to add a URL pattern value.</p> <p>b. Type the following:</p> <ul style="list-style-type: none"> • For allowed-sites—www.juniper.net and www.google.com • For blocked-sites—www.gematsu.com and www.game.co.uk <p>c. Click the tick icon</p>  |

Figure 25: Add URL Pattern List

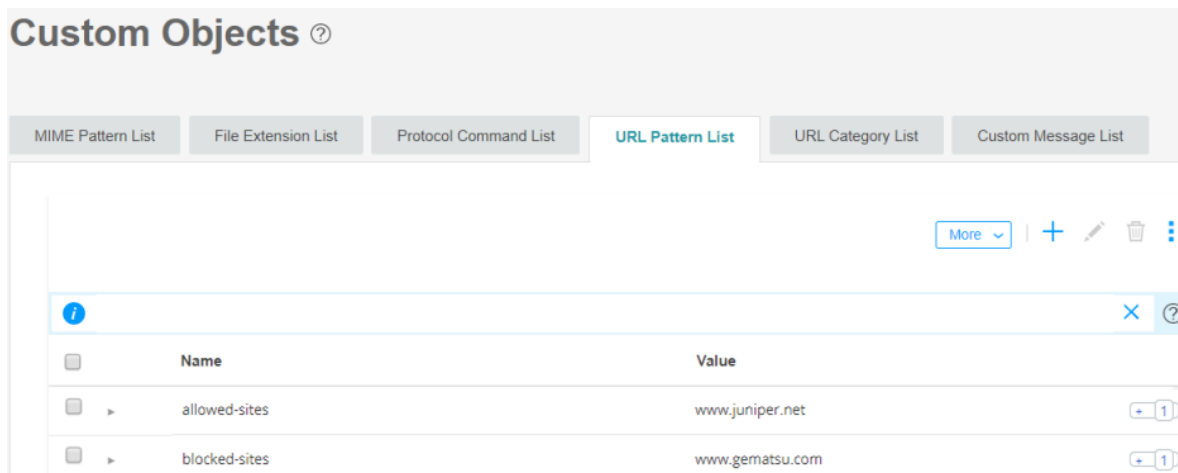


4. Click **OK** to save the changes.

Good job! Here's the result of your configuration:

-  URL pattern list name: allowed-sites
URLs allowed: www.juniper.net and www.google.com
-  URL pattern list name: blocked-sites
URLs blocked: www.gematsu.com and www.game.co.uk

8300766



Step 2: Categorize the URLs That You Want to Allow or Block

We'll now assign the created URL patterns to URL category lists. The category list defines the action associated with the associated URLs. For example, the *Gambling* category should be blocked.

You are here: **Security Services > Content Security > Custom Objects.**

To categorize URLs:

1. Click the URL Category List tab.
2. Click the add icon (+) to add a URL category list.

The Add URL Category List page appears. See [Figure 26 on page 902](#).

3. Complete the tasks listed in the Action column in the following table:

| Field | Action |
|--------------|---|
| Name | Type the URL category list name as good-sites for the allowed-sites URL pattern or stop-sites for the blocked-sites URL pattern. NOTE: Use a string beginning with a letter or underscore and consisting of alphanumeric characters and special characters such as dashes and underscores. The maximum length is 59 characters. |
| URL Patterns | <ol style="list-style-type: none"> a. Select the URL pattern values allowed-sites or blocked-sites from the Available column to associate the URL pattern values with the URL categories good-sites or stop-sites, respectively. b. Click the right arrow to move the URL pattern values to the Selected column. |

Figure 26: Add URL Category List

Add URL Category List ?

Name* ?

URL Patterns* ?

1 Available ?

| | |
|--------------------------|---------------|
| <input type="checkbox"/> | Name |
| <input type="checkbox"/> | blocked-sites |

1 Selected ?

| | |
|--------------------------|---------------|
| <input type="checkbox"/> | Name |
| <input type="checkbox"/> | allowed-sites |

[Create New URL Pattern](#)

[Cancel](#) [Ok](#)

4. Click **OK** to save the changes.

Good job! Here's the result of your configuration:

- URL category name: good-sites
URL category values: allowed-sites
 - URL category name: stop-sites
URL category values: blocked-sites
- 8300751

Custom Objects ?

MIME Pattern List | File Extension List | Protocol Command List | URL Pattern List | **URL Category List** | Custom Message List

[More](#) | [+](#) | [✎](#) | [🗑️](#) | [⋮](#)

| <input type="checkbox"/> | Name | Value |
|--------------------------|------------|---------------|
| <input type="checkbox"/> | good-sites | allowed-sites |
| <input type="checkbox"/> | stop-sites | blocked-sites |

Step 3: Add a Web Filtering Profile

Now, let's link the created URL objects (patterns and categories) to a Content Security Web filtering profile. This mapping allows you to set different values for your filtering behavior.

You are here: **Security Services > Content Security > Web Filtering Profiles.**

To create a Web filtering profile:

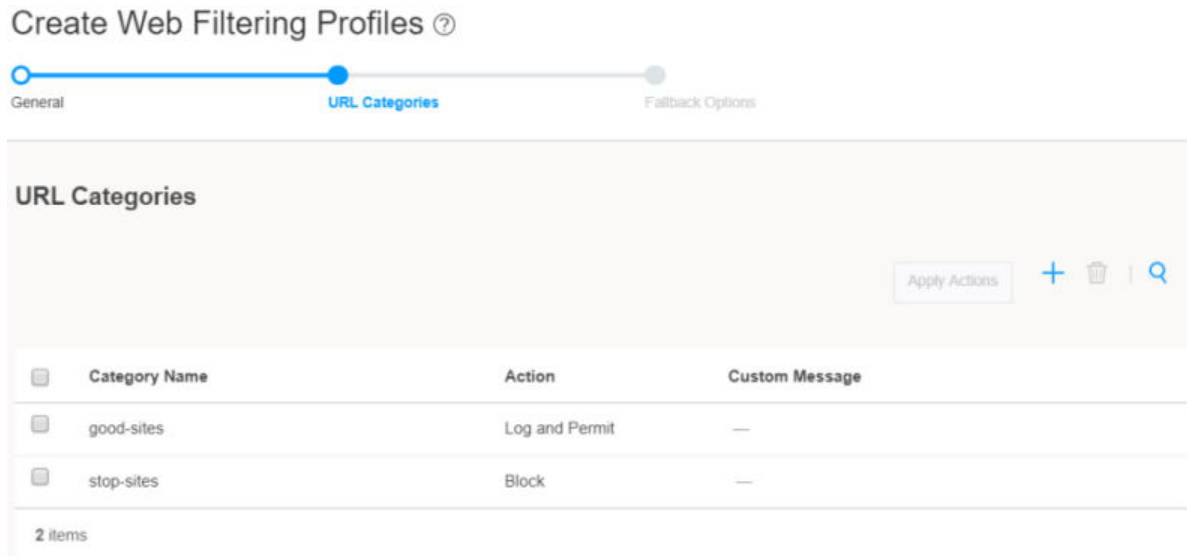
1. Click the add icon (+) to add a Web filtering profile.

The Create Web Filtering Profiles page appears. See [Figure 27 on page 904](#).

2. Complete the tasks listed in the Action column in the following table:

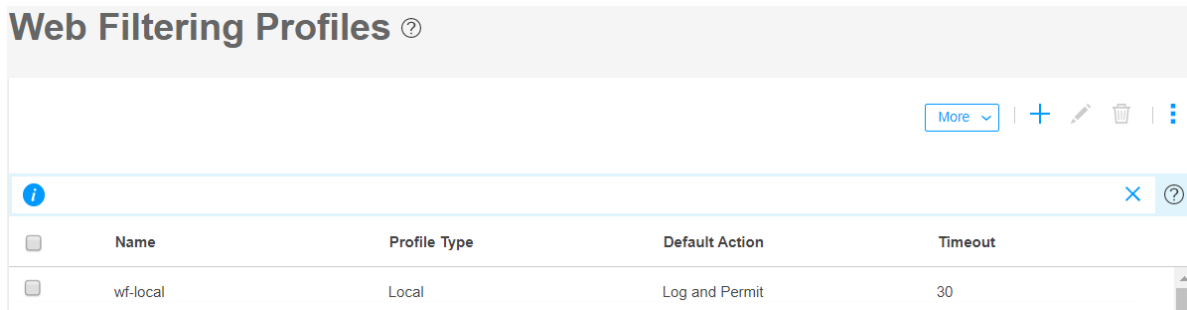
| Field | Action |
|--|--|
| General | |
| Name | Type wf-local for the Web filtering profile. NOTE: The maximum length is 29 characters. |
| Timeout | Type 30 (in seconds) to wait for a response from the Local engine. The maximum value is 1800 seconds. The default value is 15 seconds. |
| Engine type | Select the Local engine type for Web filtering. Click Next . NOTE: The default value is Juniper Enhanced. |
| URL Categories | |
| + | Click the add icon to open the Select URL Categories window. |
| Select URL categories to apply to the list | Select good-sites or stop-sites . |
| Action | Select Log and Permit for the good-sites category from the list. Select Block for the stop-sites category from the list. |

Figure 27: Create Web Filtering Profile



3. Click **Finish**. Review the summary of the configuration and click **OK** to save changes.

Good job! Here's the result of your configuration:



4. Click **Close** after you see a successful-configuration message.

Step 4: Reference a Web Filtering Profile in a Content Security Policy

We now need to assign the Web filtering profile (wf-local) to a Content Security policy that can be applied to a security policy.

You are here: **Security Services > Content Security > Content Security Policies**.

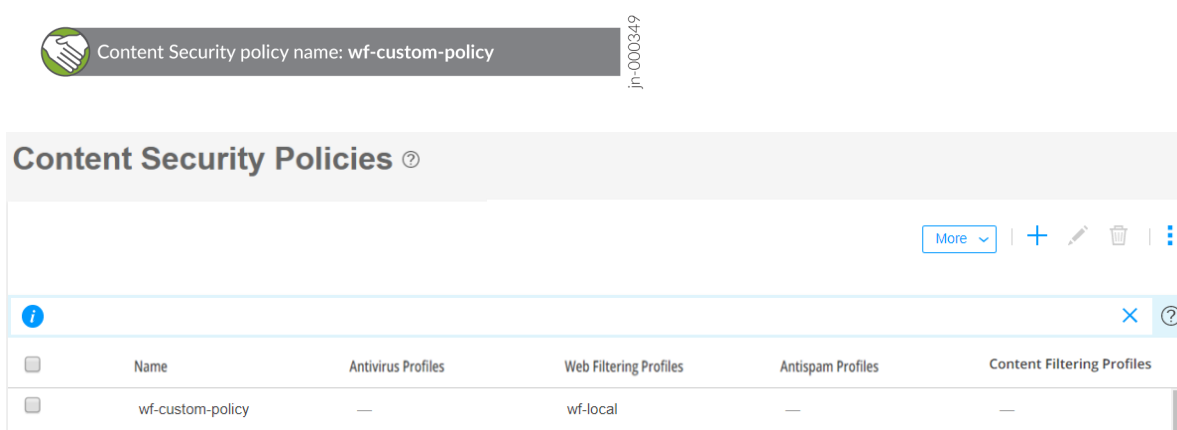
To create a Content Security policy:

1. Click the add icon (+) to add a Content Security policy.
The Create Content Security Policies page appears.
2. Complete the tasks listed in the Action column in the following table:

| Field | Action |
|---|---|
| General – General Information | |
| Name | Type wf-custom-policy for the Content Security policy. NOTE: The maximum length is 29 characters. Click Next and then click Next to skip the Antivirus configuration. |
| Web Filtering - Web Filtering Profiles by Traffic Protocol | |
| HTTP | Select wf-local from the list and click Next till the end of the workflow. |

3. Click **Finish**. Review the summary of the configuration and click **OK** to save changes.

Almost there! Here's the result of your configuration:



The screenshot shows a notification bar at the top with a green checkmark icon and the text "Content Security policy name: wf-custom-policy". To the right of the bar is the ID "jn-000349". Below the notification is a table titled "Content Security Policies" with a search icon and a "More" dropdown menu. The table has five columns: Name, Antivirus Profiles, Web Filtering Profiles, Antispam Profiles, and Content Filtering Profiles. The first row shows the policy "wf-custom-policy" with dashes in the other columns.

| Name | Antivirus Profiles | Web Filtering Profiles | Antispam Profiles | Content Filtering Profiles |
|------------------|--------------------|------------------------|-------------------|----------------------------|
| wf-custom-policy | — | wf-local | — | — |

4. Click **Close** after you see a successful message.

Almost done! Now, you create a default UTM web filtering policy that references your list of good and stop sites.

You are here: **Security Services > Content Security > Default Configuration > Web Filtering.**

5. Click the edit icon to modify the default web filtering policy.
The Web Filtering page appears.
6. Complete the tasks listed in the Action column in the following table:

| Field | Action |
|----------------------------------|---|
| Type | Select Juniper Local from the list to configure the use of the local Content Security filtering database. |
| URL Blocklist | Select stop-sites from the list to link to the list of URLs that are not allowed (blocked). |
| URL Allowlist | Select good-sites from the list to link to the list of URLs that are allowed. |
| Juniper Local > Global | |
| Custom Block Message | Enter Juniper Web Filtering has been set to block this site. |
| Default Action | Select Block from the list. Skip other fields and click OK . |

7. Click **OK** to save changes.

Almost there! Here's the result of your Content Security default Web filtering configuration.

Default Configuration ?

Anti-Virus Web Filtering Anti-Spam Content Filtering

HTTP persist :
 HTTP Reassemble :
 Type : juniper-local
 URL Blacklist : stop-sites
 URL Whitelist : good-sites

> Juniper Enhanced
 > Juniper Local

Good news! You're done with Content Security Web filtering configuration.

Step 5: Assign a Content Security Policy to a Security Policy

You haven't yet assigned the Content Security configuration to the security policy from the TRUST zone to the INTERNET zone. Filtering actions are taken only after you assign the Content Security policy to security policy rules that act as the match criteria.

NOTE: When the security policy rules are permitted, the SRX Series Firewall:

1. Intercepts an HTTP/HTTPS connection and extracts each URL (in the HTTP/HTTPS request) or IP address.

NOTE: For an HTTPS connection, Web filtering is supported through SSL forward proxy.

2. Searches for URLs in the user-configured blocklist or allowlist under Web Filtering (**Security Services > Content Security > Default Configuration**). Then, if the URL is in the:
 - a. User-configured blocklist, the device blocks the URL.
 - b. User-configured allowlist, the device permits the URL.
3. Checks the user-defined categories and blocks or allows the URL based on the user-specified action for the category.
4. Allows or blocks the URL (if a category is not configured) based on the default action configured in the Web filtering profile.

You are here: **Security Policies & Objects > Security Policies**.

To create security policy rules for the Content Security policy:

1. Click the add icon (+).
2. Complete the tasks listed in the Action column in [Table 254 on page 908](#) .

Table 254: Rule Settings

| Field | Action |
|--------------------------------------|--|
| General – General Information | |
| Rule Name | Type wf-local-policy for the security policy allowing the good-sites category and denying the stop-sites category. |
| Rule Description | Enter a description for the security policy rule. |
| Source Zone | <ol style="list-style-type: none"> a. Click +. The Select Sources page appears. b. Zone—Select TRUST from the list. c. Addresses—Leave this field with the default value Any. d. Click OK |

Table 254: Rule Settings (*Continued*)

| Field | Action |
|-------------------|--|
| Destination Zone | <p>a. Click +.</p> <p>The Select Destination page appears.</p> <p>b. Zone—Select INTERNET from the list.</p> <p>c. Addresses—Leave this field with the default value Any.</p> <p>d. Services—Leave this field with the default value Any.</p> <p>e. URL Category—Leave this field blank.</p> <p>f. Click OK</p> |
| Action | By default, Permit is selected. Leave as is. |
| Advanced Security | <p>a. Click +.</p> <p>The Select Advanced Security page appears.</p> <p>b. Content Security—Select wf-custom-policy from the list.</p> <p>c. Click OK</p> |

NOTE: Navigate to **Security Policies & Objects > Zones/Screens** to create zones. Creating zones is outside the scope of this documentation.

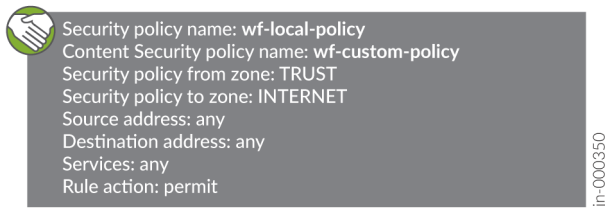
3. Click the tick icon



and then click **Save** to save changes.

NOTE: Scroll back the horizontal bar if the inline tick and cancel icons are not available when creating a new rule.

Good job! Here's the result of your configuration:



Security Policies

| Seq | Hits | Rule Name | Source Zone | Source Address | Identity | Destination Zone | Destination Address | Dynamic Application | Services | URI Category | Action | Advanced Security | Options |
|-----|------|-----------------|-------------|----------------|----------|------------------|---------------------|---------------------|----------|--------------|--------|-------------------|---------|
| 1 | - | wf-local-policy | trust | any | - | trust | any | any | any | any | Permit | IPM | |

- Click the commit icon (at the right side of the top banner) and select **Commit**.

The successful-commit message appears.

Congratulations! We're ready to filter the URL requests.

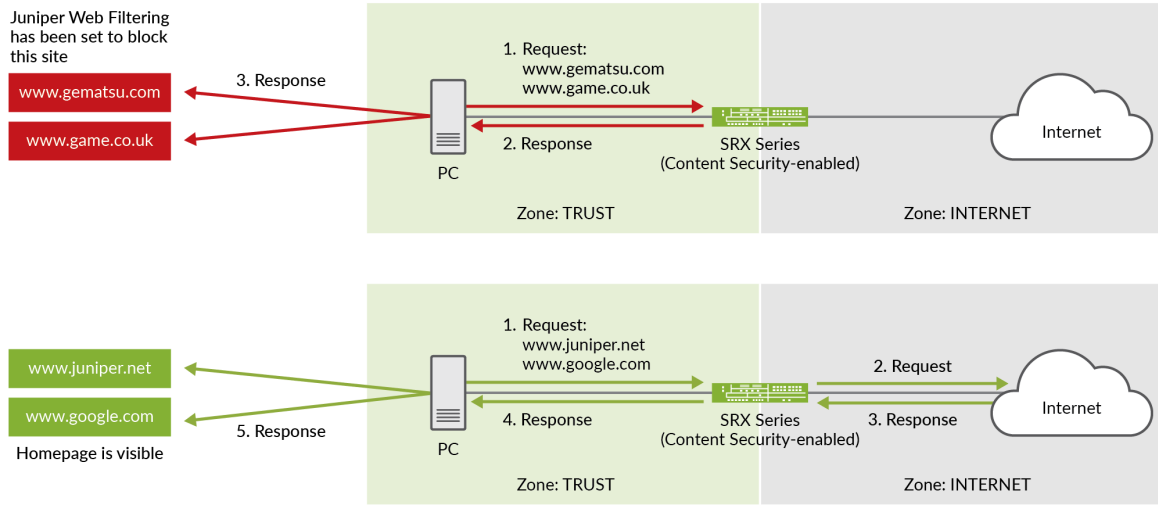
Step 6: Verify That the URLs Are Allowed or Blocked from the Server

Let's verify that our configurations and security policy work fine with the defined URLs in the topology:

- If you enter www.gematsu.com and www.game.co.uk, the SRX Series Firewall should block the URLs and send the configured blocked site message.

NOTE: Most sites use HTTPS. The blocked site message is only seen for HTTP sites. For HTTPS, you can expect a Secure Connection Failed error message, such as An error occurred during a connection to <blocked-siteurl> PR_CONNECT_RESET_ERROR.

- If you enter www.juniper.net and www.google.com, the SRX Series Firewall should allow the URLs with their homepage displayed.



What's Next

| What to do? | Where? |
|--|--|
| Monitor Content Security Web filtering information and statistics. | In J-Web, go to Monitor > Security Services > Content Security > Web Filtering . |
| Generate and view reports on URLs allowed and blocked. | In J-Web, go to Reports . Generate reports for Threat Assessment Reports and Top Blocked Applications via Webfilter logs. |
| Learn more about Content Security features. | Content Security User Guide |

Sample Configuration Output

In this section, we present samples of configurations that allow and block the websites defined in this example.

You configure the following Content Security configurations at the [edit security utm] hierarchy level.

Creating custom objects:

```

custom-objects {
  url-pattern {
    blocked-sites {
      value [ http://*.gematsu..com http://*.game.co.uk];
    }
  }
}
    
```

```

    }
    allowed-sites {
        value [ http://*.juniper.net http://*.google.com];
    }
}
custom-url-category {
    good-sites {
        value allowed-sites;
    }
    stop-sites {
        value blocked-sites;
    }
}
}
}

```

Creating the Web filtering profile:

```

default-configuration {
    web-filtering {
        url-whitelist good-sites;
        url-blacklist stop-sites;
        type juniper-local;
        juniper-local {
            default block;
            custom-block-message "Juniper Web Filtering has been set to block this
site.";
        }
        fallback-settings {
            default log-and-permit;
            server-connectivity log-and-permit;
            timeout log-and-permit;
            too-many-requests log-and-permit;
        }
    }
}
}
}

```

```

feature-profile {
    web-filtering {
        juniper-local {
            profile wf-local {
                category {

```


Content Security Antispam Profiles

IN THIS CHAPTER

- [About the Antispam Profiles Page | 914](#)
- [Add an Antispam Profile | 916](#)
- [Clone an Antispam Profile | 917](#)
- [Edit an Antispam Profile | 918](#)
- [Delete an Antispam Profile | 919](#)

About the Antispam Profiles Page

IN THIS SECTION

- [Tasks You Can Perform | 914](#)
- [Field Descriptions | 915](#)

You are here: **Security Services** > **Content Security** > **Antispam Profiles**.

Use the Antispam Profiles page to view and manage antispam profiles. An antispam profile is used to examine transmitted e-mail messages to identify e-mail spam by using a constantly updated spam block list.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create an antispam profile. See ["Add an Antispam Profile" on page 916](#) .
- Edit an antispam profile. See ["Edit an Antispam Profile" on page 918](#) .

- Delete an antispam profile. See ["Delete an Antispam Profile" on page 919](#) .
- Clone an antispam profile. See ["Clone an Antispam Profile" on page 917](#)
- View the details of an antispam profile—To do this, select the antispam profile for which you want to view the details and follow the available options:
 - Click **More** and select **Detailed View**.
 - Right-click on the selected antispam profile and select **Detailed View**.
 - Mouse over to the left of the selected antispam profile and click **Detailed View**.
- Advanced search for antispam profiles. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

For an advanced search:

1. Enter the search string in the text box.

Based on your input, a list of items from the filter context menu appears.

2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.

3. Press Enter to display the search results in the grid.
- Filter the antispam profiles based on select criteria. To do this, select the filter icon at the upper-right corner of the antispam profiles 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 antispam profiles table. To do this, click the Show Hide Columns icon in the upper-right corner of the antispam profiles table and select the options you want to view or deselect the options you want to hide on the page.

Field Descriptions

[Table 255 on page 916](#) describes the fields on the Antispam Profiles page.

Table 255: Fields on the Antispam Profiles Page

| Field | Description |
|------------------|---|
| Name | Name of the antispam profile. |
| Sophos Blocklist | Indicates whether Sophos Blocklist is enabled (server-based filtering) or disabled (local filtering). |
| Action | Action to be taken when spam is detected. |
| Custom Tag | Custom-defined tag that identifies an e-mail message as spam. |

RELATED DOCUMENTATION

[Add an Antispam Profile | 916](#)

[Clone an Antispam Profile | 917](#)

[Edit an Antispam Profile | 918](#)

[Delete an Antispam Profile | 919](#)

Add an Antispam Profile

You are here: **Security Services > Content Security > Antispam Profiles.**

To add an antispam profile:

1. Click **+** on the upper-right corner of the Antispam Profiles page.
The Create Antispam Profiles page appears.
2. Complete the configuration according to the guidelines provided in [Table 256 on page 917](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 256: Fields on the Create Antispam Profiles Page

| Field | Action |
|----------------------------|---|
| General Information | |
| Name | Enter a unique name for your antispam profile. |
| Sophos Blocklist | Enable this option to use server-based spam filtering. By default, this option is enabled. NOTE: If you disable this option, then local spam filtering is used. |
| Action | |
| Default Action | Select an option to be taken when a spam message is detected. The options available are: <ul style="list-style-type: none"> • Tag E-Mail Subject Line—Adds a custom string at the beginning of the subject of the e-mail. • Tag SMTP Header—Adds a custom string to the e-mail header. • Block E-Mail—Blocks the spam e-mail. • None—No action taken. |
| Custom Tag | Enter a custom string for identifying a message as spam. By default, the device uses ***SPAM*** . |

RELATED DOCUMENTATION
[About the Antispam Profiles Page | 914](#)
[Clone an Antispam Profile | 917](#)
[Edit an Antispam Profile | 918](#)
[Delete an Antispam Profile | 919](#)
Clone an Antispam Profile

You are here: **Security Services > Content Security > Antispam Profiles.**

To clone an antispam profile:

1. Select an antispam profile that you want to clone and select **Clone** from the More link.

NOTE: Alternatively, you can right-click on the selected antispam profile and select **Clone**.

The Clone Antispam Profiles page appears with editable fields. For more information on the fields, see ["Add an Antispam Profile" on page 916](#) .

2. Click **OK** to save the changes.

A cloned antispam profile is created for the selected antispam profile. By default, the name of the cloned antispam profile is in the format: *<Antispam profile name>_clone*.

RELATED DOCUMENTATION

[About the Antispam Profiles Page | 914](#)

[Add an Antispam Profile | 916](#)

[Edit an Antispam Profile | 918](#)

[Delete an Antispam Profile | 919](#)

Edit an Antispam Profile

You are here: **Security Services > Content Security > Antispam Profiles**.

To edit an antispam profile:

1. Select an existing antispam profile that you want to edit on the Antispam Profiles page.
2. Click the pencil icon available on the upper-right corner of the page.

The Edit Antispam Profiles page appears. You can modify any previous changes done to Sophos Blocklist, Default Action, and Custom Tag for the selected antispam profile. For more information on the options, see ["Add an Antispam Profile" on page 916](#) .

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[About the Antispam Profiles Page | 914](#)

[Add an Antispam Profile | 916](#)

[Clone an Antispam Profile | 917](#)

[Delete an Antispam Profile | 919](#)

Delete an Antispam Profile

You are here: **Security Services** > **Content Security** > **Antispam Profiles**.

To delete antispam profile(s):

1. Select one or more antispam profiles that you want to delete on the Antispam Profiles page.
2. Click the delete icon available on the upper-right corner of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the Antispam Profiles Page | 914](#)

[Add an Antispam Profile | 916](#)

[Clone an Antispam Profile | 917](#)

[Edit an Antispam Profile | 918](#)

Content Security Content Filtering Profiles

IN THIS CHAPTER

- [About the Content Filtering Profiles Page | 920](#)
- [Add a Content Filtering Profile | 922](#)
- [Clone a Content Filtering Profile | 926](#)
- [Edit a Content Filtering Profile | 927](#)
- [Delete a Content Filtering Profile | 928](#)

About the Content Filtering Profiles Page

IN THIS SECTION

- [Tasks You Can Perform | 920](#)
- [Field Descriptions | 921](#)

You are here: **Security Services** > **Content Security** > **Content Filtering Profiles**.

Use this page to configure content filtering.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a content filtering profile. See ["Add a Content Filtering Profile" on page 922](#) .
- Clone a content filtering profile. See ["Clone a Content Filtering Profile" on page 926](#)
- Edit a content filtering profile. See ["Edit a Content Filtering Profile" on page 927](#) .

- Delete a content filtering profile. See ["Delete a Content Filtering Profile" on page 928](#) .
- View the details of a content filtering profile—To do this, select the content filtering profile for which you want to view the details and follow the available options:
 - Click **More** and select **Detailed View**.
 - Right-click on the selected content filtering profile and select **Detailed View**.
 - Mouse over to the left of the selected content filtering profile and click **Detailed View**.
- Advanced search for content filtering profiles. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

For an advanced search:

1. Enter the search string in the text box.

Based on your input, a list of items from the filter context menu appears.

2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.

3. Press Enter to display the search results in the grid.
- Filter the content filtering profiles based on select criteria. To do this, select the filter icon at the upper-right corner of the content filtering profiles 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 content filtering profiles table. To do this, click the Show Hide Columns icon in the upper-right corner of the content filtering profiles table and select the options you want to view or deselect the options you want to hide on the page.

Field Descriptions

[Table 257 on page 922](#) describes the fields on the Content Filtering Profiles page.

Table 257: Fields on the Content Filtering Profiles Page

| Field | Description |
|---------------------|--|
| Name | Displays the unique name of the content filtering profile. |
| Permit Command List | Displays the permitted protocol command name. |
| Block Command List | Displays the blocked protocol command. |
| Notification Type | Displays the notification type opted. |

RELATED DOCUMENTATION

[Add a Content Filtering Profile | 922](#)

[Edit a Content Filtering Profile | 927](#)

[Delete a Content Filtering Profile | 928](#)

Add a Content Filtering Profile

You are here: **Security Services > Content Security > Content Filtering Profiles.**

To add a content filtering profile:

1. Click **+** on the upper-right corner of the Content Filtering Profiles page.
The Create Content Filtering page appears.
2. Complete the configuration according to the guidelines provided in [Table 258 on page 923](#).
3. Click **Finish**.
The Summary page is displayed with the configurations you have made.
4. Review the settings, and if you need to make any modifications, click the **Edit** link or the **Back** button.
5. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.
A new content filter profile is created.

Table 258: Fields on the Create Content Filtering Profiles Page

| Field | Action |
|--------------------------------------|---|
| General - General Information | |
| Name | Enter a unique name for the content filtering profile. |
| Notification Options | |
| Notification Mail Sender | Select the Notify Mail Sender check box to send an e-mail when a virus is detected and a content block is triggered. |
| Notification Type | Select the None , Protocol Only , or Message options from the list to specify the type of notification sent when a content block is triggered. |
| 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). |
| Protocol Commands | |

Table 258: Fields on the Create Content Filtering Profiles Page (*Continued*)

| Field | Action |
|----------------------|--|
| Command Block List | <p>Select the protocol command name to be blocked from the list. By blocking certain commands, traffic can be controlled on the protocol command level.</p> <p>To create a protocol command inline and add it to the command block list:</p> <ol style="list-style-type: none"> 1. Click Create Protocol Command. <ul style="list-style-type: none"> The Add Protocol Command List window appears. 2. Enter the following details: <ul style="list-style-type: none"> • Name—Enter a unique name for the protocol command list. <p>You can use a string beginning with an alphabet or underscore and consisting of alphanumeric characters, special characters such as dashes and underscores. The maximum length is 29 characters.</p> • Values—Click + and enter a value in the value list and click the tick mark. <p>To delete any value list, select the value and click on the delete icon.</p> 3. Click OK. <ul style="list-style-type: none"> A new protocol command is created and added to the command block list. |
| Command Permit List | <p>Select the protocol command name to be permitted from the list.</p> <p>Click Create Protocol Command to create a protocol command inline and add it to the permitted list.</p> |
| Content Types | |

Table 258: Fields on the Create Content Filtering Profiles Page (*Continued*)

| Field | Action |
|------------------------|---|
| Block Content Type | <p>Select the content type you want to block.</p> <p>The available options are:</p> <ul style="list-style-type: none"> • ActiveX • Windows executables (.exe) • HTTP Cookie • Java Applet • ZIP files |
| File Extensions | |
| Extension Block List | <p>Select an extension from the list that you want to block.</p> <p>To create a file extension inline and add it to the extension block list:</p> <ol style="list-style-type: none"> 1. Click Create File Extensions. <p>The Add File Extension List window appears.</p> <ol style="list-style-type: none"> 2. Enter the following details: <ul style="list-style-type: none"> • Name—Enter a unique name for the file extension list. <p>You can use a string beginning with an alphabet or underscore and consisting of alphanumeric characters, special characters such as dashes and underscores. The maximum length is 29 characters.</p> <ul style="list-style-type: none"> • Values—Select one or more values in the Available Column and move it to the Selected Column using the right arrow. 3. Click OK. <p>A new file extension is created and added to the extension block list.</p> |
| MIME Types | |

Table 258: Fields on the Create Content Filtering Profiles Page (*Continued*)

| Field | Action |
|------------------|--|
| MIME Block List | <p>Select the MIME type from the list.</p> <p>To create a MIME list inline and add it to the MIME block list:</p> <ol style="list-style-type: none"> Click Create MIME List. <p>The Add MIME Pattern List window appears.</p> <ol style="list-style-type: none"> Enter the following details: <ul style="list-style-type: none"> Name—Enter an unique name for the MIME pattern list. <p>You can use a string beginning with an alphabet or underscore and consisting of alphanumeric characters, special characters such as dashes and underscores. The maximum length is 40 characters.</p> <ul style="list-style-type: none"> Values—Click + and enter a value in the value list and click the tick mark. <p>To delete any value list, select the value and click on the delete icon.</p> Click OK. <p>A new MIME list is created and added to the MIME block list.</p> |
| MIME Permit List | <p>Select the MIME type from the list.</p> <p>Click Create MIME List to create a MIME list inline and add it to the MIME permit list.</p> |

RELATED DOCUMENTATION

[About the Content Filtering Profiles Page | 920](#)

[Edit a Content Filtering Profile | 927](#)

[Delete a Content Filtering Profile | 928](#)

Clone a Content Filtering Profile

You are here: **Security Services > Content Security > Content Filtering Profiles**.

To clone a content filtering profile:

1. Select a content filtering profile that you want to clone and select **Clone** from the More link.

NOTE: Alternatively, you can right-click on the selected content filtering profile and select **Clone**.

The Clone Content Filtering Profiles page appears with editable fields. For more information on the fields, see "[Add a Content Filtering Profile](#)" on page 922 .

2. Click **OK** to save the changes.

A cloned content filtering profile is created for the selected content filtering profile. By default, the name of the cloned content filtering profile is in the format: *<Content filtering profile name>_clone*.

RELATED DOCUMENTATION

[About the Content Filtering Profiles Page | 920](#)

[Edit a Content Filtering Profile | 927](#)

[Delete a Content Filtering Profile | 928](#)

Edit a Content Filtering Profile

You are here: **Security Services > Content Security > Content Filtering Profiles**.

To edit a content filtering profile:

1. Select an existing content filtering profile that you want to edit on the Content Filtering profiles page.
2. Click the pencil icon available on the upper-right corner of the page.

The Edit Content Filtering Profiles page appears with editable fields. For more information on the options, see "[Add a Content Filtering Profile](#)" on page 922 .

NOTE: Alternatively, you can right-click on the selected content filtering profile and select **Edit Profile**.

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[About the Content Filtering Profiles Page | 920](#)

[Add a Content Filtering Profile | 922](#)

[Delete a Content Filtering Profile | 928](#)

Delete a Content Filtering Profile

You are here: **Security Services** > **Content Security** > **Content Filtering Profiles**.

To delete a content filtering profile:

1. Select a content filtering profile that you want to delete on the Content Filtering Profiles page.
2. Click the delete icon available on the upper-right corner of the page.

NOTE: Alternatively, you can right-click on the selected content filtering profile and select **Delete Profile**.

3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the Content Filtering Profiles Page | 920](#)

[Add a Content Filtering Profile | 922](#)

[Edit a Content Filtering Profile | 927](#)

Content Security Custom Objects

IN THIS CHAPTER

- [About the Custom Objects Page | 929](#)
- [Add a MIME Pattern List | 932](#)
- [Add a File Extension List | 934](#)
- [Add a Protocol Command List | 934](#)
- [Add a URL Pattern List | 935](#)
- [Add a URL Category List | 936](#)
- [Add a Custom Message List | 938](#)
- [Clone Custom Objects | 939](#)
- [Edit Custom Objects | 939](#)
- [Delete Custom Objects | 940](#)

About the Custom Objects Page

IN THIS SECTION

- [Tasks You Can Perform | 930](#)
- [Field Descriptions | 931](#)

You are here: **Security Services** > **Content Security** > **Custom Objects**.

Use the Custom Objects page to define your own objects for URL filtering, antivirus filtering, and content filtering.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a MIME pattern list. See ["Add a MIME Pattern List" on page 932](#) .
- Add a file extension list. See ["Add a File Extension List" on page 934](#) .
- Add a protocol command list. See ["Add a Protocol Command List" on page 934](#) .
- Add an URL pattern list. See ["Add a URL Pattern List" on page 935](#) .
- Add an URL category list. See ["Add a URL Category List" on page 936](#) .
- Add a custom message list. See ["Add a Custom Message List" on page 938](#) .
- Edit custom objects. See ["Edit Custom Objects" on page 939](#) .
- Delete custom objects. See ["Delete Custom Objects" on page 940](#) .
- Clone custom objects. See ["Clone Custom Objects" on page 939](#) .
- View the details of custom objects—To do this, select the custom object for which you want to view the details and follow the available options:
 - Click **More** and select **Detailed View**.
 - Right-click on the selected custom object and select **Detailed View**.
 - Mouse over to the left of the selected custom object and click **Detailed View**.
- Filter the custom objects based on select criteria. To do this, select the filter icon at the upper-right corner of the custom objects 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 custom objects table. To do this, click the Show Hide Columns icon in the upper-right corner of the custom objects table and select the options you want to view or deselect the options you want to hide on the page.
- Advance search for custom objects. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

For an advanced search:

1. Enter the search string in the text box.

Based on your input, a list of items from the filter context menu appears.

2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.

3. Press Enter to display the search results in the grid.

Field Descriptions

Table 259 on page 931 describes the fields on the Custom Objects page.

Table 259: Fields on the Custom Objects Page

| Field | Description |
|--------------------------------|---|
| 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 the user-defined protocol command names. |
| Value | Displays only the user-defined protocol command values. |
| URL Pattern List | |

Table 259: Fields on the Custom Objects Page *(Continued)*

| Field | Description |
|---|---|
| Name | Displays only the user-defined URL pattern names. |
| Value | Displays only the user-defined URL pattern values. |
| URL Category List | |
| Name | Displays only the predefined URL categories. |
| Value | Displays only the 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. It also displays the type of action taken when you 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. The options are Redirect-URL or User Message. |
| Content | Displays the content of the custom message. It is either a user message or a URL to which you will be redirected. |

RELATED DOCUMENTATION

| [Add a MIME Pattern List](#) | 932

Add a MIME Pattern List

You are here: **Security Services > Content Security > Custom Objects.**

To add a MIME pattern list:

1. Click the **MIME Pattern List** tab.
2. Click **+** on the upper-right corner of the MIME Pattern List tab.
The Add MIME Pattern List page appears.
3. Complete the configuration according to the guidelines provided in [Table 260 on page 933](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 260: Fields on the Add MIME Pattern List Page

| Field | Action |
|-------|--|
| Name | <p>Enter a name for the MIME pattern list.</p> <p>You can use a string beginning with a letter or underscore and consisting of alphanumeric characters, special characters such as dashes and underscores. The maximum length is 40 characters.</p> |
| Value | <p>To add a MIME pattern value:</p> <ol style="list-style-type: none"> 1. Click +. 2. Enter the MIME pattern value in the Value List. <ul style="list-style-type: none"> NOTE: Value must be two strings separated by slash(/): • The first string beginning with a letter or number and consisting of alphanumeric characters, underscores and dashes. Dashes cannot be shown continuously in the string. • The second string can be null or begin with a letter or number and consisting of alphanumeric characters, underscores, dashes, dots and pluses. Dashes, dots, and pluses cannot be shown continuously in the string. 3. Click the tick mark. <p>If you want to delete any MIME pattern values, select the value and click the delete icon.</p> |

RELATED DOCUMENTATION

[Clone Custom Objects | 939](#)

[Edit Custom Objects | 939](#)

[Delete Custom Objects | 940](#)

Add a File Extension List

You are here: **Security Services > Content Security > Custom Objects.**

To add a file extension list:

1. Click the **File Extension List** tab.
2. Click **+** on the upper-right corner of the File Extension List tab.
The Add File Extension List page appears.
3. Complete the configuration according to the guidelines provided in [Table 261 on page 934](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 261: Fields on the Add File Extension List Page

| Field | Action |
|-------|---|
| Name | <p>Enter a name for the file extension list.</p> <p>You can use a string beginning with a letter or underscore and consisting of alphanumeric characters, special characters such as dashes and underscores. The maximum length is 29 characters.</p> |
| Value | <p>Select values from the list in the Available column to associate it with the file extension name and then click the right arrow to move it to the Selected column.</p> |

RELATED DOCUMENTATION

[Clone Custom Objects | 939](#)

[Edit Custom Objects | 939](#)

[Delete Custom Objects | 940](#)

Add a Protocol Command List

You are here: **Security Services > Content Security > Custom Objects.**

To add a protocol command list:

1. Click the **Protocol Command List** tab.
2. Click **+** on the upper-right corner of the Protocol Command List tab.

The Add Protocol Command List page appears.

3. Complete the configuration according to the guidelines provided in [Table 262 on page 935](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 262: Fields on the Add Protocol Command List Page

| Field | Action |
|-------|--|
| Name | <p>Enter a name for the protocol command list.</p> <p>You can use a string beginning with a letter or underscore and consisting of alphanumeric characters, special characters such as dashes and underscores. The maximum length is 29 characters.</p> |
| Value | <p>To add a protocol command value:</p> <ol style="list-style-type: none"> 1. Click +. 2. Enter the protocol command value in the Value List. 3. Click the tick mark. <p>If you want to delete any protocol command values, select the value and click the delete icon.</p> |

RELATED DOCUMENTATION

[Clone Custom Objects | 939](#)

[Edit Custom Objects | 939](#)

[Delete Custom Objects | 940](#)

Add a URL Pattern List

You are here: **Security Services** > **Content Security** > **Custom Objects**.

To add a URL pattern list:

1. Click the **URL Pattern List** tab.
2. Click + on the upper-right corner of the URL Pattern List tab.

The Add URL Pattern List page appears.

3. Complete the configuration according to the guidelines provided in [Table 263 on page 936](#).

4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 263: Fields on the Add URL Pattern List Page

| Field | Action |
|-------|--|
| Name | <p>Enter a name for the URL pattern list.</p> <p>You can use a string beginning with a letter or underscore and consisting of alphanumeric characters, special characters such as dashes and underscores. The maximum length is 29 characters.</p> <p>NOTE: Multiple URLs are supported in a pattern.</p> |
| Value | <p>To add a URL pattern value:</p> <ol style="list-style-type: none"> 1. Click +. 2. Enter the URL pattern value in the Value List. 3. Click the tick mark. <p>If you want to delete any URL pattern values, select the value and click the delete icon.</p> |

RELATED DOCUMENTATION

[Clone Custom Objects | 939](#)

[Edit Custom Objects | 939](#)

[Delete Custom Objects | 940](#)

Add a URL Category List

You are here: **Security Services > Content Security > Custom Objects**.

To add a URL category list:

1. Click the **URL Category List** tab.
2. Click + on the upper-right corner of the URL Category List tab.
The Add URL Category List page appears.
3. Complete the configuration according to the guidelines provided in [Table 264 on page 937](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

[Table 264 on page 937](#) provides guidelines on using the fields on the Add URL Category List page.

Table 264: Fields on the Add URL Category List Page

| Field | Action |
|-------|---|
| Name | <p>Enter a name for the URL category list.</p> <p>You can use a string beginning with a letter or underscore and consisting of alphanumeric characters, special characters such as dashes and underscores. The maximum length is 59 characters.</p> |
| Value | <p>Select values from the list in the Available column to associate it with the URL category list name and then click the right arrow to move it to the Selected column.</p> <p>To add a new URL pattern inline:</p> <ol style="list-style-type: none"> 1. Click Create New URL Pattern. The Add URL Pattern List page appears. 2. Enter a URL pattern name. You can use a string beginning with a letter or underscore and consisting of alphanumeric characters, special characters such as dashes and underscores. The maximum length is 29 characters. 3. Click + to add a URL pattern value. 4. Enter the URL pattern value in the Value List. 5. Click the tick mark. 6. Optional. If you want to delete any URL pattern values, select the value and click the delete icon. 7. Click OK to save the changes. |

RELATED DOCUMENTATION

[Clone Custom Objects | 939](#)

[Edit Custom Objects | 939](#)

[Delete Custom Objects | 940](#)

Add a Custom Message List

You are here: **Security Services** > **Content Security** > **Custom Objects**.

To add a custom message list:

1. Click the **Custom Message List** tab.
2. Click **+** on the upper-right corner of the Custom Message List tab.
The Add Custom Message List page appears.
3. Complete the configuration according to the guidelines provided in [Table 265 on page 938](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 265: Fields on the Add Custom Message List Page

| Field | Action |
|---------|---|
| Name | <p>Enter a name for the custom message list.</p> <p>You can use a string beginning with a letter or underscore and consisting of alphanumeric characters, special characters such as dashes and underscores. The maximum length is 59 characters.</p> |
| Type | <p>Select an option:</p> <ul style="list-style-type: none"> • Redirect URL—Specifies custom redirect URL server. • User Message—Specifies that website access has been blocked by an organization's access policy. |
| Content | <p>Enter content of the custom message; maximum length is 1024 characters. It is either a user message or a URL to which you will be redirected.</p> |

RELATED DOCUMENTATION

[Clone Custom Objects | 939](#)

[Edit Custom Objects | 939](#)

[Delete Custom Objects | 940](#)

Clone Custom Objects

You are here: **Security Services** > **Content Security** > **Custom Objects**.

You can clone all of the following custom objects:

- MIME pattern list
- File extension list
- Protocol command list
- URL pattern list
- URL category list
- Custom message list

To clone a custom object:

1. Right-click any of the custom objects and select **Clone**. You can also select **Clone** from the More link.
The clone page for the selected custom object appears with editable fields.
2. Make the required changes in the editable fields.
3. Click **OK** to save the changes.

A cloned custom object is created for the selected custom objects. By default, the name of the cloned custom objects is in the format: *<custom objects name>_clone*.

RELATED DOCUMENTATION

[Add a MIME Pattern List | 932](#)

[Add a File Extension List | 934](#)

[Add a Protocol Command List | 934](#)

[Add a URL Pattern List | 935](#)

[Add a URL Category List | 936](#)

[Add a Custom Message List | 938](#)

Edit Custom Objects

You are here: **Security Services** > **Content Security** > **Custom Objects**.

You can edit all of the following custom objects:

- MIME pattern list
- File extension list
- Protocol command list
- URL pattern list
- URL category list
- Custom message list

To edit a custom objects:

1. Select any of the existing custom objects that you want to edit on the Custom Objects page.
2. Click the pencil icon available on the upper-right corner of the page.
The edit page for the selected custom object appears with editable fields. You can modify the parameters of the custom object as required.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

RELATED DOCUMENTATION

[Add a MIME Pattern List | 932](#)

[Add a File Extension List | 934](#)

[Add a Protocol Command List | 934](#)

[Add a URL Pattern List | 935](#)

[Add a URL Category List | 936](#)

[Add a Custom Message List | 938](#)

Delete Custom Objects

You are here: **Security Services > Content Security > Custom Objects**.

You can delete all of the following custom objects:

- MIME pattern list
- File extension list
- Protocol command list

- URL pattern list
- URL category list
- Custom message list

To delete a custom object:

1. Select any of the existing custom objects that you want to delete from the Custom Objects page.
2. Click the delete icon available on the upper-right corner of the page.
3. Click **Yes** to delete or click **No** to retain the selected custom object.

RELATED DOCUMENTATION

[About the Custom Objects Page | 929](#)

[Clone Custom Objects | 939](#)

[Edit Custom Objects | 939](#)

Content Security Policies

IN THIS CHAPTER

- [About the Content Security Policies Page | 942](#)
- [Create a Content Security Policy | 944](#)
- [Clone a Content Security Policy | 947](#)
- [Edit a Content Security Policy | 948](#)
- [Delete a Content Security Policy | 948](#)

About the Content Security Policies Page

IN THIS SECTION

- [Tasks You Can Perform | 942](#)
- [Field Descriptions | 943](#)

You are here: **Security Services > Content Security > Content Security Policies.**

Use this page to configure Content Security Policies.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a Content Security policy. See "[Create a Content Security Policy](#)" on page 944 .
- Clone a Content Security policy. See "[Clone a Content Security Policy](#)" on page 947 .
- Edit a Content Security policy. See "[Edit a Content Security Policy](#)" on page 948 .

- Delete a Content Security policy. See "[Delete a Content Security Policy](#)" on page 948 .
- View the details of a Content Security policy—To do this, select the Content Security policy for which you want to view the details and select any of the following options:
 - Click **More** and select **Detailed View**.
 - Right-click on the selected Content Security policy and select **Detailed View**.
 - Mouse over to the left of the selected Content Security policy and click **Detailed View**.
- Advanced search for Content Security policy. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

For an advanced search:

1. Enter the search string in the text box.

Based on your input, a list of items from the filter context menu appears.

2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.

3. Press Enter to display the search results in the grid.
- Show or hide columns in the Content Security Policies table. To do this, click the Show Hide Columns icon in the upper-right corner of the Content Security policies table and select the options you want to view or deselect the options you want to hide on the page.

Field Descriptions

[Table 266 on page 944](#) describes the fields on the Content Security Policies page.

Table 266: Fields on the Content Security Policies Page

| Field | Description |
|-------------------|--|
| Name | Displays the Content Security policy name. |
| Antivirus | Displays the antivirus profile. |
| Web Filtering | Displays the Web filtering profile. |
| Antispam | Displays the antispam profile. |
| Content Filtering | Displays the content filtering profiles. |

RELATED DOCUMENTATION

[Create a Content Security Policy | 944](#)

Create a Content Security Policy

You are here: **Security Services > Content Security > Content Security Policies.**

To add a Content Security policy:

1. Click **+** on the upper-right corner of the Content Security Policies page.
The Create a Content Security Policy page appears.
2. Complete the configuration according to the guidelines provided in [Table 267 on page 945](#).
3. Click **Finish**.
The Summary page is displayed with the configurations you have made.
4. Review the settings, and if you need to make any modifications, click the **Edit** link or the **Back** button.
5. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.
A Content Security policy is created.

Table 267: Fields on the Create a Content Security Policy Page

| Field | Action |
|--|---|
| General—General Information | |
| Name | Enter a Content Security policy name. |
| Antivirus—Antivirus Profiles by Traffic Protocol | |
| Apply to all protocols | Select the check box to apply the default profile to all protocols such as HTTP, FTP, IMAP, SMTP, and POP3. If you do not select the check box, you can apply different profiles to different protocols. |
| HTTP | Select an option from the list to specify the Content Security policy for the HTTP protocol to be scanned. |
| FTP Upload | Select an option from the list to specify the Content Security policy for the FTP protocol to be scanned. |
| FTP Download | Select an option from the list to specify the Content Security policy for the FTP protocol to be scanned. |
| IMAP | Select an option from the list to specify the Content Security policy for the IMAP protocol to be scanned. |
| SMTP | Select an option from the list to specify the Content Security policy for the SMTP protocol to be scanned. |
| POP3 | Select an option from the list to specify the Content Security policy for the POP3 protocol to be scanned. |
| Create Another Profile | Click Create Another Profile to create an antivirus profile inline. For more information on the fields, see " Add an Antivirus Profile " on page 855 . |
| Web Filterings—Web Filtering Profiles by Traffic Protocol | |

Table 267: Fields on the Create a Content Security Policy Page (Continued)

| Field | Action |
|------------------------|---|
| HTTP | Select an option from the list to specify the Content Security policy for the HTTP protocol to be scanned. |
| Create Another Profile | Click Create Another Profile to create Web filtering profile inline. For more information on the fields, see "Add a Web Filtering Profile" on page 887 . |

Antispam—Antispam Profiles by Traffic Protocol

| | |
|------------------------|--|
| SMTP profile | Select an option from the list to specify the Content Security policy for the SMTP protocol to be scanned. |
| Create Another Profile | Click Create Another Profile to create antispam profile inline. For more information on the fields, see "Add an Antispam Profile" on page 916 . |

Content Filtering—Content Filtering Profiles by Traffic Protocol

| | |
|------------------------|---|
| Apply to all protocols | Select the check box to apply the default profile to all protocols such as HTTP, FTP, IMAP, SMTP, and POP3. If you do not select the check box, you can apply different profiles to different protocols. |
| HTTP | Select an option from the list to specify the Content Security policy for the HTTP protocol to be scanned. |
| FTP Upload | Select an option from the list to specify the Content Security policy for the FTP protocol to be scanned. |
| FTP Download | Select an option from the list to specify the Content Security policy for the FTP protocol to be scanned. |
| IMAP | Select an option from the list to specify the Content Security policy for the IMAP protocol to be scanned. |

Table 267: Fields on the Create a Content Security Policy Page (Continued)

| Field | Action |
|------------------------|---|
| SMTP | Select an option from the list to specify the Content Security policy for the SMTP protocol to be scanned. |
| POP3 | Select an option from the list to specify the Content Security policy for the POP3 protocol to be scanned. |
| Create Another Profile | Click Create Another Profile to create content filtering Profile inline. For more information on the fields, see " Add a Content Filtering Profile " on page 922 . |

RELATED DOCUMENTATION

[About the Content Security Policies Page | 942](#)

[Clone a Content Security Policy | 947](#)

[Edit a Content Security Policy | 948](#)

[Delete a Content Security Policy | 948](#)

Clone a Content Security Policy

You are here: **Security Services** > **Content Security** > **Content Security Policies**.

To clone a Content Security policy:

1. Select a Content Security policy that you want to clone and select **Clone** from the More link.

NOTE: Alternatively, you can right-click on the selected Content Security policy and select **Clone**.

The Clone Content Security Policies page appears with editable fields. For more information on the fields, see "[Create a Content Security Policy](#)" on page 944 .

2. Click **OK** to save the changes.

A cloned Content Security policy is created for the selected Content Security policy. By default, the name of the cloned Content Security policy is in the format: *<Content Security policy name>_clone*.

RELATED DOCUMENTATION

[About the Content Security Policies Page | 942](#)

[Edit a Content Security Policy | 948](#)

[Delete a Content Security Policy | 948](#)

Edit a Content Security Policy

You are here: **Security Services > Content Security > Content Security Policies.**

To edit a Content Security policy:

1. Select an existing Content Security policy that you want to edit on the Content Security Policies page.
2. Click the pencil icon available on the upper-right corner of the page.

The Edit Content Security Policies page appears with editable fields. For more information on the options, see "[Create a Content Security Policy](#)" on page 944 .

NOTE: Alternatively, you can right-click on the selected Content Security policy and select **Edit Policy**.

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[About the Content Security Policies Page | 942](#)

[Delete a Content Security Policy | 948](#)

Delete a Content Security Policy

You are here: **Security Services > Content Security > Content Security Policies.**

To delete a Content Security policy:

1. Select a Content Security policy that you want to delete on the Content Security Policies page.
2. Click the delete icon available on the upper-right corner of the page.

NOTE: Alternatively, you can right-click on the selected Content Security policy and select **Delete Policy**.

3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the Content Security Policies Page | 942](#)

[Clone a Content Security Policy | 947](#)

[Create a Content Security Policy | 944](#)

IPS Policies

IN THIS CHAPTER

- [About the IPS Policies Page | 950](#)
- [Import IPS Predefined Policies | 952](#)
- [Add an IPS Policy | 953](#)
- [Clone an IPS Policy | 953](#)
- [Edit an IPS Policy | 954](#)
- [Delete an IPS Policy | 955](#)
- [Add Rules to an IPS Policy | 955](#)
- [Edit an IPS Policy Rule | 965](#)
- [Delete an IPS Policy Rule | 966](#)

About the IPS Policies Page

IN THIS SECTION

- [Tasks You Can Perform | 951](#)
- [Field Descriptions | 951](#)

You are here: **Security Services > IPS > Policies.**

An intrusion prevention system (IPS) policy defines how your device handles the network traffic. It allows you to enforce various attack detection and prevention techniques on traffic traversing your network. You can define policy rules to match a section of traffic based on a zone, network, and application, and then take active or passive preventive actions on that traffic.

Tasks You Can Perform

You can perform the following tasks from this page:

- Import predefined policies. See ["Import IPS Predefined Policies" on page 952](#) .
- Set an IPS policy as default policy. To do this, select an existing IPS policy and click **More > Set Default**.
- Create an IPS policy. See ["Add an IPS Policy" on page 953](#) .

NOTE: IPS 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.

- Edit an IPS policy. See ["Edit an IPS Policy" on page 954](#) .
- Delete an IPS policy. See ["Delete an IPS Policy" on page 955](#) .
- Clone an IPS policy. See ["Clone an IPS Policy" on page 953](#) .
- Add rules to the IPS policy. See ["Add Rules to an IPS Policy" on page 955](#) .
- Edit an IPS policy rule. See ["Edit an IPS Policy Rule" on page 965](#) .
- Delete an IPS policy rule. See ["Delete an IPS Policy Rule" on page 966](#) .
- Search a policy. To do this:
 1. Click the search icon in the upper-right corner of the IPS Policies table.
 2. Enter the policy name that you want to find and click the search icon.

Based on your input, a list of matching policies appears.
- Show or hide columns in the IPS Policies table. To do this, click the Show Hide Columns icon in the upper-right corner of the IPS Policies table and select the options you want to view or deselect the options you want to hide on the page.

Field Descriptions

[Table 268 on page 952](#) describes the fields on the IPS Policies page.

Table 268: Fields on the IPS Policies Page

| Field | Description |
|----------------------|--|
| Policy Name | Displays the IPS policy name. |
| Rules | Displays the number of rules that are configured for the policy or allows you to add new rules to the policy. |
| Predefined or Custom | Displays if the IPS policy is a predefined or a custom policy. NOTE: This option is not available for logical systems and tenants. |

RELATED DOCUMENTATION

[Add an IPS Policy | 953](#)

[Add Rules to an IPS Policy | 955](#)

[Edit an IPS Policy | 954](#)

[Delete an IPS Policy | 955](#)

[Clone an IPS Policy | 953](#)

Import IPS Predefined Policies

The predefined policies are templates which can be used as a guideline. Each template is set of rules of a specific rulebase type that you can clone and then update to meet your needs. Use this page to import the IPS predefined policies.

NOTE: This option is not available for logical systems and tenants.

To import the predefined policy templates:

1. Click **Import Predefined Policies** at the upper-right corner of the IPS Policies page.
The Import Predefined Policies page appears.
2. Select the predefined policy templates from the Available column that you want to import.
3. Click on the right arrow to move the selected predefined policy templates to the Selected column.

4. Click **OK**.

The imported predefined policy template are displayed in the IPS Policies page.

RELATED DOCUMENTATION

[About the IPS Policies Page | 950](#)

[Add an IPS Policy | 953](#)

[Add Rules to an IPS Policy | 955](#)

Add an IPS Policy

You are here: **Security Services > IPS > Policies**.

To add an IPS policy:

1. Click **+** on the upper-right corner of the IPS Policies page.
The Create IPS Policy page appears.
2. Enter a name for the IPS policy.
Name of the IPS policy must be a unique string of alphanumeric and special characters, including colons, periods, hyphens, and underscores; 250-character maximum.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.
The IPS policy is displayed on the IPS Policies page.

RELATED DOCUMENTATION

[About the IPS Policies Page | 950](#)

[Add Rules to an IPS Policy | 955](#)

[Edit an IPS Policy | 954](#)

[Delete an IPS Policy | 955](#)

[Clone an IPS Policy | 953](#)

Clone an IPS Policy

You are here: **Security Services > IPS > Policies**.

To clone an IDP policy:

1. Select an IPS policy that you want to clone and click **More** > **Clone** on the upper-right corner of the IPS Policies page.

The Clone IPS Policy page appears with the editable name field. By default, the clone name will show as *<IPS policy name>_clone*.

2. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

You can see the cloned IPS policy on the IPS Policies page. You can edit the rules of the cloned IPS policy. For more information on the IPS policy and its rules, see ["Add an IPS Policy" on page 953](#) and ["Add Rules to an IPS Policy" on page 955](#).

RELATED DOCUMENTATION

[About the IPS Policies Page | 950](#)

[Edit an IPS Policy | 954](#)

[Delete an IPS Policy | 955](#)

[Add Rules to an IPS Policy | 955](#)

[Edit an IPS Policy Rule | 965](#)

Edit an IPS Policy

You are here: **Security Services** > **IPS** > **Policies**.

To edit an IPS policy:

1. Select an existing IPS policy that you want to edit on the IPS Policies page.
2. Click the pencil icon available on the upper-right corner of the page.

The Edit IPS Policy page appears with editable fields. For more information on the options, see ["Add an IPS Policy" on page 953](#).

NOTE: Alternatively, you can right-click on the selected IPS policy and select **Edit**.

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[About the IPS Policies Page | 950](#)

[Add an IPS Policy | 953](#)

[Add Rules to an IPS Policy | 955](#)

[Clone an IPS Policy | 953](#)

[Delete an IPS Policy | 955](#)

Delete an IPS Policy

You are here: **Security Services** > **IPS** > **Policies**.

To delete an IPS policy:

1. Select an IPS policy that you want to delete on the IPS Policies page.
2. Click the delete icon available on the upper-right corner of the page.

NOTE: Alternatively, you can right-click on the selected IPS policy and select **Delete**.

3. Click **Yes** to delete or click **No** to retain the policy.

RELATED DOCUMENTATION

[About the IPS Policies Page | 950](#)

[Add an IPS Policy | 953](#)

[Add Rules to an IPS Policy | 955](#)

[Edit an IPS Policy | 954](#)

[Clone an IPS Policy | 953](#)

Add Rules to an IPS Policy

You are here: **Security Services** > **IPS** > **Policies**.

To add rules to an IPS policy:

NOTE: You can only add rules for the custom IPS policies.

1. Click **Add Rules** or on the rule number available next to the column of your IPS policy name.
The IPS Rules page appears.
2. Click **+** on the upper-right corner of the IPS Rules or Exempt Rules page.
The IPS Rules or Exempt Rules page with the inline editable fields will appear.
3. Complete the configuration according to the guidelines provided in [Table 269 on page 956](#) .
4. Click the tick icon on the right-side of the row once done with the configuration.
Once you configure the IPS policy rules, you can associate the IPS policy with the security policy.

Table 269: Fields on the IPS Rules or Exempt Rules Page

| Field | Action |
|-------------------------|---|
| Rule Name | Enter the rule name for the IPS policy. |
| Description | Enter the description for the rule. |
| Network Criteria | |
| Sources | |
| Source zone | <p>Select a source zone to be associated with the IPS policy:</p> <ul style="list-style-type: none"> • Not configured—Matches the configured source zone from firewall policy. • Any—Matches any source zone from firewall policy. • Specific—Select a source zone from the list where network traffic originates. |
| Source addresses | <p>Select a source address to be associated with the IPS policy:</p> <ul style="list-style-type: none"> • Not configured—Matches the configured source IP address from firewall policy. • Any—Matches any source IP address from firewall policy. • Specific—A source IP address from which network traffic originates. <p>Select the addresses from the Available column and then click the right arrow to move it to the Selected column. You can select Exclude Selected to exclude only the selected address from the list.</p> |
| Destinations | |

Table 269: Fields on the IPS Rules or Exempt Rules Page (Continued)

| Field | Action |
|-----------------------|--|
| Destination zone | <p>Select a destination zone to be associated with the IPS policy:</p> <ul style="list-style-type: none"> • Not configured—Matches the configured destination zone from firewall policy. • Any—Matches any destination zone from firewall policy. • Specific—Select a destination zone from the list to which network traffic is sent. |
| Destination addresses | <p>Select a destination address to be associated with the IPS policy:</p> <ul style="list-style-type: none"> • Not configured—Matches the configured destination IP address from firewall policy. • Any—Matches any destination IP address from firewall policy. • Specific—A destination IP address to which the network traffic is sent. <p>Select the addresses from the Available column and then click the right arrow to move it to the Selected column. You can select Exclude Selected to exclude only the selected address from the list.</p> |
| IPS Signatures | |
| Add | Select predefined or custom signatures from the list to add it to the IPS policy rules. |
| Delete | Select the IPS signatures you do not want to add to the IPS policy rules and click the delete icon. |
| Name | Displays name of the IPS predefined or custom signatures. |
| Category | Displays the predefined attack or attack groups categories. For example, App, HTTP, and LDAP. |
| Severity | Displays the attack severity level that the signature reports. |
| Attack Type | Displays the attack type (signature or anomaly). |

Table 269: Fields on the IPS Rules or Exempt Rules Page *(Continued)*

| Field | Action |
|----------------------------------|--|
| Recommended Action | Displays the specified action taken from the device when it detects an attack. For example, ignore and drop. |
| Type | Displays if the IPS signature type is predefined or custom. |
| Add Predefined Signatures | |
| View by | View and select the desired predefined attacks or attack groups and click OK to add it to the selected IPS policy. |
| Show or Hide Columns | Use the Show Hide Columns icon in the upper-right corner of the page and select the options you want to show or deselect to hide options on the page. |
| Name | Displays name of the predefined attack objects or attack object group. |
| Category | Displays the predefined attack or attack groups categories. For example, App, HTTP, and LDAP. |
| Severity | Displays the attack severity level that the signature reports. |
| Type Attack | Displays the attack type (signature or anomaly). |
| Recommended | Displays the added predefined attacks recommended by Juniper Networks to the dynamic attack group. |
| Recommended Action | Displays the specified action taken from the device when it detects an attack. For example, ignore and drop. |
| Performance | Displays a performance filter (fast, normal, slow, and unknown) to add attack objects based on the performance level that is vulnerable to the attack. |
| Direction | Displays the connection direction (any, client-to-server, or server-to-client) of the attack. |

Table 269: Fields on the IPS Rules or Exempt Rules Page *(Continued)*

| Field | Action |
|---|---|
| Add Custom Signatures | |
| View by | View and select the desired custom attacks, static groups, or dynamic groups and click OK to add it to the selected IPS policy. |
| Custom Signatures—Custom Attacks | |
| Name | Displays the custom attack object name. |
| Severity | Displays the attack severity level that the signature reports. |
| Attack Type | Displays the attack type (signature or anomaly). |
| Recommended Action | Displays the specified action taken from the device when it detects an attack. For example, ignore and drop. |
| Custom Signatures—Static Group | |
| Name | Displays static group name for the custom signatures. |
| Group Members | Displays the name of the attack object or group attack object. The members can be predefined attacks, predefined attack groups, custom attacks, or custom dynamic groups. |
| Custom Signatures—Dynamic Groups | |
| Name | Displays dynamic group name for the custom signatures. |
| Attack Prefix | Displays prefix match for attack names. For example: HTTP:* |
| Severity | Displays the attack severity level that the signature reports. |

Table 269: Fields on the IPS Rules or Exempt Rules Page (Continued)

| Field | Action |
|-------------|---|
| Attack Type | Displays the attack type (signature or anomaly). |
| Category | Displays the dynamic attack groups categories. For example, App, HTTP, and LDAP. |
| Direction | Displays the connection direction (any, client-to-server, or server-to-client) of the attack. |

Table 269: Fields on the IPS Rules or Exempt Rules Page *(Continued)*

| Field | Action |
|----------------|--|
| Action | <p>NOTE: This option is not available for exempt rules.</p> <p>Select any one of the actions from the list:</p> <ul style="list-style-type: none"> • Recommended (default)—All predefined attack objects have a default action associated with them. This is the action that we recommend when that attack is detected. • No Action—No action is taken. Use this action when you want to only generate logs for some traffic. • Drop Connection—Drops all packets associated with the connection, preventing traffic for the connection from reaching its destination. Use this action to drop connections for traffic that is not prone to spoofing. • Drop Packet—Drops a matching packet before it can reach its destination but does not close the connection. Use this action to drop packets for attacks in traffic that is prone to spoofing, such as UDP traffic. Dropping a connection for such traffic could result in a denial of service that prevents you from receiving traffic from a legitimate source-IP address. • Close Client—Closes the connection and sends an RST packet to the client but not to the server. • Close Server—Closes the connection and sends an RST packet to the server but not to the client. • Close Client & Server—Closes the connection and sends an RST packet to both the client and the server. • Ignore Connection—Stops scanning traffic for the rest of the connection if an attack match is found. IPS disables the rulebase for the specific connection. • Mark DiffServ—Assigns the indicated service-differentiation value to the packet in an attack, then passes them on normally. |
| Options | <p>NOTE: This option is not available for exempt rules.</p> |
| Log Attacks | Enable the log attacks to create a log record that appears in the log viewer. |

Table 269: Fields on the IPS Rules or Exempt Rules Page (Continued)

| Field | Action |
|-------------|---|
| Log Packets | Enable the log packets to capture the packets received before and after the attack for further offline analysis of attacker behavior. |

Advanced

NOTE: This option is not available for exempt rules.

Threat Profiling

NOTE: Feeds are only displayed if you have enrolled to Juniper ATP Cloud. You can also download the feeds using the command, `request services security-intelligence download`.

| | |
|----------------------|--|
| Add attacker to feed | Select from the list to add the attackers IP addresses to the feed to configure IPS rule with threat profiles. |
| Add target to feed | Select from the list to add the target IP addresses to the feed to configure IPS rule with threat profiles. |

Notifications

| | |
|---------------------|--|
| Packets before | Enter the number of packets processed before the attack is captured. Range: 1 through 255. Default is 1. NOTE: This option is available when you enable Log Packets. |
| Packets after | Enter the number of packets processed after the attack is captured. Range: 0 through 255. Default is 1. NOTE: This option is available when you enable Log Packets. |
| Post window timeout | Enter the time limit for capturing post-attack packets for a session. No packet capture is conducted after the timeout has expired. Range: 0 through 1800 seconds. Default is 1 second. NOTE: This option is available when you enable Log Packets. |

Table 269: Fields on the IPS Rules or Exempt Rules Page *(Continued)*

| Field | Action |
|-------------------|--|
| Alert Flag | <p>Enable this option to set an alert flag in the Alert column of the Log Viewer for the matching log record.</p> <p>NOTE: This option is available when you enable Log Attacks.</p> |
| IP Actions | |
| Action | <p>Specifies the action that IPS takes against future connections that use the same IP address.</p> <p>Select an IP action from the list:</p> <ul style="list-style-type: none"> • None—Do not take any action, which is the default setting. • Notify—Don't take any action on future traffic but log the event. • Close—Close future connections of new sessions that match the IP address by sending RST packets to the client and server. • Block—Block future connections of any session that matches the IP address. |

Table 269: Fields on the IPS Rules or Exempt Rules Page *(Continued)*

| Field | Action |
|-----------------------------|--|
| IP Target | <p>Configure how the traffic should be matched to the configured IP actions.</p> <p>Select an IP target from the list:</p> <ul style="list-style-type: none"> • None—Do not match any traffic. • Destination address—Match traffic based on the destination IP address of the attack traffic. • Service—For TCP and UDP, match traffic based on the source IP address, source port, destination IP address, and destination port of the attack traffic. • Source address—Match traffic based on the source IP address of the attack traffic. • Source zone—Match traffic based on the source zone of the attack traffic. • Source zone address—Match traffic based on the source zone and source IP address of the attack traffic. • Zone service—Match traffic based on the source zone, destination IP address, destination port, and protocol of the attack traffic. |
| Refresh timeout | <p>Enable refresh of the IP action timeout (that you specify in the Timeout field) if future traffic matches the configured IP actions.</p> |
| Timeout | <p>Specifies the number of seconds the IP action should remain effective before new sessions are initiated within that specified timeout value.</p> <p>Enter the timeout value, in seconds. The maximum value is 65,535 seconds. Default is 300 seconds.</p> |
| Log IP-Action hits | <p>Enable to log information about the IP action against the traffic that matches a rule. By default, this setting is disabled.</p> |
| Log IP-Action rule creation | <p>Enable to generate an event when the IP action filter is triggered. By default, this setting is disabled.</p> |
| Rule Modifiers | |

Table 269: Fields on the IPS Rules or Exempt Rules Page *(Continued)*

| Field | Action |
|-------------------|---|
| Severity override | Severity level (None, Critical, Info, Major, Minor, Warning) to override the inherited attack severity in the rules. The most dangerous level is critical, which attempts to crash your server or gain control of your network. Informational level is least dangerous and is used by network administrators to find flaws in their security systems. |
| Terminal matching | Enable to mark an IPS rule as terminal. When a terminal rule is matched, the device stops matching for the remaining rules in that IPS policy. |

RELATED DOCUMENTATION

[About the IPS Policies Page | 950](#)

[Edit an IPS Policy Rule | 965](#)

[Delete an IPS Policy Rule | 966](#)

[Add an IPS Policy | 953](#)

[Clone an IPS Policy | 953](#)

[Delete an IPS Policy | 955](#)

Edit an IPS Policy Rule

You are here: **Security Services > IPS > Policies.**

To edit an IPS policy rule:

1. Click on the existing IPS policy rule on the IPS Policies page.
The IPS Rules page appears.
2. Select the IPS or exempt rules you want to edit.
3. Click the pencil icon available on the upper-right corner of the page.
Editable fields on the IPS Rules or Exempt Rules page appears.

NOTE: Alternatively, you can right-click on the selected IPS policy and select **Edit**.

4. Edit the required options and click the tick icon on the right-side of the row once done with the configuration.

For more information on the rules options, see ["Add Rules to an IPS Policy" on page 955](#) .

The selected IPS policy rules are edited.

RELATED DOCUMENTATION

[About the IPS Policies Page | 950](#)

[Delete an IPS Policy Rule | 966](#)

[Add an IPS Policy | 953](#)

[Add Rules to an IPS Policy | 955](#)

[Clone an IPS Policy | 953](#)

[Delete an IPS Policy | 955](#)

Delete an IPS Policy Rule

You are here: **Security Services > IPS > Policies**.

To delete an IPS policy rule:

1. Click on the existing IPS policy rule on the IPS Policies page.
The IPS Rules page appears.
2. Select the IPS or exempt rules you want to delete.
3. Click the delete icon available on the upper-right corner of the page.
4. Click **Yes** to delete or click **No** to retain the rule.

RELATED DOCUMENTATION

[About the IPS Policies Page | 950](#)

[Edit an IPS Policy Rule | 965](#)

[Add an IPS Policy | 953](#)

[Add Rules to an IPS Policy | 955](#)

[Clone an IPS Policy | 953](#)

[Delete an IPS Policy | 955](#)

IPS Signatures

IN THIS CHAPTER

- [About the IPS Signatures Page | 967](#)
- [Import Snort Rules | 972](#)
- [Create a Custom IPS Signature | 973](#)
- [Create IPS Signature Static Groups | 989](#)
- [Create IPS Signature Dynamic Group | 992](#)
- [Clone an IPS Signature | 997](#)
- [Edit an IPS Signature | 998](#)
- [Delete an IPS Signature | 999](#)

About the IPS Signatures Page

IN THIS SECTION

- [Tasks You Can Perform | 968](#)
- [Field Descriptions | 969](#)

You are here: **Security Services > IPS > Signatures.**

The intrusion prevention system (IPS) compares traffic against signatures of known threats and blocks traffic when a threat is detected. Network intrusions are attacks on, or other misuses of, network resources. To detect such activity, IPS uses signatures. A signature specifies the types of network intrusions that the device should detect and report. Whenever a traffic pattern matches a signature, IPS triggers the alarm and blocks the traffic from reaching its destination. One of the key components of IPS is the signature database. It contains definitions of different objects that is used in defining IPS policy rules, such as attack objects, application signature objects, and service objects.

You can group the attack objects to keep IPS policies organized and manageable. An attack object group can contain one or more types of attack objects. Junos OS supports the following three types of attack groups:

- **IPS signature**—Contains objects present in the signature database.
- **Dynamic group**—Contains attack objects that meets the specified matching criteria. During a signature update, dynamic group membership is automatically updated based on the matching criteria for that group. For example, you can dynamically group the attacks that are related to a specific application using dynamic attack group filters.
- **Static group**—Contains a list of attacks that are specified in the attack definition.

Tasks You Can Perform

You can perform the following tasks from this page:

- Associate IPS signatures to IPS policies. To do this, click **IPS Policies** link available below the IPS Signatures page title to directly navigate to the IPS Policies page. Then, click **Add rules** to assign the IPS signature to a specific policy. For more information, see ["Add Rules to an IPS Policy" on page 955](#).
- View the list of IPS signature predefined attacks or attack groups. To do this, click the **PREDEFINED** tab and select **Predefined Attacks** or **Predefined Attack Group** from the View by list.
- View the details of a predefined IPS signature. To do this, select an existing IPS signature on the PREDEFINED tab and follow the available options:
 - Click **More** and select **Detailed View**.
 - Right-click on the selected IPS signature and select **Detailed View**.
 - Hover over to the left of the selected IPS signature name and click the **Detailed View** icon.
- View the custom signatures of custom attacks, static groups, or dynamic groups. To do this, click the **CUSTOM** tab and select **Custom Attacks**, **Static Groups**, or **Dynamic Groups** from the View by list.
- Import snort rules to convert them as custom attacks. See ["Import Snort Rules" on page 972](#).
- Create IPS signature custom attacks. See ["Create a Custom IPS Signature" on page 973](#).
- Create IPS signature static groups. See ["Create IPS Signature Static Groups" on page 989](#).
- Create IPS signature dynamic groups. See ["Create IPS Signature Dynamic Group" on page 992](#).
- View the details of an IPS signature for custom attacks, static groups, and dynamic groups. To do this, select an existing IPS signature, static group, or dynamic group on the CUSTOM tab and follow the available options:

- Click **More** and select **Detailed View**.
- Right-click on the selected IPS signature and select **Detailed View**.
- Hover over to the left of the selected IPS signature and click **Detailed View**.
- Clone an IPS signature. See "[Clone an IPS Signature](#)" on page 997 .
- Edit an IPS signature. See "[Edit an IPS Signature](#)" on page 998 .
- Delete an IPS signature. See "[Delete an IPS Signature](#)" on page 999 .
- Show or hide columns in the Predefined table. To do this, click the Show Hide Columns icon in the upper-right corner of the Predefined table. Then, select the options you want to view or clear the options you want to hide on the page.
- Advanced search for predefined or custom IPS signatures. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

For an advanced search:

1. Enter the search string in the text box.

Based on your input, a list of items from the filter context menu appears.

2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

NOTE: Press spacebar to add an AND operator or OR operator to the search string. Predefined signatures support only the AND operator. Press backspace at any time when typing a search criteria to delete only one character.

3. Press **Enter** to display the search results in the grid.

Field Descriptions

[Table 270 on page 970](#) and [Table 271 on page 971](#) describes the fields on the IPS Signatures page.

Table 270: Fields on the PREDEFINED Tab

| Field | Description |
|--------------------|--|
| Name | Displays the name of the predefined IPS signature. |
| Category | Displays the category of the attack object. |
| Severity | Displays the severity level of the attack that the signature will report. |
| Attack Type | Displays if the type of attack object is signature, anomaly, or chain. NOTE: This field is applicable only for predefined attacks. |
| Type Attack | Displays if the attack type is static or dynamic group. NOTE: This field is applicable only for predefined attack groups. |
| Recommended | Indicates whether the attack objects are recommended by Juniper (True) or not (False). |
| Recommended Action | Displays the action or actions taken when the monitored traffic matches the attack objects specified in the IPS rules. |
| False Positive | Displays the frequency or frequencies with which the attack produces a false positive on your network. |
| Performance | Displays the IPS signature performance impact filter or filters. |
| Direction | Displays the traffic direction or traffic directions for which the attack is detected. For example, client to server. |
| Service | Displays the protocol, service, or list of both protocol and services that the attack uses to enter your network. |

Table 271: Fields on the Custom Tab

| Field | Description |
|-------|-------------|
|-------|-------------|

View by: Custom Attacks

| | |
|--------------------|---|
| Name | Displays the name of the custom attack IPS signature. |
| Severity | Displays the severity level of the attack that the signature will report. |
| Attack Type | Displays if the type of attack object is signature, anomaly, or chain. |
| Recommended Action | Displays the action taken when the monitored traffic matches the attack objects specified in the IPS rules. |

View by: Static Groups

| | |
|---------------|--|
| Name | Displays the name of the static group IPS signature. |
| Group Members | Displays the IPS signatures or IPS signature dynamic groups that are part of the IPS static group. |

View by: Dynamic Groups

| | |
|---------------|--|
| Name | Displays the name of the dynamic group IPS signature. |
| Attack Prefix | Displays the value or values for attack name prefix match. |
| Severity | Displays the severity level or severity levels of the attack that the signature will report. |
| Attack Type | Displays if the type of attack object is signature, anomaly, or chain. |
| Category | Displays the category or categories of the attack object. |

Table 271: Fields on the Custom Tab (Continued)

| Field | Description |
|--------------------|---|
| Direction | Displays the traffic direction or traffic directions for which the attack is detected. For example, client to server. |
| Attack Excluded | Displays the excluded attack or attacks that are part of the database updates. |
| File Type | Displays the attack file type or file types that are used as a dynamic group filter. |
| False Positive | Displays the frequency or frequencies with which the attack produces a false positive on your network. |
| Recommended | Indicates whether the attack objects are recommended by Juniper (True) or not (False). |
| Service | Displays the protocol, service, or list of protocols and services that the attack uses to enter your network. |
| Vendor | Displays the vendor or product that the attack belongs to. |
| Vulnerability Type | Displays the attack vulnerability type or vulnerability types that are used as a dynamic group filter. |
| Performance | Performance impact filter or filters used for the dynamic group. |
| CVSS Score | Displays the Common Vulnerability Scoring System (CVSS) score or scores that is used as a dynamic group filter. |
| Age of attack | Displays the age of the attack (in years) that is used as a dynamic group filter. |

Import Snort Rules

Snort is an open-source intrusion prevention system (IPS) and help detect malicious attacks. You can convert the Snort IPS rules into Juniper IPS custom attack signatures using the Juniper Integration of

Snort Tool (JIST). By default, Junos OS includes the JIST. The tool supports Snort version 2 and version 3 rules.

To import the Snort rules:

1. Click the **CUSTOM** tab on the IPS Signatures page.
2. Click **Import Snort Rules** at the upper-right corner of the Custom Signatures page.

NOTE: This option is only available if you have selected **Custom Attacks** in the View by list.

The Import Snort Rules page appears.

3. Click **Browse** and select the file to upload the Snort rules file and click **OK**.

The supported file formats are: .rules, .txt, .set, and .srt

The Custom Signatures page lists the converted custom attack signatures. The unconverted rules and error log files are downloaded automatically.

RELATED DOCUMENTATION

[About the IPS Signatures Page | 967](#)

[Create a Custom IPS Signature | 973](#)

[Create IPS Signature Static Groups | 989](#)

[Create IPS Signature Dynamic Group | 992](#)

[Clone an IPS Signature | 997](#)

[Edit an IPS Signature | 998](#)

[Delete an IPS Signature | 999](#)

Create a Custom IPS Signature

You are here: **Security Services > IPS > Signatures**.

Create custom attack objects to detect a known or unknown attack for protecting your network.

To create a custom IPS signature:

1. Click the **CUSTOM** tab.
2. Click **Create > Custom** on the upper-right corner of the Custom Signatures page.
The Create Custom Attack page appears.

3. Complete the configuration according to the guidelines provided from [Table 272 on page 974](#) to [Table 275 on page 982](#) .
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.
You are returned to the Custom Signatures page and displays the custom signatures that you successfully created.

Table 272: Fields on the IPS Signatures Page—Create Custom

| Field | Action |
|----------------|--|
| General | |
| Name | Enter the name of the custom attack object. 250-character maximum. |
| Description | Enter a description for the custom attack object. |

Table 272: Fields on the IPS Signatures Page—Create Custom (*Continued*)

| Field | Action |
|--------------------|--|
| Recommended action | <p>Select an action from the list to perform when the device detects an attack:</p> <ul style="list-style-type: none"> • None—No action is taken. Use this action to only generate logs for some traffic. • Close—Reset the client and the server. • Close client—Closes the connection and sends an RST packet to the client but not to the server. • Close server—Closes the connection and sends an RST packet to the server but not to the client. • Drop—Drops all packets associated with the connection, preventing traffic for the connection from reaching its destination. Use this action to drop connections for traffic that is not prone to spoofing. • Drop packet—Drops a matching packet before it can reach its destination but does not close the connection. Use this action to drop packets for attacks in traffic that is prone to spoofing, such as UDP traffic. Dropping a connection for such traffic could result in a denial of service that prevents you from receiving traffic from a legitimate source-IP address. • Ignore—Stops scanning traffic for the rest of the connection if an attack match is found. IPS disables the rulebase for the specific connection. |

Table 272: Fields on the IPS Signatures Page—Create Custom (*Continued*)

| Field | Action |
|------------------|--|
| Severity | <p>Select a severity from the list that matches the attack object severity on your network:</p> <ul style="list-style-type: none"> • Critical—Contains attack objects matching exploits that attempt to evade detection, cause a network device to crash, or gain system-level privileges. • Info—Contains attack objects that matches the following parameters: <ul style="list-style-type: none"> • Normal and harmless traffic containing URLs • DNS lookup failures • SNMP public community strings • Peer-to-Peer (P2P) • Major—Contains attack objects that matches the exploits that attempt to: <ul style="list-style-type: none"> • Disrupt a service. • Gain user-level access to a network device. • Activate a Trojan horse previously loaded on a device. • Minor—Contains attack objects that matches the exploits that detect reconnaissance efforts attempting to access vital informational through directory traversal or information leaks. • Warning—Contains attack objects that matches the exploits that attempt to obtain noncritical information or scan a network with a scanning tool. |
| Detection Filter | |

Table 272: Fields on the IPS Signatures Page—Create Custom (*Continued*)

| Field | Action |
|------------------|---|
| Time count | <p>Set the number of times that the attack object must detect an attack within the specified scope. The detection occurs before the device determines if or not the attack object matches the attack.</p> <p>Range: 0 through 4,294,967,295</p> |
| Time scope | <p>Select the scope from the list within which the count occurs:</p> <ul style="list-style-type: none"> • None—No action is taken. Use this option when you only want to generate logs for some traffic. • Destination—Detects the signature in traffic from the destination IP address for the specified number of times, regardless of the source IP address. • Session—Detects the signature in traffic between source and destination IP addresses of the sessions for the specified number of times. • Source—Detects the signature in traffic from the source IP address for the specified number of times, regardless of the destination IP address. |
| Time interval | <p>Enter the maximum time interval between any two instances of a time-binding custom attack.</p> <p>Supported format is MMm-SSs.</p> <p>Range: 0 minutes and 0 seconds to 60 minutes and 0 seconds.</p> |
| Signature | |

Table 272: Fields on the IPS Signatures Page—Create Custom (*Continued*)

| Field | Action |
|-------------|---|
| Attack type | <p>Select one of the following attack type from the list:</p> <ul style="list-style-type: none"> • Signature—IPS uses stateful signatures to detect attacks. Using stateful signatures, IPS look for the specific protocol or service that was used to carry out the attack. For fields description, see Table 273 on page 978 . • Anomaly—Protocol anomaly attack objects detect abnormal or ambiguous messages within a connection using the protocol's set of rules. For fields description, see Table 274 on page 982 . • Chain—Chain attack object combines multiple signatures and/or protocol anomalies into a single object. Traffic must match all of the combined signatures and/or protocol anomalies to match the chain attack object. For fields description, see Table 275 on page 982 . |

Table 273: Fields on the Attack Type—Signature

| Field | Action |
|------------------|---|
| Attack type | Signature—IPS uses stateful signatures to detect attacks. Using stateful signatures, IPS look for the specific protocol or service that was used to carry out the attack. |
| Context | Select an attack context from the list which defines the location of the signature where IPS should look for the attack in a specific Application Layer protocol. |
| Protocol binding | Select a protocol from the list that the attack uses to enter your network. |

Table 273: Fields on the Attack Type—Signature (Continued)

| Field | Action |
|-----------------|---|
| Application | <p>Select an application from the list under which the attack must match.</p> <p>NOTE: This option is available only when protocol binding type is Application.</p> |
| Protocol number | <p>Set the transport layer protocol number which allows IPS to match the attack to it.</p> <p>Range: 0 through 139</p> <p>NOTE: This option is available only when protocol binding type is IP and IPv6.</p> |
| Program number | <p>Set the remote procedure call (RPC) program number which allows to match the attack to it.</p> <p>NOTE: This option is available only when protocol binding type is RPC.</p> |
| Minimum port | <p>Set the minimum port in the port range.</p> <p>Range: 0 through 65,535</p> <p>NOTE: This option is available only when protocol binding type is TCP.</p> |
| Maximum port | <p>Set the maximum port in the port range.</p> <p>Range: 0 through 65,535</p> <p>NOTE: This option is available only when protocol binding type is TCP.</p> |

Table 273: Fields on the Attack Type—Signature (Continued)

| Field | Action |
|----------------|---|
| Direction | <p>Select the traffic direction from the list for which the attack is detected:</p> <ul style="list-style-type: none"> • Client to Server—Detects the attack only in client-to-server traffic. • Server to Client—Detects the attack only in server-to-client traffic. • Any Direction—Detects the attack in either direction. |
| Content | |
| DFA pattern | <p>Enter the signature pattern in deterministic finite automation (DFA) format.</p> <p>For example:</p> <p>When you use the syntax: <code>\[hello\]</code>, pattern is hello and it is case insensitive.</p> <p>Example matches for the syntax are hEILo, HEIIO, and heLLO.</p> |
| PCRE pattern | <p>Enter the signature pattern in standard Perl Compatible Regular Expression (PCRE) format.</p> <p>Example syntax: <code>Sea[ln]</code>, pattern is Seal and it is case insensitive.</p> <p>Example matches for the syntax are Seal, Seam, and Sean</p> |
| Depth | <p>Allows you to specify the depth in a packet to search for the given pattern. The depth is not relative. For example, you can specify a value for depth as 100.</p> |
| Variable | <p>Enter the depth variable name.</p> |

Table 273: Fields on the Attack Type—Signature (Continued)

| Field | Action |
|------------|---|
| Value | <p>Set the depth value to be used.</p> <p>Range: 1 through 65535</p> |
| Offset | <p>Allows you to specify where to start searching for a pattern within a packet. Offset is not relative. For example, you can specify a value for depth as 100.</p> |
| Variable | <p>Enter the offset variable name.</p> |
| Value | <p>Set the offset value to be used.</p> <p>Range: 1 through 65535</p> |
| Is data at | <p>Enable this option to allow you to verify that the payload has data at a specified location.</p> |
| Negate | <p>Enable this option to negate the result of Is data at.</p> |
| Relate | <p>Enable this option to use an offset relative to last pattern match.</p> |
| Offset | <p>Allows you to specify where to start searching for a pattern within a packet. Offset is not relative. For example, you can specify a value for depth as 100.</p> |
| Variable | <p>Enter the offset variable name.</p> |
| Value | <p>Set the offset value to be used.</p> <p>Range: 1 through 65535</p> |

Table 274: Fields on the Attack Type—Anomaly

| Field | Action |
|--------------|--|
| Attack type | Anomaly—Protocol anomaly attack objects detect abnormal or ambiguous messages within a connection using the protocol's set of rules. |
| Service | Select a service from the list. Service is a protocol whose anomaly is defined in the attack. Example: IP, TCP, and ICMP. |
| Test anomaly | Select a protocol anomaly test condition from the list to be checked. |
| Direction | Select a traffic direction from the list for which the attack is detected: <ul style="list-style-type: none"> • Any Direction—Detects the attack in either direction. • Client to Server—Detects the attack only in client-to-server traffic. • Server to Client—Detects the attack only in server-to-client traffic. |

Table 275: Fields on the Attack Type—Chain

| Field | Action |
|------------------|--|
| Attack type | Chain—Chain attack object combines multiple signatures and/or protocol anomalies into a single object. Traffic must match all of the combined signatures and/or protocol anomalies to match the chain attack object. |
| Protocol binding | Select a protocol from the list that the attack uses to enter your network. |

Table 275: Fields on the Attack Type—Chain (Continued)

| Field | Action |
|-----------------|---|
| Application | <p>Select an application under which the attack must match.</p> <p>NOTE: This option is available only when protocol binding type is Application.</p> |
| Protocol Number | <p>Set the transport layer protocol number which allows IPS to match the attack to it.</p> <p>Range: 0 through 139</p> <p>NOTE: This option is available only when protocol binding type is IP and IPv6.</p> |
| Program Number | <p>Set the remote procedure call (RPC) program number which allows to match the attack to it.</p> <p>NOTE: This option is available only when protocol binding type is RCP.</p> |
| Minimum Port | <p>Set the minimum port in the port range.</p> <p>Range: 0 through 65,535</p> <p>NOTE: This option is available only when protocol binding type is TCP.</p> |
| Maximum Port | <p>Set the maximum port in the port range.</p> <p>Range: 0 through 65,535</p> <p>NOTE: This option is available only when protocol binding type is TCP.</p> |

Table 275: Fields on the Attack Type—Chain (Continued)

| Field | Action |
|-------------------------|---|
| Chain order expressions | <p>Select a Boolean expression that defines the condition for the individual members of a chain attack that will decide if the chain attack is hit:</p> <ul style="list-style-type: none"> • AND—If both of the member name patterns match, the expression matches. The order of the members does not matter. • OR—If either of the member name patterns match, the expression matches. • OAND—If both of the member name patterns match, and if they appear in the same order as in the Boolean Expression, the expression matches. |
| Customized ordering | <p>Enable this option to create a compound attack object that must match each member signature or protocol anomaly in the order you specify. If you do not specify an ordered match, the compound attack object still must match all members, but the attacks or protocol anomalies can appear in random order.</p> |
| Reset | <p>Enable this option if the compound attack should be matched more than once within a single session or transaction.</p> |
| Scope | <p>Select one of the following scopes:</p> <ul style="list-style-type: none"> • session—Allows multiple matches for the object within the same session. • transaction—Matches the object across multiple transactions that occur within the same session. |
| Add signatures | |
| Edit (pencil icon) | <p>Select an existing signature that you want to edit. Click the edit (pencil) icon, make the required changes, and click OK.</p> |

Table 275: Fields on the Attack Type—Chain (Continued)

| Field | Action |
|-------------------------|---|
| Delete (trash can icon) | Select an existing signature that you want to delete. Click the delete (trash can) icon and click Yes . |
| + | Click + to add one or more signature attack objects that use a stateful attack signature (a pattern that always exists within a specific section of the attack) to detect known attacks. |
| Signature No | Displays the system-generated signature number. You cannot modify this field. |
| Context | Select the attack context from the list which defines the location of the signature where IPS should look for the attack in a specific Application Layer protocol. |
| Direction | <p>Select a traffic direction from the list for which the attack is detected:</p> <ul style="list-style-type: none"> • Any Direction—Detects the attack in either direction. • Client to Server—Detects the attack only in client-to-server traffic. • Server to Client—Detects the attack only in server-to-client traffic. |
| Content | |
| DFA pattern | <p>Enter the signature pattern in deterministic finite automation (DFA) format.</p> <p>Example syntax: <code>\[he]llo\]</code>, pattern is hello and it is case insensitive.</p> <p>Example matches for the syntax are hEILo, HEIIo, and heLLO.</p> |

Table 275: Fields on the Attack Type—Chain (Continued)

| Field | Action |
|--------------|---|
| PCRE pattern | <p>Enter the signature pattern in standard Perl Compatible Regular Expression (PCRE) format.</p> <p>Example syntax: Sea[ln], pattern is Seal and it is Unicode insensitive.</p> <p>Example matches to the syntax Seal, Seam, and Sean</p> |
| Depth | <p>Allows you to specify the depth in a packet to search for the given pattern. The depth is not relative. For example, you can specify a value for depth as 100.</p> |
| Variable | <p>Enter the depth variable name.</p> |
| Value | <p>Set the depth value to be used.</p> <p>Range: 1 through 65535</p> |
| Distance | <p>Allows you to specify how much of the packet data should the IPS engine ignore before it begins searching for the specified pattern relative to the end of the previous pattern match.</p> |
| Variable | <p>Enter the distance variable name.</p> |
| Value | <p>Set the match value to be used. This is always relative to previous match.</p> |
| Offset | <p>Allows you to specify where to start searching for a pattern within a packet. Offset is not relative. For example, you can specify a value for depth as 100.</p> |
| Variable | <p>Enter the offset variable name.</p> |
| Value | <p>Set the offset value to be used.</p> <p>Range: 1 through 65535</p> |

Table 275: Fields on the Attack Type—Chain (Continued)

| Field | Action |
|-------------------------|--|
| Is data at | Enable this option to allow you to verify that the payload has data at a specified location. |
| Negate | Enable this option to negate the result of Is data at. |
| Relate | Enable this option to use an offset relative to last pattern match. |
| Offset | Allows you to specify where to start searching for a pattern within a packet. Offset is not relative. For example, you can specify a value for depth as 100. |
| Variable | Enter the offset variable name. |
| Value | Set the offset value to be used. Range: 1 through 65535 |
| Within | Allows you to specify that there are maximum N bytes between pattern matches. |
| Variable | Enter the match variable name. |
| Value | Set the match value to be used. This is always relative to previous match. |
| Add anomaly | |
| Edit (pencil icon) | Select an existing anomaly that you want to edit. Click the edit (pencil) icon, make the required changes, and click OK . |
| Delete (trash can icon) | Select an existing anomaly that you want to delete. Click the delete (trash can) icon and click Yes . |

Table 275: Fields on the Attack Type—Chain (Continued)

| Field | Action |
|--------------|---|
| + | Click + to add one or more protocol anomaly attack objects to detect abnormal or ambiguous messages within a connection according to the set of rules for the particular protocol being used. |
| Anomaly No | Displays the system-generated anomaly number. You cannot modify this field. |
| Test Anomaly | Select a protocol anomaly test condition to be checked. |
| Direction | <p>Select a traffic direction from the list for which the attack is detected:</p> <ul style="list-style-type: none"> • Any Direction—Detects the attack in either direction. • Client to Server—Detects the attack only in client-to-server traffic. • Server to Client—Detects the attack only in server-to-client traffic. |

RELATED DOCUMENTATION

[About the IPS Signatures Page | 967](#)

[Import Snort Rules | 972](#)

[Create IPS Signature Static Groups | 989](#)

[Create IPS Signature Dynamic Group | 992](#)

[Clone an IPS Signature | 997](#)

[Edit an IPS Signature | 998](#)

[Delete an IPS Signature | 999](#)

Create IPS Signature Static Groups

You are here: **Security Services > IPS > Signatures.**

Create static groups for better manageability because you can group different types of signatures into one entity.

To create an IPS signatures static group:

1. Click the **CUSTOM** tab.
2. Click **Create > Static Group** on the upper-right corner of the Custom Signatures page.
The Create Static Group page appears.
3. Complete the configuration according to the guidelines provided in [Table 276 on page 989](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

You are returned to the Custom Signatures page and displays the static group that you successfully created.

Table 276: Fields on the Create Static Group Page

| Field | Action |
|----------------------------------|--|
| Name | Name must be a string beginning with a letter or underscore and consisting of letters, numbers, dashes and underscores; 250-character maximum. |
| Group Members | |
| Add | Click Add and select either Predefined Signatures or Custom Signatures to add to the static group. |
| Add Predefined Signatures | |
| View by | Select Predefined Attack Groups or Predefined Attacks from the list. |
| Predefined Attack Groups | Select one or more predefined attack groups and click OK to add predefined attack groups to the static group. |

Table 276: Fields on the Create Static Group Page (Continued)

| Field | Action |
|--------------------------|--|
| Predefined Attacks | Select one or more predefined attacks and click OK to add predefined attacks to the static group. |
| Detailed View | To view the details of an IPS signature, select a predefined attack or attack group and then click More > Detailed View . |
| Three vertical dots | Click the Show Hide Columns icon, then select options to view or clear the options to hide on the page. |
| Advanced Search | <ol style="list-style-type: none"> 1. Enter the search string in the search text box present above the table grid. 2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation. NOTE: Press spacebar to add an AND operator to the search string. Press backspace at any time when typing a search criteria to delete only one character. 3. Press Enter to display the search results in the grid. |
| Custom Signatures | |
| View by | <p>Select one of the following custom signatures to add to the static group:</p> <ul style="list-style-type: none"> • Custom Attacks • Static Groups • Dynamic Groups |
| Custom Attacks | Select one or more custom attacks and click OK to add custom attacks to the static group. |

Table 276: Fields on the Create Static Group Page (Continued)

| Field | Action |
|---------------------|--|
| Static Groups | Select one or more static groups and click OK to add static groups to the static group. |
| Dynamic Groups | Select one or more dynamic groups and click OK to add dynamic groups to the static group. |
| Detailed View | To view the details of an IPS signature, select a custom attack, static group, or dynamic group and then click More > Detailed View . |
| Three vertical dots | Click the Show Hide Columns icon, then select options to view or clear the options to hide on the page. |
| Advanced Search | <ol style="list-style-type: none"> 1. Enter the search string in the search text box present above the table grid. 2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation. NOTE: Press spacebar to add an AND operator to the search string. Press backspace at any time when typing a search criteria to delete only one character. 3. Press Enter to display the search results in the grid. |

RELATED DOCUMENTATION

[About the IPS Signatures Page | 967](#)

[Import Snort Rules | 972](#)

[Create a Custom IPS Signature | 973](#)

[Create IPS Signature Dynamic Group | 992](#)

[Clone an IPS Signature | 997](#)

[Edit an IPS Signature | 998](#)

[Delete an IPS Signature | 999](#)

Create IPS Signature Dynamic Group

You are here: **Security Services > IPS > Signatures.**

Create a dynamic attack group to select its members based on the specified filters in the group. The list of attacks is updated (added or removed) automatically when a new signature database is used.

To create an IPS signatures dynamic group:

1. Click the **CUSTOM** tab.
2. Click **Create > Dynamic Group** on the upper-right corner of the Custom Signatures page.
The Create Dynamic Group page appears.
3. Complete the configuration according to the guidelines provided in [Table 277 on page 992](#) .
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

You are returned to the Custom Signatures page and the dynamic group you successfully created is displayed.

Table 277: Fields on the Create Dynamic Group Page

| Field | Action |
|------------------------|--|
| Name | Name must be a string beginning with a letter or underscore and consisting of letters, numbers, dashes and underscores; 250-character maximum. |
| Filter Criteria | |
| Attack prefix | Select one or more values from the list for the attack name prefix match. |

Table 277: Fields on the Create Dynamic Group Page (*Continued*)

| Field | Action |
|-------------|---|
| Severity | <p>Select one or more severity values from the list to add attack objects based on the attack severity levels (critical, info, major, minor, or warning).</p> <ul style="list-style-type: none"> • Critical—The attack is a critical one. • Info—Provides information of attack when it matches. • Major—The attack is a major one. • Minor—The attack is a minor one. • Warning—Issues a warning when attack matches. |
| Service | <p>Select one or more service values from the list to add attack objects based on the attack service. For example, BGP, FTP, and HTTP.</p> |
| Category | <p>Select one or more category values from the list to add attack objects based on the category.</p> |
| Recommended | <p>Select one of the following filter:</p> <ul style="list-style-type: none"> • None—No action is performed. • Yes—The recommended filter to add predefined attacks recommended by Juniper Networks to the dynamic attack group. • No—The non-recommended attack objects in the dynamic attack group. |

Table 277: Fields on the Create Dynamic Group Page (*Continued*)

| Field | Action |
|------------|---|
| Direction | <p>Select one or more direction values from the list:</p> <ul style="list-style-type: none"> • Any—Monitors traffic from client to server and server to client. • Client to Server—Monitors traffic only from client to server (most attacks occur over client to server connections). • Exclude Any—Allows traffic from client to server and server to client. • Exclude Client to Server—Allows traffic only from server to client. • Exclude Server to Client—Allows traffic only from client to server. • Server to Client—Monitors traffic only from server to client. |
| Expression | <p>Select one of the following expressions from the list:</p> <ul style="list-style-type: none"> • None—No action is performed. • AND—If both the directions match, the expression matches. • OR—If either of the directions match, the expression matches. |

Table 277: Fields on the Create Dynamic Group Page (Continued)

| Field | Action |
|-----------------|--|
| Performance | <p>Select one or more performance values from the list:</p> <ul style="list-style-type: none"> • Fast—Fast track performance level. • Normal—Normal track performance level. • Slow—Slow track performance level. • Unknown—By default, all compound attack objects are set to Unknown. As you fine-tune IPS to your network traffic, you can change this setting to help you track performance level. |
| False positives | <p>Select one or more false positives value from the list:</p> <ul style="list-style-type: none"> • Frequently—Frequently track false positive occurrences. • Occasionally—Occasionally track false positive occurrences. • Rarely—Rarely track false positive occurrences. • Unknown—By default, all compound attack objects are set to Unknown. As you fine-tune IPS to your network traffic, you can change this setting to help you track false positives. |
| Attack type | <p>Select Anomaly or Signature attack type from the list. If you choose None, no action will be taken.</p> |
| Attacks | <p>Select Excluded or Not Excluded from the list to check the signatures that are part of the database updates. If you choose None, no action will be taken.</p> |

Table 277: Fields on the Create Dynamic Group Page (Continued)

| Field | Action |
|--------------------|--|
| CVSS score | <p>Select Greater than or Less than from the list to specify the Common Vulnerability Scoring System (CVSS) score of the attack.</p> <p>CVSS score of the attack is a free and open industry standard for assessing the severity of computer system security vulnerabilities. CVSS attempts to assign severity scores to vulnerabilities allowing responders to prioritize responses and resources according to threats.</p> |
| Greater than | <p>Set to match the CVSS score greater than the value specified.</p> <p>Range: 0 through 10</p> |
| Less than | <p>Set to match the CVSS score lesser than the value specified.</p> <p>Range: 0 through 10</p> |
| Age of attack | <p>Select Greater than or Less than from the list to specify the age of the attack.</p> |
| Value | <p>Set to match when age of attack in terms of years is greater than or less than the specified value (years).</p> <p>Range: 1 through 100.</p> |
| File type | <p>Select the file type from the list that the attack targets. For example, HTML and PDF.</p> |
| Vulnerability type | <p>Select the vulnerability type for IPS from the list that indicates which applications are weak and can be manipulated. The vulnerability type is reported for fixing these vulnerabilities.</p> |

Table 277: Fields on the Create Dynamic Group Page (Continued)

| Field | Action |
|--------|--|
| Vendor | <p>Group attacks specific to the product of a vendor.</p> <p>You can add, modify, or delete a vendor.</p> <p>To add a vendor to the dynamic group:</p> <ol style="list-style-type: none"> 1. Click +. 2. Select the vendor name and product name from the list. 3. Click the tick icon to save the vendor details. <p>To edit a vendor, select it and click the pencil icon.</p> <p>To delete a vendor, select it and click the delete icon.</p> |

RELATED DOCUMENTATION

[About the IPS Signatures Page | 967](#)

[Import Snort Rules | 972](#)

[Create a Custom IPS Signature | 973](#)

[Create IPS Signature Static Groups | 989](#)

[Clone an IPS Signature | 997](#)

[Edit an IPS Signature | 998](#)

[Delete an IPS Signature | 999](#)

Clone an IPS Signature

You are here: **Security Services > IPS > Signatures.**

You can clone both the predefined and the custom IPS signatures.

To clone a predefined IPS signature:

1. Click the **PREDEFINED** tab.
2. Select an existing predefined IPS signature you want to clone.

3. Click **More** > **Clone** on the upper-right corner of the Predefined Signatures page.

The Clone Predefined Group Details page appears.

4. Edit the required fields and click **OK**.

The cloned signature is displayed on the Predefined Signatures page.

NOTE: By default, the name of the cloned signature is in the *<Signature name>_clone* format.

To clone a custom IPS signature:

1. Click the **CUSTOM** tab.
2. Select an existing custom IPS signature, static group, or dynamic group that you want to clone.
3. Click **More** > **Clone** on the upper-right corner of the Custom Signatures page.

The Clone *<Custom Attack or Static Group or Dynamic Group>* page appears.

4. Edit the required fields and click **OK**.

The cloned signature is displayed on the Custom Signatures page.

NOTE: By default, the name of the cloned signature is in the *<Signature name>_clone* format.

RELATED DOCUMENTATION

[About the IPS Signatures Page | 967](#)

[Import Snort Rules | 972](#)

[Create a Custom IPS Signature | 973](#)

[Create IPS Signature Static Groups | 989](#)

[Create IPS Signature Dynamic Group | 992](#)

[Edit an IPS Signature | 998](#)

[Delete an IPS Signature | 999](#)

Edit an IPS Signature

You are here: **Security Services** > **IPS** > **Signatures**.

You can edit a custom IPS signature, static group, or dynamic group.

To edit a custom IPS signature, static group, or dynamic group:

1. Click the **CUSTOM** tab.
2. Select an existing custom IPS signature, static group, or dynamic group that you want to edit.
3. Click the pencil icon on the upper-right corner of the Custom Signatures page.

The Edit *<Custom Attack or Static Group or Dynamic Group>* page appears.

NOTE: When editing a dynamic group, click **Preview Filtered Signatures** at the bottom of the page to view the list of filtered signatures.

4. Make the required changes and click **OK**.

The edited signature is displayed on the Custom Signatures page.

NOTE: You cannot edit the name of the custom IPS signature, static group, or dynamic group.

RELATED DOCUMENTATION

[About the IPS Signatures Page | 967](#)

[Import Snort Rules | 972](#)

[Create a Custom IPS Signature | 973](#)

[Create IPS Signature Static Groups | 989](#)

[Create IPS Signature Dynamic Group | 992](#)

[Clone an IPS Signature | 997](#)

[Delete an IPS Signature | 999](#)

Delete an IPS Signature

You are here: **Security Services > IPS > Signatures**.

You can delete one or more custom IPS signature, static group, or dynamic group.

To delete a custom IPS signature, static group, or dynamic group:

1. Click the **CUSTOM** tab.

2. Select one or more existing custom IPS signatures, static groups, or dynamic groups that you want to delete on the Custom Signatures page.

NOTE: Alternatively, you can right-click on the selected name and select **Delete**.

3. Click the delete icon on the upper-right corner of the Custom Signatures page.
4. Click **Yes** to delete or click **No** to retain the existing custom IPS signatures, static groups, or dynamic groups.

RELATED DOCUMENTATION

[About the IPS Signatures Page | 967](#)

[Import Snort Rules | 972](#)

[Create a Custom IPS Signature | 973](#)

[Create IPS Signature Static Groups | 989](#)

[Create IPS Signature Dynamic Group | 992](#)

[Clone an IPS Signature | 997](#)

[Edit an IPS Signature | 998](#)

IPS Sensor

IN THIS CHAPTER

- [About the Sensor Page | 1001](#)

About the Sensor Page

IN THIS SECTION

- [Field Descriptions | 1001](#)

You are here: **Security Services > IPS > Sensor.**

You can configure sensor settings to limit the number of sessions running application identification and also to limit memory usage for application identification.

Field Descriptions

[Table 278 on page 1001](#) describes the fields on the Sensor page.

Table 278: Fields on the Sensor Page

| Field | Description |
|-----------------------|---|
| Packet Capture | |
| Local Storage | Enable this option to store the PCAP file locally (<code>/var/log/pcap/idp/</code>) on the SRX Series Firewall. |

Table 278: Fields on the Sensor Page (Continued)

| Field | Description |
|-------------------------------|--|
| Maximum files | Enter or select the maximum number of unique packet capture files to create before the oldest file is overwritten by a newly created file. Range: 1 through 5000. |
| Storage limit | Enter or select the maximum disk space (Megabytes) that can be used in the Routing Engine for packet capture files. Range: 1 MB through 4096 MB. |
| External Server | Enable this option to send the PCAP file to an external server. |
| IP Address | Enter the external server IPv4 address that captures the packet. |
| Port | Enter or select the port number of the server for SRX Series Firewalls to send the packet capture object. Port number: 0 through 65535. Default port is 2050. |
| Source Address | Enter the source IPv4 address for the carrier TCP or UDP packet. |
| Intelligent IDP ByPass | |
| IDP By Pass | Enable or disable the IDP Intelligent Bypass option. |
| IDP By Pass CPU Threshold | Enter the threshold value. Range: 0 through 99. Default value: 85. |
| IDP By Pass CPU Tolerance | Enter the CPU tolerance value. Range: 1 through 99. Default value: 5. |

Table 278: Fields on the Sensor Page (Continued)

| Field | Description |
|------------------------|---|
| Intelligent Inspection | <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— Enable this option to enable payload 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. <p>Range: 0 through 99 percent.</p> <ul style="list-style-type: none"> • CPU Tolerance (%)—Enter the value of CPU usage tolerance percentage for intelligent inspection. <p>Range: 1 through 99 percent.</p> <ul style="list-style-type: none"> • Memory Tolerance—Enter the value of memory tolerance percentage for intelligent inspection. <p>Range: 1 through 100 percent.</p> <ul style="list-style-type: none"> • Free Memory Threshold—Enter the value of free memory threshold percentage for intelligent inspection. <p>Range: 1 through 100 percent.</p> <ul style="list-style-type: none"> • Session Bytes Depth—Enter the value of session bytes scanning depth. <p>Range: 1 through 1000000 bytes.</p> |
| Memory Lower Threshold | <p>Enter the memory lower threshold limit percentage.</p> <p>Range: 1 through 100.</p> |

Table 278: Fields on the Sensor Page (Continued)

| Field | Description |
|----------------------------|---|
| Memory Upper Threshold | Enter the memory upper threshold limit percentage. Range: 1 through 100. |
| Advanced Settings | |
| IDP Protection Mode | |
| Protection Mode | Select an option to specify 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. |
| Exception Handling | |
| Drop On Limit | Enable this option to specify the dropped connections on exceeding resource limits. |
| Drop On Failover | Enable this option to specify the dropped traffic on HA failover sessions. |
| Drop If No Policy Loaded | Enable this option to specify all the dropped traffic till IDP policy gets loaded. |
| IDP Flow | |
| Log Errors | Enable this option to specify if the flow errors have to be logged. Select an option from the list. |
| Flow FIFO Max Size | Enter a value to specify the maximum FIFO size. Range: : 1 through 65535. Default value is 1. |

Table 278: Fields on the Sensor Page (Continued)

| Field | Description |
|-----------------------|---|
| Hash Table Size | Enter a value to specify the hash table size. Range: 1024 through 1,000,000. Default value is 1024. |
| Max Timers Poll Ticks | Enter a value to specify the maximum amount of time at which the timer ticks at a regular interval. Range: 0 through 1000 ticks. Default value is 1000 ticks. |
| Reject Timeout | Enter a value to specify the amount of time in milliseconds within which a response must be received. Range: 1 through 65,535 seconds. Default value is 300 seconds. |
| Global | |
| Enable All Qmodules | Select an option from the list to specify all the qmodules of the global rulebase IDP security policy are enabled. |
| Enable Packet Pool | Select an option from the list to specify the packet pool is enabled to be used when the current pool is exhausted. |
| Policy Lookup Cache | Select an option from the list to specify the cache is enabled to accelerate IDP policy lookup. |
| Memory Limit Percent | Enter a value to specify the limit IDP memory usage at this percent of available memory. Range: 10 through 90 percent. |
| HTTP X-Forwarded | When you enable this option, during traffic flow, IDP saves the source IP addresses (IPv4 or IPv6) from the contexts of HTTP traffic, and displays it in the attack logs. |
| IPS | |
| Detect Shellcode | Select an option from the list to specify if shellcode detection has to be applied. |

Table 278: Fields on the Sensor Page (Continued)

| Field | Description |
|---------------------------------|---|
| Ignore Regular Expression | Select an option from the list to specify if the sensor has to bypass DFA and PCRE matching. |
| Process Ignore Server-to-Client | Select an option from the list to specify if the sensor has to bypass IPS processing for server-to-client flows. |
| Process Override | Select an option from the list to specify if the sensor has to execute protocol decoders even without an IDP policy. |
| Process Port | Enter an integer to specify a port on which the sensor executes protocol decoders. Range: 0 through 65535. |
| IPS FIFO Max Size | Enter an integer to specify the maximum allocated size of the IPS FIFO. Range: 1 through 65535. |
| Minimum Log Supercade | Enter an integer to specify the minimum number of logs to trigger the signature hierarchy feature. Range: 0 through 65535. |
| Log | |
| Cache Size | Enter a value to specify the size in bytes for each user's log cache. |
| Disable Suppression | Enable this option to specify if the log suppression has to be disabled. |
| Include Destination Address | Select an option from the list to specify if combine log records for events with a matching source address. |
| Max Logs Operate | Enter a value to specify the maximum number of logs on which log suppression can operate. Range is 255 through 65536. |

Table 278: Fields on the Sensor Page (Continued)

| Field | Description |
|-----------------------------------|--|
| Max Time Report | Enter a value to specify the time (seconds) after which suppressed logs will be reported. IDP reports suppressed logs after 5 seconds by default. |
| Start Log | Enter a value to specify the number of log occurrences after which log suppression begins. Log suppression begins with the first occurrence by default. Range is 1 through 128. |
| Reassembler | |
| Ignore Memory Overflow | Select an option from the list to specify if the user has to allow per-flow memory to go out of limit. |
| Ignore Reassembly Memory Overflow | Select an option from the list to specify if the user has to allow per-flow reassembly memory to go out of limit. |
| Ignore Reassembly Overflow | Enable this option to specify the TCP reassembler to ignore the global reassembly overflow to prevent the dropping of application traffic. |
| Max Flow Memory | Enter an integer to specify the maximum per-flow memory for TCP reassembly in kilobytes. Range: 64 through 4,294,967,295 kilobytes. |
| Max Packet Memory | Enter an integer to specify the maximum packet memory for TCP reassembly in kilobytes. Range: 64 through 4,294,967,295 kilobytes |
| Max Synacks Queued | Enter an integer to specify the maximum limit for queuing Syn/Ack packets with different SEQ numbers. Range: 0 through 5 |
| Packet Log | |

Table 278: Fields on the Sensor Page (Continued)

| Field | Description |
|--------------|--|
| Max Sessions | Enter an integer to specify the maximum number of sessions actively conducting pre-attack packet captures on a device at one time. Range: 1 through 100 percent |
| Total Memory | Enter an integer to specify the maximum amount of memory to be allocated to packet capture for the device. Range: 1 through 100 percent |

Detectors—Click +.

The Detector window opens up and enter the following field details.

| | |
|---------------|---|
| Protocol | Select the name of the protocol from the list to enable or disable the detector. |
| Tunable Name | Select the name of the specific tunable parameter from the list to enable or disable the protocol detector for each of the services. |
| Tunable Value | Enter the protocol value of the specific tunable parameter to enable or disable the protocol detector for each of the services. Range: 0 to 4294967295 |

RELATED DOCUMENTATION

| [About the IPS Policies Page](#) | 950

ALG

IN THIS CHAPTER

- [About the ALG Page | 1009](#)

About the ALG Page

IN THIS SECTION

- [Field Descriptions | 1009](#)

You are here: **Security Services > ALG.**

Use this page to configure Application Layer Gateway (ALG).

Field Descriptions

[Table 279 on page 1009](#) describes the fields on the ALG page.

Once the configuration is complete, click **OK** to save the changes or click **Reset** to revert back the changes.

Table 279: Fields on the ALG Page

| Field | Description |
|-------------|-------------|
| Main | |

Table 279: Fields on the ALG Page (Continued)

| Field | Description |
|-------------|---|
| Enable PPTP | <p>Select the check box to enable the Point-to-Point Tunneling Protocol (PPTP) for ALG.</p> <p>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.</p> |
| Enable RSH | <p>Select the check box to enable RSH for ALG.</p> <p>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.</p> |
| Enable RTSP | <p>Select the check box to enable the Real-Time Streaming Protocol (RTSP) for ALG.</p> |
| Enable SQL | <p>Select the check box to enable Structured Query Language (SQL) for ALG.</p> <p>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.</p> |
| Enable TALK | <p>Select the check box to enable the TALK protocol for ALG.</p> <p>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.</p> |
| Enable TFTP | <p>Select the check box to enable the Trivial File Transfer Protocol (TFTP) for ALG.</p> <p>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.</p> |
| DNS | |
| Enable DNS | <p>Select the check box to enable the domain name system (DNS) for ALG.</p> <p>The DNS ALG monitors DNS query and reply packets and closes the session if the DNS flag indicates the packet is a reply message.</p> |

Table 279: Fields on the ALG Page (Continued)

| Field | Description |
|----------------------------------|---|
| Doctoring | Select one of the following options: <ul style="list-style-type: none"> Sanity Check—Performs only DNS ALG sanity checks. None—Disables all DNS ALG doctoring. |
| Maximum Message length | Select a number to specify the maximum DNS message length. Range: 512 through 8192 bytes. |
| Enable Oversize message drop. | Select the check box to enable oversize message drop. |
| FTP | |
| Enable FTP | Select the check box to enable the File Transfer Protocol (FTP) for ALG. 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. |
| Enable allow mismatch IP address | Select the check box to allow any mismatch in IP address. |
| Enable FTPs Extension | Select the check box to enable secure FTP and FTP SSL protocols. |
| Enable line Break Extension | Select the check box to enable line-break-extension. This option will enable the FTP ALG to recognize the LF as line break in addition to the standard CR+LF (carriage return, followed by line feed). |
| H323 | |

Table 279: Fields on the ALG Page (Continued)

| Field | Description |
|--------------------|---|
| Enable H323 | Select the check box to enable the H.323 ALG. |
| Application Screen | <p>Specify the security screens for the H.323 protocol ALG.</p> <p>Enter the following details:</p> <ul style="list-style-type: none"> • Message Flood Gatekeeper Threshold—Enter a value. The value range is 1 to 50000 messages per second. <p>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.</p> <ul style="list-style-type: none"> • Action on receiving unknown message: <ul style="list-style-type: none"> • Enable Permit NAT Applied—Select the check box to specify how unidentified H.323 (unsupported) messages are handled by the device. <p>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> • Enable Permit Routed—Select the check box to specify that unknown messages be allowed to pass if the session is in route mode. <p>Sessions in transparent mode are treated as though they are in route mode.</p> |
| DSCP Code Rewrite | <p>Code Point—Select a 6-bit string from the list.</p> <p>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.</p> <p>The VoIP rewrite rules modifies the appropriate class of service (CoS) bits in an outgoing packet through Differentiated Services Code Point (DSCP) mechanism that improves the VoIP quality in a congested network.</p> |

Table 279: Fields on the ALG Page (Continued)

| Field | Description |
|---------------------------|---|
| Endpoints | <p>Enter the following details:</p> <ul style="list-style-type: none"> • Timeout For Endpoint—Enter a timeout value in seconds for entries in the NAT table. Range: 10 through 50,000 seconds Controls the duration of the entries in the NAT table. • Enable Permit Media From Any Source Port—Select this option to allow media traffic from any port number. |
| IKE-ESP | |
| Enable IKE-ESP | Select the check box to enable IKE-ESP. |
| ESP Gate Timeout (sec) | Select the gate timeout from 2 to 30 seconds. |
| ESP Session Timeout (sec) | Select the ESP timeout session from 60 to 2400 seconds. |
| ALG State Timeout (Sec) | Select the ALG state time out from 180 to 86400 sec. |
| MGCP | |
| Enable MGCP | Select the check box to enable the Media Gateway Control Protocol (MGCP). |
| Inactive Media Timeout | <p>Select a value to specify the maximum amount of time that the temporary openings in the firewall (pinholes) remain open for media if no activity is detected. range is from 10 through 2,550 seconds.</p> <p>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.</p> |

Table 279: Fields on the ALG Page (Continued)

| Field | Description |
|-----------------------|---|
| Maximum Call Duration | <p>Select a value from 3 through 720 minutes.</p> <p>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.</p> |
| Transaction Timeout | <p>Enter a value from 3 through 50 seconds to specify</p> <p>Specifies a timeout value for MGCP transactions. A transaction is a signaling message, for example, a NOTIFY 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.</p> |
| Application Screen | <p>Enter the following details:</p> <ul style="list-style-type: none"> • Message Flood Threshold—Enter a value from 2 through 50,000 seconds per media gateway. <p>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.</p> • Connection Flood Threshold—Enter a value from 2 through 10,000. <p>Limits the number of new connection requests allowed per Media Gateway (MG) per second. Messages exceeding the ALG.</p> • Action On Receiving Unknown Message—Enter any of the following: <ul style="list-style-type: none"> • Enable Permit NAT Applied—Select the check box to specify how unidentified MGCP messages are handled by the Juniper Networks device. <p>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> • Enable Permit Routed—Select the check box. <p>Specifies that unknown messages be allowed to pass if the session is in route mode. (Sessions in transparent mode are treated as route mode.)</p> |

Table 279: Fields on the ALG Page (Continued)

| Field | Description |
|-------------------------|---|
| DSCP Code Rewrite | Specifies a code-point alias or bit set to apply to a forwarding class for a rewrite rule. Code Point—Enter a six-bit DSCP code point value. |
| MSRPC | |
| Enable MSRPC | Select the check box to enable the 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. |
| Maximum Group Usage (%) | Select the group usage % from 10 to 100%. |
| Map Entry Timeout (min) | Select the map entry timeout session from 5 to 4320 minutes. |
| SCCP | |
| Enable SCCP | Select the check box to enable the Skinny Client Control Protocol. |
| Inactive Media Timeout | Select a value from 10 through 600 seconds. 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. |
| Application Screen | Call Flood Threshold—Select a value from 2 through 1,000. Protects SCCP ALG clients from flood attacks by limiting the number of calls they attempt to process. |

Table 279: Fields on the ALG Page (Continued)

| Field | Description |
|--------------------------------------|---|
| Action On Receiving Unknown Messages | <ul style="list-style-type: none"> • Enable Permit NAT Applied—Select the check box. <p>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.</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> <ul style="list-style-type: none"> • Enable Permit Routed—Select the check box. <p>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.)</p> |
| DSCP Code Rewrite | Code Point—Enter a six-bit DSCP code point value. |
| SIP | |
| Enable SIP | Select the check box to enable Session Initiation Protocol (SIP). |
| Enable Retain Hold Resource | <p>Select the check box to enable whether the device frees media resources for a SIP, even when a media stream is placed on hold.</p> <p>By default, media stream resources are released when the media stream is held.</p> |
| Maximum Call Duration | <p>Select a value from 3 through 720 minutes.</p> <p>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.</p> |

Table 279: Fields on the ALG Page (Continued)

| Field | Description |
|------------------------|--|
| C Timeout | <p>Select a value from 3 through 10 minutes.</p> <p>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.</p> |
| T4 Interval | <p>Select a value from 5 through 10 seconds.</p> <p>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.</p> |
| Inactive Media Timeout | <p>Select a value from 10 through 2,550 seconds.</p> <p>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.</p> |
| T1 Interval | <p>Select a value from 500 through 5000 milliseconds.</p> <p>Specifies the round-trip 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.</p> |

Table 279: Fields on the ALG Page (Continued)

| Field | Description |
|--------------------|---|
| Application Screen | <p>Action On Receiving Unknown Message:</p> <ul style="list-style-type: none"> • Enable Permit NAT Applied—Select the check box to enable handling unidentified SIP messages by the device. <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> <ul style="list-style-type: none"> • Enable Permit Routed—Select the check box to enable to allow unknown messages to pass if the session is in route mode. (Sessions in transparent mode are treated as route mode.) |
| Protect Options | <ul style="list-style-type: none"> • SIP Invite Attack Table Entry Timeout—Enter a value from 1 through 3,600 seconds. <p>Specifies the time (in seconds) to make an attack table entry for each INVITE, which is listed in the application screen.</p> <ul style="list-style-type: none"> • Enable Attack Protection—Select one of the options: All Servers, Selected Servers, or None. <p>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> <p>When you select Selected Servers, enter the destination IP address and click +. You can select the destination IP address and click X to delete it.</p> |
| DSCP Code Rewrite | Code Point—Enter a six-bit DSCP code point value. |
| SUNRPC | |
| Enable SUNRPC | <p>Select the check box to enable SUNRPC.</p> <p>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.</p> |

Table 279: Fields on the ALG Page (Continued)

| Field | Description |
|-------------------------|--|
| Maximum Group Usage (%) | Select the maximum group usage % from 10 to 100%. |
| Map Entry Timeout | Select the map entry timeout session from 5 to 4320 minutes. |

Metadata Streaming Profile

IN THIS CHAPTER

- [About the Metadata Streaming Profile Page | 1020](#)
- [Configure DNS Filter | 1022](#)
- [Create a Metadata Streaming Profile | 1023](#)
- [Edit a Metadata Streaming Profile | 1026](#)
- [Delete a Metadata Streaming Profile | 1026](#)

About the Metadata Streaming Profile Page

IN THIS SECTION

- [Tasks You Can Perform | 1020](#)
- [Field Descriptions | 1021](#)

You are here: **Security Services** > **Metadata Streaming Profile**.

You can create a metadata streaming profile and assign it to a metadata streaming policy to protect and defend your network from advanced threats using DNS.

Tasks You Can Perform

- Associate the created metadata streaming profiles with metadata streaming policies. To do this:
 1. Click **Metadata Streaming Policy** link under the Metadata Streaming Profile page title to directly navigate to the Metadata Streaming Policy page.
 2. Click **+** to add a new metadata streaming policy configuration or click the pencil icon to edit an existing policy configuration.

3. Select the metadata streaming profile under Metadata Streaming Profile to a specific policy configuration. For more information on assigning the metadata streaming profile to a metadata streaming policy, see ["Create a Metadata Streaming Policy" on page 777](#) .
- Configure DNS filter. See ["Configure DNS Filter" on page 1022](#) .
 - Create a metadata streaming profile. See ["Create a Metadata Streaming Profile" on page 1023](#) .
 - Edit a metadata streaming profile. See ["Edit a Metadata Streaming Profile" on page 1026](#) .
 - Delete a metadata streaming profile. See ["Delete a Metadata Streaming Profile" on page 1026](#) .
 - Show or hide columns in the Metadata Streaming Profile table. To do this, use the Show Hide Columns icon in the upper-right corner of the page and select the options to show or deselect to hide options on the page.
 - Advanced search for metadata streaming profiles. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

For an advanced search:

1. Enter the search string in the text box.

Based on your input, a list of items from the filter context menu appears.

2. Select a value from the list and then select a valid operator to perform the advanced search operation.

NOTE: Press Spacebar to add an AND operator or an OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.

3. Press Enter to display the search results in the grid.

Field Descriptions

[Table 280 on page 1022](#) describes the fields on the Metadata Streaming Profile page.

Table 280: Fields on the Metadata Streaming Profile Page

| Field | Description |
|----------------------------|---|
| Name | Displays the metadata streaming profile name. |
| DGA Detection | Displays the action and logs that the SRX Series Firewall will take when a DGA-based attack is detected on DNS packets. |
| Tunnel Detection | Displays the action and logs that the SRX Series Firewall will take when a DNS tunneling is detected. |
| Encrypted Traffic Insights | <p>Displays the action and logs that the SRX Series Firewall will take when a malicious threats are detected.</p> <p>The detection is made when malicious threats are hidden in an encrypted traffic without intercepting and decrypting the traffic.</p> |

RELATED DOCUMENTATION

[Create a Metadata Streaming Profile | 1023](#)

Configure DNS Filter

You are here: **Security Services > Metadata Streaming Profile.**

Configure the settings for filtering DNS requests for allowed and disallowed domains.

To configure DNS filter:

1. Click **DNS Filter** on the upper-right corner of the Metadata Streaming Profile page.
The DNS Filter page opens.
2. Complete the configuration according to the guidelines provided in [Table 281 on page 1023](#).
3. Click **OK** to save the changes. To discard your changes, click **Cancel**.

Table 281: Fields on the DNS Filter Page

| Field | Action |
|-----------|---|
| Allowlist | <p>Allowlist logs the DNS request and allows the access.</p> <p>To configure the allowlist:</p> <ol style="list-style-type: none"> a. Click +. b. Enter a domain to allow the access. c. Click the tick icon on the upper right of the row once done with the configuration. |
| Blocklist | <p>Blocklist blocks access to the site by sending the client a DNS response that includes an IP address or domain name of a sinkhole server instead of the disallowed domain.</p> <p>To configure the blocklist:</p> <ol style="list-style-type: none"> a. Click +. b. Enter a domain to block. c. Click the tick icon on the upper right of the row once done with the configuration. |

RELATED DOCUMENTATION

[About the Metadata Streaming Profile Page | 1020](#)

Create a Metadata Streaming Profile

You are here: **Security Services > Metadata Streaming Profile.**

Create a metadata streaming profile to protect and defend your network from advanced threats using DNS.

To create a metadata streaming profile:

1. Click **+** on the upper-right corner of the Metadata Streaming Profile page.
The Create Metadata Streaming Profile page opens.
2. Complete the configuration according to the guidelines provided in [Table 282 on page 1024](#) .
3. Click **OK** to save the changes. To discard your changes, click **Cancel**.

Once you create the metadata streaming profile, you can associate it with metadata streaming policies.

Table 282: Fields on the Create Metadata Streaming Profile Page

| Field | Action |
|-------------------------|--|
| Name | <p>Enter a name for the metadata streaming profile.</p> <p>The name must be a unique string and can include alphabets, numbers, or special characters, and 64 characters maximum. Special characters such as & () ? " # are not allowed.</p> |
| DGA detection | |
| DGA detection | Enable to detect DGA-based attacks on DNS packets. |
| Action | <p>Select an action that the SRX Series Firewall will take when a detection is made:</p> <ul style="list-style-type: none"> • Deny—Drops DGA session. • Sinkhole—Drops the DGA session and sinkholes the domain. • Permit—Permits DGA session. |
| Logs | <p>Select an action to log the event:</p> <ul style="list-style-type: none"> • Log detections—(Recommended) Generates log only for malicious DNS detections. <p>Log everything—Generates log for every request (malicious or not) that passes through the device.</p> |
| Tunnel detection | |

Table 282: Fields on the Create Metadata Streaming Profile Page *(Continued)*

| Field | Action |
|---|--|
| Tunnel detection | Enable to detect DNS tunneling. |
| Action | <p>Select an action that the SRX Series Firewall will take when a detection is made:</p> <ul style="list-style-type: none"> • Deny—Drops tunnel session. • Sinkhole—Drops the tunnel session and sinkholes the domain. • Permit—Permits tunnel session. |
| Logs | <p>Select an action to log the event:</p> <ul style="list-style-type: none"> • Log detections—(Recommended) Generates log only for malicious tunnel detections. <p>Log everything—Generates log for every request (malicious or not) that passes through the device.</p> |
| Encrypted Traffic Insights (ETI) | |
| Encrypted Traffic Insights (ETI) | Enable to detect malicious threats that are hidden in encrypted traffic without intercepting and decrypting the traffic. |
| Action | Permits security metadata streaming actions. |
| Logs | Enable to log all security metadata streaming actions. |

RELATED DOCUMENTATION

[About the Metadata Streaming Profile Page | 1020](#)

[Edit a Metadata Streaming Profile | 1026](#)

[Delete a Metadata Streaming Profile | 1026](#)

Edit a Metadata Streaming Profile

You are here: **Security Services** > **Metadata Streaming Profile**.

To edit a metadata streaming profile:

1. Select an existing metadata streaming profile to edit on the Metadata Streaming Profile page.
2. Click the pencil icon available on the upper-right corner of the page.
The Edit Metadata Streaming Profile page opens with editable fields. For more information on the options, see "[Create a Metadata Streaming Profile](#)" on page 1023 .
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[About the Metadata Streaming Profile Page | 1020](#)

[Delete a Metadata Streaming Profile | 1026](#)

Delete a Metadata Streaming Profile

You are here: **Security Services** > **Metadata Streaming Profile**.

To delete metadata streaming profile(s):

1. Select one or more metadata streaming profiles to delete on the Metadata Streaming Profile page.
2. Click the delete icon available on the upper-right corner of the page.
3. Click **Yes** to delete the profile or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the Metadata Streaming Profile Page | 1020](#)

[Create a Metadata Streaming Profile | 1023](#)

[Edit a Metadata Streaming Profile | 1026](#)

ATP Anti-malware

IN THIS CHAPTER

- [About the Anti-malware Page | 1027](#)
- [Create an Anti-malware Profile | 1029](#)
- [Edit an Anti-malware Profile | 1035](#)
- [Delete an Anti-malware Profile | 1036](#)

About the Anti-malware Page

IN THIS SECTION

- [Tasks You Can Perform | 1027](#)
- [Field Descriptions | 1029](#)

You are here: **Security Services > Advanced Threat Prevention > Anti-malware.**

SRX Series Firewalls use intelligence provided by Juniper Advanced Threat Prevention Cloud (Juniper ATP Cloud) to remediate malicious content using security policies. If configured, security policies block the content before it is delivered to the destination address.

The anti-malware profile defines the content to scan for any malware and the action to be taken when malware is detected. Juniper ATP Cloud uses a pipeline approach to analyzing and detecting malware. If an analysis reveals that the file is malware, it is not necessary to continue the pipeline to further examine the malware.

Tasks You Can Perform

You can perform the following tasks from this page:

- Associate anti-malware profiles with security policies. To do this:
 1. Click **Security Policies** under the Anti-malware page title to directly navigate to the Security Policies page.
 2. Click + to add a new rule or click the pencil icon to edit an existing rule.
 3. Select the anti-malware profile under Advance Services to a specific policy. For more information, see ["Add a Rule to a Security Policy" on page 729](#) .
- Create an anti-malware profile. See ["Create an Anti-malware Profile" on page 1029](#) .
- Edit an anti-malware profile. See ["Edit an Anti-malware Profile" on page 1035](#) .
- Delete an anti-malware profile. See ["Delete an Anti-malware Profile" on page 1036](#) .
- Clone an anti-malware profile. To do this:
 1. Select an existing anti-malware profile to clone.
 2. Select **Clone** from the More link.

The Clone Anti-malware Profile page opens with editable fields. For more information on the options, see ["Create an Anti-malware Profile" on page 1029](#) .
- Show or hide columns in the Anti-malware table. To do this, use the Show Hide Columns icon in the upper-right corner of the page, and select the options to show or deselect to hide options on the page.
- Advanced search for anti-malware profile. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

For an advanced search:

1. Enter the search string in the text box.

Based on your input, a list of items from the filter context menu opens.

2. Select a value from the list and then select a valid operator to perform the advanced search operation.

NOTE: Press Spacebar to add an AND operator or an OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.

3. Press Enter to display the search results in the grid.

Field Descriptions

Table 283 on page 1029 describes the fields on the Anti-malware page.

Table 283: Fields on the Anti-malware Page

| Field | Description |
|--------------------|--|
| Name | Displays the anti-malware profile name. |
| Verdict threshold | Displays the threshold value to determine when a file is considered malware. |
| Protocols | Displays whether the protocol is HTTP, IMAP, SMB, and/or SMTP. Mouse over the protocol name to view the configuration details of inspection profile, action, and logs. |
| Additional Logging | Displays whether the additional logs configured are files under verdict threshold, Allowlist, and/or Blocklist. |

Create an Anti-malware Profile

You are here: **Security Services > Advanced Threat Prevention > Anti-malware.**

Configure the anti-malware profiles for SRX Series Firewall. The profile lets you define which files to send to the cloud for inspection and the action to be taken when malware is detected.

To create an anti-malware profile:

1. Click **+** on the upper-right corner of the Anti-malware page.
The Create Anti-malware Profile page opens.
2. Complete the configuration according to the guidelines provided in [Table 284 on page 1030](#).
3. Click **OK** to save the changes. To discard your changes, click **Cancel**.

Once you create the anti-malware profile, you can associate it with the security policies.

Table 284: Fields on the Create Anti-malware Profile Page

| Field | Action |
|-------------------|--|
| Name | <p data-bbox="837 373 1276 401">Enter a name for the anti-malware profile.</p> <p data-bbox="837 432 1409 533">The name must be a unique string of alphanumeric, special characters and 64 characters maximum. Special characters such as & ()] ? " # are not allowed.</p> |
| Verdict threshold | <p data-bbox="837 600 1227 627">Select a threshold value from the list.</p> <p data-bbox="837 659 1396 793">The threshold value determines when a file is considered malware. If the cloud service returns a file verdict equal to or higher than the configured threshold, then that file is considered as malware.</p> |
| Protocols | |

Table 284: Fields on the Create Anti-malware Profile Page (*Continued*)

| Field | Action |
|-------|--|
| HTTP | <p>Enable this option to inspect advanced anti-malware (AAMW) files downloaded by hosts through HTTP protocol. The AAMW files are then submitted to Juniper ATP Cloud for malware screening.</p> <p>Once you enable this option, configure the following:</p> <ul style="list-style-type: none"> • Action (known verdict)—Select Permit or Block action from the list based on the detected malware. • Action (unknown verdict)—Select Permit or Block action from the list based on the detected malware having a verdict of “unknown.” • Notification—Select one of the following options to permit or block actions based on detected malware: <ul style="list-style-type: none"> • Redirect URL—Enter HTTP URL redirection for a customized client notification based on detected malware with the block action. • Redirect message—Enter the message for a customized client notification based on detected malware with the block action. <p>Range: 1 through 1023</p> • File name—Click Browse to upload a customized file to which users will be directed. The files must be in .php, .html, or .py format and the files will be stored in <code>/jail/var/tmp</code>. • Inspection profile—Select a Juniper Advanced Threat Prevention (ATP) Cloud profile name from the list. The ATP Cloud profile defines the types of files to scan. <p>To view the default and other inspection profiles on the SRX Series Firewall, your device must be enrolled with Juniper ATP Cloud.</p> <ul style="list-style-type: none"> • Logs—Enable this option to add the event to the log file. |

Table 284: Fields on the Create Anti-malware Profile Page (*Continued*)

| Field | Action |
|-------|---|
| IMAP | <p>Enable this option to inspect and manage email attachments sent over IMAP email management.</p> <p>Once you enable this option, configure the following:</p> <ul style="list-style-type: none"> • Inspection profile—Select a Juniper Advanced Threat Prevention (ATP) Cloud profile name from the list. The ATP Cloud profile defines the types of files to scan. <p>To view the default and other inspection profiles on the SRX Series Firewall, your device must be enrolled with Juniper ATP Cloud.</p> <ul style="list-style-type: none"> • Logs—Enable this option to add the event to the log file. |
| SMB | <p>Enable this option to inspect files downloaded by hosts through Server Message Block (SMB) protocol. SMB protocol enables applications or users to access files and other resources on a remote server.</p> <p>Once you enable this option, configure the following:</p> <ul style="list-style-type: none"> • Action—Select Permit or Block action from the list based on the downloaded files. • Inspection profile—Select a Juniper Advanced Threat Prevention (ATP) Cloud profile name from the list. The ATP Cloud profile defines the types of files to scan. <p>To view the default and other inspection profiles on the SRX Series Firewall, your device must be enrolled with Juniper ATP Cloud.</p> <ul style="list-style-type: none"> • Logs—Enable this option to add the event to the log file. |

Table 284: Fields on the Create Anti-malware Profile Page (*Continued*)

| Field | Action |
|-------------------------|--|
| SMTP | <p>Enable this option to inspect and manage email attachments sent over SMTP email management.</p> <p>Once you enable this option, configure the following:</p> <ul style="list-style-type: none"> • Inspection profile—Select a Juniper Advanced Threat Prevention (ATP) Cloud profile name from the list. The ATP Cloud profile defines the types of files to scan. <p>To view the default and other inspection profiles on the SRX Series Firewall, your device must be enrolled with Juniper ATP Cloud.</p> <ul style="list-style-type: none"> • Logs—Enable this option to add the event to the log file. |
| Fallback Actions | |
| Global fallback action | Select None , Permit , or Block action from the list to permit or block the file regardless of its threat level. |
| Logs | Enable this option to add the event to the log file. |

Table 284: Fields on the Create Anti-malware Profile Page (*Continued*)

| Field | Action |
|----------------------------------|---|
| Specific Fallback Configurations | <ul style="list-style-type: none"> • Invalid content size: <ul style="list-style-type: none"> • Select None, Permit, or Block action from the list if the content size exceeds the supported range (32 MB). • Logs—Enable this option to add the event to the log file. • Out of resource action <ul style="list-style-type: none"> • Select None, Permit, or Block action from the list if the service is out of resources. • Logs—Enable this option to add the event to the log file. • Service not ready action <ul style="list-style-type: none"> • Select None, Permit, or Block action from the list if the service is not yet ready. • Logs—Enable this option to add the event to the log file. • Submission timeout action <ul style="list-style-type: none"> • Select None, Permit, or Block action from the list if the submission is timed out. • Logs—Enable this option to add the event to the log file. • Unknown file action: <ul style="list-style-type: none"> • Select None, Permit, or Block action from the list if the file type is unknown. • Logs—Enable this option to add the event to the log file. • Verdict timeout action |

Table 284: Fields on the Create Anti-malware Profile Page (*Continued*)

| Field | Action |
|-------------------------------|--|
| | <ul style="list-style-type: none"> • Select None, Permit, or Block action from the list if the verdict response is timed out. • Logs—Enable this option to add the event to the log file. |
| Additional Logging | |
| Files under verdict threshold | Enable this option to create a system log entry when the file verdict number is less than the threshold. |
| Blocklist | Enable this option to create a system log entry when an attempt is made to access that are listed in the blocklist. |
| Allowlist | Enable this option to create a system log entry when an attempt is made to access that are listed in the allowlist. |

RELATED DOCUMENTATION

[About the Anti-malware Page | 1027](#)

[Edit an Anti-malware Profile | 1035](#)

[Delete an Anti-malware Profile | 1036](#)

Edit an Anti-malware Profile

You are here: **Security Services > Advanced Threat Prevention > Anti-malware.**

To edit an anti-malware profile:

1. Select an existing anti-malware profile to edit.
2. Click the pencil icon on the upper-right corner of the Anti-malware page.

The Edit Anti-malware Profile page opens with editable fields. For more information on the options, see "[Create an Anti-malware Profile](#)" on page 1029 .

Alternatively, you can right-click on the selected anti-malware profile and select **Edit**.

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[About the Anti-malware Page](#) | 1027

[Create an Anti-malware Profile](#) | 1029

[Delete an Anti-malware Profile](#) | 1036

Delete an Anti-malware Profile

You are here: **Security Services** > **Advanced Threat Prevention** > **Anti-malware**.

To delete anti-malware profiles:

1. Select one or more existing anti-malware profiles to delete.
2. Click the delete icon on the upper-right corner of the Anti-malware page.
Alternatively, you can right-click on the selected anti-malware profile and select **Delete**.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the Anti-malware Page](#) | 1027

[Create an Anti-malware Profile](#) | 1029

[Edit an Anti-malware Profile](#) | 1035

ATP SecIntel Profiles

IN THIS CHAPTER

- [About the SecIntel Profiles Page | 1037](#)
- [Configure DNS Sinkhole | 1040](#)
- [Create a Command and Control Profile | 1041](#)
- [Edit a Command and Control Profile | 1044](#)
- [Delete a Command and Control Profile | 1044](#)
- [Create a DNS Profile | 1045](#)
- [Edit a DNS Profile | 1046](#)
- [Delete a DNS Profile | 1047](#)
- [Create an Infected Hosts Profile | 1048](#)
- [Edit an Infected Hosts Profile | 1050](#)
- [Delete an Infected Hosts Profile | 1051](#)

About the SecIntel Profiles Page

IN THIS SECTION

- [Tasks You Can Perform | 1038](#)
- [Field Descriptions | 1039](#)

You are here: **Security Services > Advanced Threat Prevention > SecIntel Profiles.**

Juniper Networks Security Intelligence (SecIntel) provides carefully curated and verified threat intelligence from industry-leading threat feeds to SRX Series Firewalls. This enables blocking malicious and unwanted traffic such as Command and Control (C&C) communications, GeolP, Attacker IPs, and

more with minimum latency. SecIntel delivers real-time threat intelligence by enabling automatic and responsive traffic filtering.

Configure SecIntel profiles to work with security intelligence feeds, such as C&C, DNS, and infected hosts. The Security Intelligence process is responsible for downloading the security intelligence feeds and parsing from the feed connector or ATP Cloud feed server. Anything that matches these scores is considered malware or an infected host.

Tasks You Can Perform

You can perform the following tasks from this page:

- View the list of C&C, DNS, and infected hosts profiles. To do this, select **All**, **Command & Control**, **DNS**, or **Infected Hosts** from the View by list.
- Configure DNS sinkhole. See ["Configure DNS Sinkhole" on page 1040](#) .
- Create a C&C profile. See ["Create a Command and Control Profile" on page 1041](#) .
- Edit a C&C profile. See ["Edit a Command and Control Profile" on page 1044](#) .
- Delete a C&C profile. See ["Delete a Command and Control Profile" on page 1044](#) .
- Create a DNS profile. See ["Create a DNS Profile" on page 1045](#) .
- Edit a DNS profile. See ["Edit a DNS Profile" on page 1046](#) .
- Delete a DNS profile. See ["Delete a DNS Profile" on page 1047](#) .
- Create an infected hosts profile. See ["Create an Infected Hosts Profile" on page 1048](#) .
- Edit an infected hosts profile. See ["Edit an Infected Hosts Profile" on page 1050](#) .
- Delete an infected hosts profile. See ["Delete an Infected Hosts Profile" on page 1051](#) .
- Clone a C&C, DNS, or an infected hosts profile. To do this:
 1. Select an existing C&C, DNS, or an infected hosts profile to clone from the SecIntel Profiles page.
 2. Select **Clone** from the More link.

The Clone *<Command & Control, DNS, or Infected Hosts>* Profile page opens with editable fields.
- Show or hide columns in the SecIntel Profiles table. To do this, use the Show Hide Columns icon in the upper-right corner of the page, and select the options to show or deselect to hide options on the page.
- Advanced search for SecIntel profiles. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when

you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

For an advanced search:

1. Enter the search string in the text box.

Based on your input, a list of items from the filter context menu appears.

2. Select a value from the list and then select a valid operator to perform the advanced search operation.

NOTE: Press Spacebar to add an AND operator or an OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.

3. Press Enter to display the search results in the grid.

Field Descriptions

[Table 285 on page 1039](#) describes the fields on the SecIntel Profiles page.

Table 285: Fields on the SecIntel Profiles Page

| Field | Description |
|--------------|--|
| Name | Displays the SecIntel profile name. |
| Type | Displays if the SecIntel profile is a C&C, a DNS, or an infected hosts profile. |
| Feeds | Displays the feeds that are associated with the C&C, DNS, or infected hosts profile. |
| Block Action | Displays the notification action taken with the block action. For example, Redirect URL, Redirect Message, and Sinkhole. |
| Description | Displays the description of the SecIntel profile. |

Configure DNS Sinkhole

You are here: **Security Services > Advanced Threat Prevention > SecIntel Profiles.**

Configure DNS sinkhole to identify and block DNS requests for the disallowed domains by resolving the domains to a sinkhole server or by rejecting the DNS requests.

To configure DNS sinkhole:

1. Click **DNS Sinkhole**.
The DNS Sinkhole page opens.
2. Complete the configuration according to the guidelines provided in [Table 286 on page 1040](#).
3. Click **OK** to save the changes. To discard your changes, click **Cancel**.

Table 286: Fields on the DNS Sinkhole Page

| Field | Action |
|----------------------------|--|
| IPv4 address | Enter IPv4 address of Juniper Networks or external sinkhole server. |
| FQDN | Enter Fully qualified domain name (FQDN) that must be sent in the DNS response for the sinkhole servers. By default, sinkhole.junipersecurity.net is displayed when your SRX Series Firewall is enrolled with Juniper ATP Cloud. |
| IPv6 address | Enter IPv6 address of Juniper Networks or external sinkhole server. |
| DNS response TTL | Enter Time-to-live (TTL) value in seconds to send the DNS response after taking the DNS sinkhole action. Range: 0 through 3600. Default is 1800. |
| Server response error code | Select a DNS response error code from the list that must be sent for bad domains for server query type: <ul style="list-style-type: none"> • No error—No error response. • Refused—Refuse the DNS query. By default, this option will be selected. |

Table 286: Fields on the DNS Sinkhole Page (Continued)

| Field | Action |
|--------------------------|--|
| Text response error code | <p>Select a DNS response error code from the list that must be sent for bad domains for text query type.</p> <ul style="list-style-type: none"> • No error—No error response. • Refused—Refuse the text query. By default, this option will be selected. |
| Wildcard level | <p>Select number of wildcarding levels that will be iteratively examined for a domain match.</p> <p>Range: 0 through 10. Default is 2.</p> |

RELATED DOCUMENTATION

[About the SecIntel Profiles Page | 1037](#)

Create a Command and Control Profile

You are here: **Security Services > Advanced Threat Prevention > SecIntel Profiles.**

Create a Command and Control (C&C) profile to provide information on C&C servers that have attempted to contact and compromise hosts on your network. A C&C server is a centralized computer that issues commands to botnets of compromised networks of computers and receives reports back from them.

To create a C&C profile:

1. Click **Create > Command & Control** on the upper-right corner of the SecIntel Profiles page. The Create Command & Control Profile page opens.
2. Complete the configuration according to the guidelines provided in [Table 287 on page 1042](#).
3. Click **OK** to save the changes. To discard your changes, click **Cancel**.

Once you create the C&C profile, you can associate it with the SecIntel profile groups.

Table 287: Fields on the Create Command & Control Profile page

| Field | Action |
|------------------------------|---|
| Name | <p>Enter a name for the C&C profile.</p> <p>The name must be a unique string of alphanumeric and special characters; 63-character maximum. Special characters < and > are not allowed.</p> |
| Description | <p>Enter a description for the C&C profile.</p> |
| Default action for all feeds | <p>Drag the slider to change the action to be taken for all the feed types. Actions are Permit (1 - 4), Log (5-6), and Block (7 - 10).</p> <p>Log will have the permit action and also logs the event.</p> |
| Feeds & threat score | <p>Do the following:</p> <ol style="list-style-type: none"> a. Click + to define feeds and threat score to the C&C profile. <ul style="list-style-type: none"> The Add Feeds window appears. b. Enter the following details: <ol style="list-style-type: none"> i. Feeds—Select one or more feeds that are known command and control for botnets from the Available column and move it to the Selected column. ii. Threat score—Drag the slider to change the action to be taken based on the threat score. c. Click OK. |

Table 287: Fields on the Create Command & Control Profile page (*Continued*)

| Field | Action |
|-----------------------|---|
| Block action | <p>Select one of the following block actions from the list:</p> <ul style="list-style-type: none"> • Drop Packets—Device silently drops the session's packet and the session eventually times out. • Close session options—Device sends a TCP RST packet to the client and server and the session is dropped immediately. |
| Close session options | Select one of the following options from the list: None, Redirect URL, Redirect message, or File. |
| Redirect URL | Enter a remote file URL to redirect users when connections are closed. |
| Redirect message | Enter a custom message to send to the users when connections are closed. |
| Upload file | <p>Click Browse to select and upload a file. This file is used to send to the users when connections are closed.</p> <p>NOTE: The files must be in .php, .html, or .py format and will be stored in /jail/var/tm</p> |

RELATED DOCUMENTATION

[About the SecIntel Profiles Page | 1037](#)

[Create a Command and Control Profile | 1041](#)

[Edit a Command and Control Profile | 1044](#)

[Delete a Command and Control Profile | 1044](#)

Edit a Command and Control Profile

You are here: **Security Services** > **Advanced Threat Prevention** > **SecIntel Profiles**.

To edit a Command & Control (C&C) profile:

NOTE: You can edit only the C&C profiles created in J-Web.

1. Select an existing C&C profile to edit.
2. Click the pencil icon on the upper-right corner of the SecIntel Profiles page.
The Edit Command & Control Profile page opens with editable fields. For more information on the options, See "[Create a Command and Control Profile](#)" on page 1041 .
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[About the SecIntel Profiles Page | 1037](#)

[Create a Command and Control Profile | 1041](#)

[Delete a Command and Control Profile | 1044](#)

Delete a Command and Control Profile

You are here: **Security Services** > **Advanced Threat Prevention** > **SecIntel Profiles**.

To delete Command & Control (C&C) profile(s):

1. Select one or more existing C&C profiles to delete.

NOTE: Ensure that selected profiles are not mapped to the SecIntel profile groups.

2. Click the delete icon on the upper-right corner of the SecIntel Profile page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the SecIntel Profiles Page | 1037](#)

[Create a Command and Control Profile | 1041](#)

[Edit a Command and Control Profile | 1044](#)

Create a DNS Profile

You are here: **Security Services** > **Advanced Threat Prevention** > **SecIntel Profiles**.

Create a DNS profile to configure feeds and threat score to list the domains that are known to be connected to malicious activity.

To create a DNS profile:

1. Click **Create** > **DNS** on the upper-right corner of the SecIntel Profiles page.
The Create DNS Profile page opens.
2. Complete the configuration according to the guidelines provided in [Table 288 on page 1045](#).
3. Click **OK** to save the changes. To discard your changes, click **Cancel**.

Once you create the DNS profile, you can associate it with the SecIntel profile groups.

Table 288: Fields on the Create DNS Profile Page

| Field | Action |
|------------------------------|---|
| Name | Enter a name for the DNS profile. The name must be a unique string of alphanumeric and special characters; 63-character maximum. Special characters such as < and > are not allowed. |
| Description | Enter a description for the DNS profile. |
| Default action for all feeds | Drag the slider to change the action to be taken for all the feed types. Actions are Permit (1 - 4), Log (5-6), and Block (7 - 10). Log will have the permit action and also logs the event. |

Table 288: Fields on the Create DNS Profile Page (*Continued*)

| Field | Action |
|----------------------|--|
| Feeds & threat score | <p>Do the following:</p> <ol style="list-style-type: none"> a. Click + to define feeds and threat score to the DNS profile. The Add Feeds window appears. b. Enter the following details: <ol style="list-style-type: none"> i. Feeds—Select one or more feeds from the Available column and move it to the Selected column to associate with the DNS profile. ii. Threat score—Drag the slider to change the action to be taken based on the threat score. c. Click OK. |
| Block action | <p>Select one of the following block actions from the list:</p> <ul style="list-style-type: none"> • Drop Packets—Device silently drops the session’s packet and the session eventually times out. • Sinkhole—DNS sinkhole action for malicious DNS queries. |

RELATED DOCUMENTATION

[About the SecIntel Profiles Page | 1037](#)

[Edit a DNS Profile | 1046](#)

[Delete a DNS Profile | 1047](#)

Edit a DNS Profile

You are here: [Security Services](#) > [Advanced Threat Prevention](#) > [SecIntel Profiles](#).

To edit a DNS profile:

NOTE: You can edit only the DNS profiles created in J-Web.

1. Select an existing DNS profile to edit.
2. Click the pencil icon on the upper-right corner of the SecIntel Profiles page.
The Edit DNS Profile page opens with editable fields. For more information on the options, see "[Create a DNS Profile](#)" on page 1045 .
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[About the SecIntel Profiles Page | 1037](#)

[Create a DNS Profile | 1045](#)

[Delete a DNS Profile | 1047](#)

Delete a DNS Profile

You are here: **Security Services > Advanced Threat Prevention > SecIntel Profiles.**

To delete DNS profile(s):

1. Select one or more existing DNS profiles to delete.

NOTE: Ensure that selected profiles are not mapped to the SecIntel profile groups.

2. Click the delete icon on the upper-right corner of the SecIntel Profile page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the SecIntel Profiles Page | 1037](#)

[Create a DNS Profile | 1045](#)

[Edit a DNS Profile | 1046](#)

Create an Infected Hosts Profile

You are here: **Security Services > Advanced Threat Prevention > SecIntel Profiles.**

Create an infected hosts profile to configure feeds and threat score to list the IP address or IP subnet of the compromised host. Infected hosts indicate local devices that are potentially compromised because they appear to be part of a C&C network or exhibit other symptoms.

To create an infected hosts profile:

1. Click **Create > Infected Hosts** on the upper-right corner of the SecIntel Profiles page.
The Create Infected Hosts Profile page opens.
2. Complete the configuration according to the guidelines provided in [Table 289 on page 1048](#) .
3. Click **OK** to save the changes. To discard your changes, click **Cancel**.

Once you create the infected hosts profile, you can associate it with the SecIntel profile groups.

Table 289: Fields on the Create Infected Hosts Profile Page

| Field | Action |
|------------------------------|--|
| Name | Enter a name for the infected hosts profile. The name must be a unique string of alphanumeric and special characters; 63-character maximum. Special characters such as < and > are not allowed. |
| Description | Enter a description for the infected hosts profile. |
| Default action for all feeds | Drag the slider to change the action to be taken for all the feed types. Actions are Permit (1 - 4), Log (5-6), and Block (7 - 10). Log will have the permit action and also logs the event. |

Table 289: Fields on the Create Infected Hosts Profile Page (*Continued*)

| Field | Action |
|-----------------------|---|
| Feeds & threat score | <p>Do the following:</p> <ol style="list-style-type: none"> a. Click + to define feeds and threat score to the infected hosts profile. The Add Feeds window appears. b. Enter the following details: <ol style="list-style-type: none"> i. Feeds—Select one or more feeds from the Available column and move it to the Selected column to associate with the infected hosts profile. ii. Threat score—Drag the slider to change the action to be taken based on the threat score. c. Click OK. |
| Block action | <p>Select one of the following block actions from the list:</p> <ul style="list-style-type: none"> • Drop Packets—Device silently drops the session's packet and the session eventually times out. • Close session options—Device sends a TCP RST packet to the client and server and the session is dropped immediately. |
| Close session options | <p>Select one of the following options from the list: None, Redirect URL, Redirect message, or File.</p> |
| Redirect URL | <p>Enter a remote file URL to redirect users when connections are closed.</p> |
| Redirect message | <p>Enter a custom message to send to the users when connections are closed.</p> |

Table 289: Fields on the Create Infected Hosts Profile Page (*Continued*)

| Field | Action |
|-------------|--|
| Upload file | <p>Click Browse to select and upload a file. This file is used to send to the users when connections are closed.</p> <p>NOTE: The files must be in .php, .html, or .py format and will be stored in /jail/var/tm</p> |

RELATED DOCUMENTATION

[About the SecIntel Profiles Page | 1037](#)

[Edit an Infected Hosts Profile | 1050](#)

[Delete an Infected Hosts Profile | 1051](#)

Edit an Infected Hosts Profile

You are here: **Security Services > Advanced Threat Prevention > SecIntel Profiles.**

To edit an infected hosts profile:

NOTE: You can edit only the infected hosts profiles created in J-Web.

1. Select an existing infected hosts profile to edit.
2. Click the pencil icon on the upper-right corner of the SecIntel Profiles page.
The Edit Infected Hosts Profile page opens with editable fields. For more information on the options, see "[Create an Infected Hosts Profile](#)" on page 1048 .
3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[About the SecIntel Profiles Page | 1037](#)

[Create an Infected Hosts Profile | 1048](#)

Delete an Infected Hosts Profile

You are here: [Security Services](#) > [Advanced Threat Prevention](#) > [SecIntel Profiles](#).

To delete an infected hosts profile:

1. Select one or more existing infected hosts profiles to delete.

NOTE: Ensure that selected profiles are not mapped to the SecIntel profile groups.

2. Click the delete icon on the upper-right corner of the SecIntel Profile page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the SecIntel Profiles Page | 1037](#)

[Create an Infected Hosts Profile | 1048](#)

[Edit an Infected Hosts Profile | 1050](#)

ATP SecIntel Profile Groups

IN THIS CHAPTER

- [About the SecIntel Profile Groups Page | 1052](#)
- [Create a SecIntel Profile Group | 1054](#)
- [Edit a SecIntel Profile Group | 1056](#)
- [Delete a SecIntel Profile Group | 1056](#)

About the SecIntel Profile Groups Page

IN THIS SECTION

- [Tasks You Can Perform | 1052](#)
- [Field Descriptions | 1053](#)

You are here: **Security Services** > **Advanced Threat Prevention** > **SecIntel Profile Groups**.

Configure a SecIntel profile group to add SecIntel profiles, such as C&C, DNS, and infected hosts. Once created, you can assign this group to the security policy.

Tasks You Can Perform

You can perform the following tasks from this page:

- Associate SecIntel profile groups with Security Policies. To do this:
 1. Click **Security Policies** under the SecIntel Profile Groups page title to directly navigate to the Security Policies page.
 2. Click + to add a new rule or click the pencil icon to edit an existing rule.

3. Select the SecIntel profile group under Advance Services to a specific policy. For more information, see ["Add a Rule to a Security Policy" on page 729](#) .
- Create a SecIntel profile group. See ["Create a SecIntel Profile Group" on page 1054](#) .
 - Edit a SecIntel profile group. See ["Edit a SecIntel Profile Group" on page 1056](#) .
 - Delete a SecIntel profile group. See ["Delete a SecIntel Profile Group" on page 1056](#) .
 - Clone a SecIntel profile group. To do this:
 1. Select an existing a SecIntel profile group to clone.
 2. Select **Clone** from the More link.

The Clone SecIntel Profile Group page opens with editable fields. For more information on the options, see ["Create a SecIntel Profile Group" on page 1054](#) .
 - Show or hide columns in the SecIntel Profile Groups table. To do this, use the Show Hide Columns icon in the upper-right corner of the page and select the options to show or deselect to hide options on the page.
 - Advanced search for SecIntel profile groups. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

For an advanced search:

1. Enter the search string in the text box.

Based on your input, a list of items from the filter context menu appears.

2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

NOTE: Press Spacebar to add an AND operator or an OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.

3. Press Enter to display the search results in the grid.

Field Descriptions

[Table 290 on page 1054](#) describes the fields on the SecIntel Profile Groups page.

Table 290: Fields on the SecIntel Profile Groups Page

| Field | Description |
|-------------------|---|
| Name | Displays the SecIntel profile group name. |
| Command & Control | Displays the C&C profile that you have associated with the SecIntel profile group. |
| DNS | Displays the DNS profile that you have associated with the SecIntel profile group. |
| Infected Hosts | Displays the infected hosts profile that you have associated with the SecIntel profile group. |
| Description | Displays the description for the SecIntel profile group. |

Create a SecIntel Profile Group

You are here: **Security Services > Advanced Threat Prevention > SecIntel Profile Groups.**

Create a SecIntel profile group with SecIntel profiles, such as C&C, DNS, and infected hosts. Once created, you can assign this group to the security policy.

To create a SecIntel profile group:

1. Click **+** on the upper-right corner of the SecIntel Profile Groups page.
The Create SecIntel Profile Groups page opens.
2. Complete the configuration according to the guidelines provided in [Table 291 on page 1055](#).
3. Click **OK** to save the changes. To discard your changes, click **Cancel**.

Once you create the SecIntel profile group, you can associate it with the security policies.

Table 291: Fields on the Create SecIntel Profile Groups Page

| Field | Action |
|-------------------|--|
| Name | <p>Enter a name for the SecIntel profile group.</p> <p>The name must be a unique string of alphanumeric, special characters and 64-character maximum. Special characters such as & ()] ? " # < > are not allowed.</p> |
| Description | <p>Enter description for the SecIntel profile group.</p> |
| Command & Control | <p>Select a C&C profile from the list to associate with the SecIntel profile group.</p> <p>Click Create New to create a new C&C profile inline. For more information on a new C&C profile, see "Create a Command and Control Profile" on page 1041 .</p> |
| DNS | <p>Select a DNS profile from the list to associate with the SecIntel profile group.</p> <p>Click Create New to create a new DNS profile inline. For more information on a new DNS profile, see "Create a DNS Profile" on page 1045 .</p> |
| Infected Hosts | <p>Select a infected hosts profile from the list to associate with the SecIntel profile group.</p> <p>Click Create New to create a new infected hosts profile inline. For more information on a new infected hosts profile, see "Create an Infected Hosts Profile" on page 1048 .</p> |

RELATED DOCUMENTATION

[About the SecIntel Profile Groups Page | 1052](#)

[Edit a SecIntel Profile Group | 1056](#)

[Delete a SecIntel Profile Group | 1056](#)

Edit a SecIntel Profile Group

You are here: **Security Services > Advanced Threat Prevention > SecIntel Profile Groups.**

To edit a SecIntel profile group:

1. Select an existing SecIntel profile group to edit.
2. Click the pencil icon on the upper-right corner of the SecIntel Profile Groups page.
The Edit SecIntel Profile Groups page opens with editable fields. For more information on the options, see "[Create a SecIntel Profile Group](#)" on page 1054 .

Alternatively, you can right-click on the selected SecIntel profile group and select **Edit**.

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[About the SecIntel Profile Groups Page | 1052](#)

[Create a SecIntel Profile Group | 1054](#)

[Delete a SecIntel Profile Group | 1056](#)

Delete a SecIntel Profile Group

You are here: **Security Services > Advanced Threat Prevention > SecIntel Profile Groups.**

To delete SecIntel profile group(s):

1. Select an existing SecIntel profile group to delete.
2. Click the delete icon on the upper-right corner of the SecIntel Profile Groups page.
3. Click **Yes** to delete or click **No** to retain the profile group.

RELATED DOCUMENTATION

[About the SecIntel Profile Groups Page | 1052](#)

[Create a SecIntel Profile Group | 1054](#)

[Edit a SecIntel Profile Group | 1056](#)

SSL Initiation Profiles

IN THIS CHAPTER

- [About the SSL Initiation Profile Page | 1057](#)
- [Add an SSL Initiation Profile | 1059](#)
- [Edit an SSL Initiation Profile | 1062](#)
- [Delete SSL Initiation Profile | 1063](#)

About the SSL Initiation Profile Page

IN THIS SECTION

- [Tasks You Can Perform | 1057](#)
- [Field Descriptions | 1058](#)

You are here: **Security Services > SSL Profiles > SSL Initiation.**

You can configure SSL Initiation profiles.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add an SSL initiation profile. See ["Add an SSL Initiation Profile" on page 1059](#) .
- Edit an SSL initiation profile. See ["Edit an SSL Initiation Profile" on page 1062](#) .
- Delete SSL initiation profile. See ["Delete SSL Initiation Profile" on page 1063](#) .

- Show or hide columns in the SSL Initiation Profile table. To do this, use the Show Hide Columns icon in the upper-right corner of the page and select the options you want to show or deselect to hide options on the page.
- Advance search for SSL initiation profile. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

For an advanced search:

1. Enter the search string in the text box.

Based on your input, a list of items from the filter context menu appears.

2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.

3. Press Enter to display the search results in the grid.

Field Descriptions

Table 292 on page 1058 describes the fields on the SSL Initiation Profile page.

Table 292: Fields on the SSL Initiation Profile Page

| Field | Description |
|------------------|---|
| 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 292: Fields on the SSL Initiation Profile Page (Continued)

| Field | Description |
|-------------------------------|--|
| 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. |

RELATED DOCUMENTATION

[Add an SSL Initiation Profile | 1059](#)

[Edit an SSL Initiation Profile | 1062](#)

[Delete SSL Initiation Profile | 1063](#)

Add an SSL Initiation Profile

You are here: **Security Services > SSL Profiles > SSL Initiation.**

To add an SSL initiation profile:

1. Click **+** on the upper-right corner of the SSL Initiation Profile page.
The Create SSL Initiation Profile page appears.
2. Complete the configuration according to the guidelines provided in [Table 293 on page 1060](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 293: Fields on the Create SSL Initiation Profile Page

| Field | Action |
|----------------------------|--|
| General Information | |
| Name | <p>Enter a unique name of the SSL initiation profile.</p> <p>The string must consist of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed; maximum length is 63 characters.</p> |
| Flow Tracing | <p>Select this option to enable flow trace for troubleshooting policy-related issues for this profile.</p> |
| Protocol Version | <p>Specifies the accepted protocol SSL version.</p> <p>Select the protocol from the list: None, All, TLSv1, TLSv1.1, or TLSv1.2.</p> |
| Preferred Cipher | <p>Specify the cipher depending on their key strength. Select a preferred cipher from the list:</p> <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. |
| Custom Ciphers | <p>Select one or more Ciphers from the list.</p> <p>Click Clear All to clear the selected ciphers from the list.</p> |
| Session Cache | <p>Select this option to enable SSL session cache.</p> |
| Certificate | |

Table 293: Fields on the Create SSL Initiation Profile Page *(Continued)*

| Field | Action |
|-------------------------------|---|
| Trusted CA | <p>Select the trusted certificate authority profile from the list.</p> <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> |
| Client Certificate | <p>Specify a client certificate that is required to effectively authenticate the client.</p> <p>Select the appropriate client certificate from the list.</p> <ul style="list-style-type: none"> • None • SSLRP_Automation_Cert_2 • SSLFP_Automation_Cert_1 • SSLRP_Automation_Cert_1 • SSLFP_Automation_Cert_2 • SSL2 |
| Actions | |
| Server Authentication Failure | <p>Select this option 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> |

Table 293: Fields on the Create SSL Initiation Profile Page *(Continued)*

| Field | Action |
|-----------------------|--|
| CRL Validation | Enable this option to disable CRL validation. |
| Action | Select an action from the list if CRL info is not present: <ul style="list-style-type: none"> • None • Allow • Drop |
| Hold Instruction Code | Select Ignore if you want to keep the instruction code on hold for this profile. |

RELATED DOCUMENTATION

[About the SSL Initiation Profile Page | 1057](#)

[Edit an SSL Initiation Profile | 1062](#)

[Delete SSL Initiation Profile | 1063](#)

Edit an SSL Initiation Profile

You are here: **Security Services > SSL Profiles > SSL Initiation.**

To edit an SSL initiation profile:

1. Select the existing SSL initiation profile that you want to edit on the SSL Initiation Profile page.
2. Click the pencil icon available on the upper-right corner of the page.

The Edit an SSL Initiation Profile page appears with editable fields. For more information on the options, see ["Add an SSL Initiation Profile" on page 1059](#).

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[About the SSL Initiation Profile Page | 1057](#)

[Add an SSL Initiation Profile | 1059](#)

[Delete SSL Initiation Profile | 1063](#)

Delete SSL Initiation Profile

You are here: **Security Services > SSL Profiles > SSL Initiation.**

To delete an SSL initiation profile:

1. Select an SSL initiation profile that you want to delete on the SSL Initiation Profile page.
2. Click the delete icon available on the upper-right corner of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the SSL Initiation Profile Page | 1057](#)

[Add an SSL Initiation Profile | 1059](#)

[Edit an SSL Initiation Profile | 1062](#)

SSL Proxy Profiles

IN THIS CHAPTER

- [About the SSL Proxy Page | 1064](#)
- [Add an SSL Proxy Profile | 1067](#)
- [Clone an SSL Proxy Profile | 1073](#)
- [Edit an SSL Proxy Profile | 1074](#)
- [Delete a SSL Proxy Profile | 1074](#)

About the SSL Proxy Page

IN THIS SECTION

- [Tasks You Can Perform | 1064](#)
- [Field Descriptions | 1065](#)

You are here: **Security Services** > **SSL Profiles** > **SSL Proxy**.

You can create, add, edit, and delete SSL proxy or global policy configurations.

Tasks You Can Perform

You can perform the following tasks from this page:

- Configure global policy. To do this, click **Global Config** at the upper-right corner of the table and enter the session cache timeout in seconds.
- Add an SSL proxy profile. See ["Add an SSL Proxy Profile" on page 1067](#) .
- Edit na SSL proxy profile. See ["Edit an SSL Proxy Profile" on page 1074](#) .

- Delete SSL proxy profile. See ["Delete a SSL Proxy Profile" on page 1074](#) .
- Clone an SSL proxy profile. See ["Clone an SSL Proxy Profile" on page 1073](#) .
- View the details of an SSL proxy profile—To do this, select the SSL proxy profile for which you want to view the details and follow the available options:
 - Click **More** and select **Detailed View**.
 - Right-click on the selected SSL proxy profile and select **Detailed View**.
 - Mouse over to the left of the selected SSL proxy profile and click **Detailed View**.
- Deselect the selected SSL proxy profiles. To do this, click **More** and select **Clear All Selections**.
- Show or hide columns in the SSL Proxy Profiles table. To do this, click the Show Hide Columns icon in the upper-right corner of the custom objects table and select the options you want to view or deselect the options you want to hide on the page.
- Advance search for SSL proxy profiles. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

For an advanced search:

1. Enter the search string in the text box.

Based on your input, a list of items from the filter context menu appears.

2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.

3. Press Enter to display the search results in the grid.

Field Descriptions

[Table 294 on page 1066](#) describes the fields on the SSL Proxy page.

Table 294: Fields on the SSL Proxy Page

| Field | Description |
|---------------------|--|
| 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. |
| Interface | Displays the name of the interface associated with the VLAN. |
| MAC Address | Displays the MAC address associated with the VLAN. |

RELATED DOCUMENTATION

[Add an SSL Proxy Profile | 1067](#)

Add an SSL Proxy Profile

You are here: **Security Services > SSL Profiles > SSL Proxy.**

To add an SSL proxy profile:

1. Click **+** on the upper-right corner of the SSL Proxy Profile page.
The Create SSL Proxy Profile page appears.
2. Complete the configuration according to the guidelines provided in [Table 295 on page 1067](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 295: Fields on the Create SSL Proxy Profile Page

| Field | Action |
|----------------------------|--|
| General Information | |
| Name | <p>Enter a name of the SSL proxy profile.</p> <p>The string must contain alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed; maximum length is 63 characters.</p> |
| Preferred Cipher | <p>Specifies the cipher depending on their key strength. Select a preferred cipher from the list:</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. |

Table 295: Fields on the Create SSL Proxy Profile Page (Continued)

| Field | Action |
|----------------|--|
| Custom Ciphers | <p>Specifies 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>Select the set of ciphers from the list:</p> <ol style="list-style-type: none"> 1. <code>rsa-with-RC4-128-md5—RSA</code>, 128-bit RC4, MD5 hash 2. <code>rsa-with-RC4-128-sha—RSA</code>, 128-bit RC4, SHA hash 3. <code>rsa-with-des-cbc-sha—RSA</code>, DES/CBC, SHA hash 4. <code>rsa-with-3DES-ede-cbc-sha—RSA</code>, 3DES EDE/CBC, SHA hash 5. <code>rsa-with-aes-128-cbc-sha—RSA</code>, 128-bit AES/CBC, SHA hash 6. <code>rsa-with-aes-256-cbc-sha—RSA</code>, 256-bit AES/CBC, SHA hash 7. <code>rsa-export-with-rc4-40-md5—RSA-export</code>, 40-bit RC4, MD5 hash 8. <code>rsa-export-with-des40-cbc-sha—RSA-export</code>, 40-bit DES/CBC, SHA hash 9. <code>rsa-with-aes-256-gcm-sha384—RSA</code>, 256-bit AES/GCM, SHA384 hash 10. <code>rsa-with-aes-256-cbc-sha256—RSA</code>, 256-bit AES/CBC, SHA256 hash 11. <code>rsa-with-aes-128-gcm-sha256—RSA</code>, 128-bit AES/GCM, SHA256 hash 12. <code>rsa-with-aes-128-cbc-sha256—RSA</code>, 256-bit AES/CBC, SHA256 hash 13. <code>ecdhe-rsa-with-aes-256-gcm-sha384—ECDHE</code>, RSA, 256-bit AES/GCM, SHA384 hash |

Table 295: Fields on the Create SSL Proxy Profile Page (Continued)

| Field | Action |
|------------------|--|
| | <p>14. ecdhe-rsa-with-aes-256-cbc-sha—ECDHE, RSA, 256-bit AES/CBC, SHA hash</p> <p>15. ecdhe-rsa-with-aes-256-cbc-sha384—ECDHE, RSA, 256-bit AES/CBC, SHA384 hash</p> <p>16. ecdhe-rsa-with-aes-3des-ede-cbc-sha—ECDHE, RSA, 3DES, EDE/CBC, SHA hash</p> <p>17. ecdhe-rsa-with-aes-128-gcm-sha256—ECDHE, RSA, 128-bit AES/GCM, SHA256 hash</p> <p>18. ecdhe-rsa-with-aes-128-cbc-sha—ECDHE, RSA, 128-bit AES/CBC, SHA hash</p> <p>19. ecdhe-rsa-with-aes-128-cbc-sha256—ECDHE, RSA, 128-bit AES/CBC, SHA256 hash</p> |
| Flow Trace | Select the check box to enable flow trace for troubleshooting policy-related issues. Else leave it blank. |
| 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> |
| Certificate | <p>Select the certificate that you want to associate with this SSL proxy profile from the list.</p> <p>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.</p> |

Table 295: Fields on the Create SSL Proxy Profile Page (*Continued*)

| Field | Action |
|---------------------------------|---|
| Trusted Certificate Authorities | <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 column and move it to the Selected column.</p> |
| Exempted Addresses | <p>Specifies addresses to create whitelists that bypass SSL forward proxy processing.</p> <p>Select the addresses from the from the Available column and move it to the Selected column.</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> |
| Exempted URL Categories | <p>Specifies URL categories to create whitelists that bypass SSL forward proxy processing.</p> <p>Select URL categories from the from the Available column and move it to the Selected column.</p> <p>These URL categories are exempted during SSL inspection. Only the predefined URL categories can be selected for the exemption.</p> |
| Actions | |

Table 295: Fields on the Create SSL Proxy Profile Page *(Continued)*

| Field | Action |
|---------------------|---|
| Server Auth Failure | <p>Select the check box 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> |
| Session Resumption | <p>Select the check box if you do not want session resumption.</p> <p>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.</p> |
| Logging | <p>Select an option from the list to generate logs.</p> <p>You can choose to log All events, Warning, Info, Errors, or different sessions (whitelisted, Allowed, Dropped, or Ignored).</p> |

Table 295: Fields on the Create SSL Proxy Profile Page *(Continued)*

| Field | Action |
|-------------------------------|---|
| 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. <p>Select if a change in SSL parameters requires renegotiation. The options are: None (selected by default), Allow, Allow-secure, and Drop.</p> |
| Certificate Revocation | Select the check box if you want to revoke the certificate. |
| If CRL info not present | <p>Specifies if you want to allow or drop if CRL info is not present.</p> <p>Select the following actions from the list if CRL info is not present : Allow session, Drop session, or None.</p> |
| Hold Instruction Code | Select Ignore if you want to keep the instruction code on hold. |
| Mirror Decrypt Traffic | |

Table 295: Fields on the Create SSL Proxy Profile Page (*Continued*)

| Field | Action |
|--|--|
| Interface | Select an SSL decryption port mirroring interface from the list. This is an Ethernet interface on SRX Series Firewall through which the copy of the SSL decrypted traffic is forwarded to a mirror port. |
| Only after Security Policies Enforcement | Select the check box to enable forwarding the copy of the decrypted traffic to the external mirror traffic collector after enforcing the Layer 7 security services through a security policy. |
| MAC Address | Enter the MAC address of the external mirror traffic collector port. |

RELATED DOCUMENTATION

[About the SSL Proxy Page | 1064](#)

[Edit an SSL Proxy Profile | 1074](#)

[Delete a SSL Proxy Profile | 1074](#)

[Clone an SSL Proxy Profile | 1073](#)

Clone an SSL Proxy Profile

You are here: **Security Services > SSL Profiles > SSL Proxy.**

To clone an SSL proxy profile:

1. Select an SSL Proxy profile that you want to clone and select **Clone** from the More link.

NOTE: Alternatively, you can right-click on the selected SSL Proxy profile and select **Clone**.

The Clone SSL Proxy Profile page appears with editable fields. For more information on the options, see ["Add an SSL Proxy Profile" on page 1067](#).

2. Click **OK** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

[About the SSL Proxy Page | 1064](#)

[Edit an SSL Proxy Profile | 1074](#)

[Delete a SSL Proxy Profile | 1074](#)

Edit an SSL Proxy Profile

You are here: **Security Services > SSL Profiles > SSL Proxy.**

To edit an SSL proxy profile:

1. Select the existing SSL proxy profile that you want to edit on the SSL Proxy Profile page.
2. Click the pencil icon available on the upper-right corner of the page.

The Update SSL Initiation Profile page appears with editable fields. For more information on the options, see "[Add an SSL Proxy Profile](#)" on page 1067 .

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[About the SSL Proxy Page | 1064](#)

[Delete a SSL Proxy Profile | 1074](#)

[Clone an SSL Proxy Profile | 1073](#)

Delete a SSL Proxy Profile

You are here: **Security Services > SSL Profiles > SSL Proxy.**

To delete SSL proxy profile(s):

1. Select one or more SSL proxy profiles that you want to delete on the SSL Proxy page.
2. Click the delete icon available on the upper-right corner of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the SSL Proxy Page | 1064](#)

[Add an SSL Proxy Profile | 1067](#)

[Edit an SSL Proxy Profile | 1074](#)

[Clone an SSL Proxy Profile | 1073](#)

Firewall Authentication—Access Profile

IN THIS CHAPTER

- [About the Access Profile Page | 1076](#)
- [Add an Access Profile | 1078](#)
- [Edit an Access Profile | 1085](#)
- [Delete an Access Profile | 1086](#)

About the Access Profile Page

IN THIS SECTION

- [Tasks You Can Perform | 1076](#)
- [Field Descriptions | 1077](#)

You are here: **Security Services** > **Firewall Authentication** > **Access Profile**.

Use this page to configure Access Profile. Access profiles enable you to define the authentication and accounting servers and their priorities.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create an access profile. See ["Add an Access Profile" on page 1078](#).
- Edit an access profile. See ["Edit an Access Profile" on page 1085](#).
- Delete an access profile. See ["Delete an Access Profile" on page 1086](#).

- View the details of the Access profile—To do this, select the Access profile for which you want to view the details and follow the available options:
 - Click **More** and select **Detailed View**.
 - Right-click on the selected Access profile and select **Detailed View**.
 - Mouse over to the left of the selected Access profiles and click **Detailed View**.
- Show or hide columns in the Access Profile table. To do this, click Show Hide Columns icon in the upper-right corner of the Access Profiles table and select the columns you want to display or deselect the columns you want to hide on the page.
- Advance search for Access profile. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. An example filter condition is displayed in the search text box when you hover over the Search icon. When you start entering the search string, the icon indicates whether the filter string is valid or not.

For an advanced search:

1. Enter the search string in the text box.

Based on your input, a list of items from the filter context menu appears.

2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace to delete a character of the search string.

3. Press Enter to display the search results in the grid.

Field Descriptions

[Table 296 on page 1077](#) describes the fields on the Access Profile page.

Table 296: Fields on the Access Profile Page

| Field | Description |
|--------------|---|
| Profile Name | Displays the name of an access profile. |

Table 296: Fields on the Access Profile Page (Continued)

| Field | Description |
|----------------|--|
| Order 1 | Shows the order in which Junos OS tries different authentication methods when verifying that a client can access the devices. |
| Order 2 | Shows 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. |
| Local Users | Displays the usernames that are created for accessing the application. |
| LDAP Servers | Displays the IP address of the LDAP authentication server. |
| RADIUS Servers | Displays the RADIUS server configuration. |

RELATED DOCUMENTATION

[Add an Access Profile | 1078](#)

[Edit an Access Profile | 1085](#)

[Delete an Access Profile | 1086](#)

Add an Access Profile

You are here: **Security Services > Firewall Authentication > Access Profile.**

To add an access profile:

1. Click **+** on the upper-right corner of the Access Profile page.
The Create Access Profile page appears.
2. Complete the configuration according to the guidelines provided in [Table 297 on page 1079](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 297: Fields on the Access Profile Page

| Field | Description |
|-----------------------|--|
| Name | Enter a name for the access profile. The name must be a unique string of alphanumeric characters, colons, periods, dashes, and underscores. Maximum length is 64 characters. |
| Address assignment | <p>Select an address pool from the list that can be used by different client applications.</p> <p>Click Create Address Pool to add a new address pool. For more information on creating a new address pool, see "Add an Address Pool" on page 1089 .</p> <p>NOTE: If you have selected an address pool in Address Assignment, you need not assign an address pool for LDAP while creating allowed groups.</p> <p>NOTE: For junos-ike package installed platforms, address assignment supports IPv6 address in Juniper Secure Connect > Local Gateway > User Authentication > Create Access Profile > Create Address Pool.</p> |
| Authentication | |
| Local | <p>Select Local to configure local authentication services.</p> <p>To create a new local authentication user:</p> <ol style="list-style-type: none"> Click +. <ul style="list-style-type: none"> The Create Local Authentication User page appears. Enter the following details: <ul style="list-style-type: none"> Username—Enter the user name of the user requesting access. Password—Enter the user password. XAUTH IP Address—Enter the IPv4 address for the client. Group—Enter the group name to store several user accounts together. Click OK to save changes. <p>To edit, select the local authentication user configuration and click the pencil icon.</p> <p>To delete, select the local authentication user configuration and click the delete icon.</p> |

Table 297: Fields on the Access Profile Page (Continued)

| Field | Description |
|--------|--|
| RADIUS | <p>Select RADIUS to configure RADIUS authentication services.</p> <p>To create a new RADIUS server:</p> <ol style="list-style-type: none"> Click +. The Create RADIUS Server page appears. Enter the following details: <ul style="list-style-type: none"> Address—Enter the IPv4 or IPv6 address of the RADIUS server. Secret—Enter the secret password to access the RADIUS server. Port—Enter the port number on which to contact the RADIUS server. Range is 1 through 65535. Default is 1812. Source virtual router—Select the source virtual router from the list. Source interface—Select a source interface (with IP configured) from the list. The IP address of the interface is configured as source address. Timeout—Enter the amount of time that the local device waits to receive a response from a RADIUS authentication server. Range is 1 through 1000 seconds. Default is 3. Retry—Enter the number of retries that a device can attempt to contact a RADIUS server. Range is 1 through 100 seconds. Default is 3. Click OK to save changes. <p>To edit, select the RADIUS server configuration and click the pencil icon.</p> <p>To delete, select the RADIUS server configuration and click the delete icon.</p> |

Table 297: Fields on the Access Profile Page (Continued)

| Field | Description |
|-------|--|
| LDAP | <p>Select LDAP to configure LDAP authentication services.</p> <p>To create a new LDAP server:</p> <ol style="list-style-type: none"> 1. Click +. <ul style="list-style-type: none"> The Create LDAP Server page appears. 2. Enter the following details: <ul style="list-style-type: none"> • Address—Enter the IPv4 or IPv6 address of the LDAP server. • Port—Enter the port number on which to contact the LDAP server. Range is 1 through 65535. Default is 389. • Source virtual router—Select the source virtual router from the list. • Source interface—Select a source interface (with IP configured) from the list. The IP address of the interface is configured as source address. • Timeout—Enter the amount of time that the local device waits to receive a response from an LDAP authentication server. Range is 3 through 90. Default is 5. • Retry—Enter the number of retries that a device can attempt to contact an LDAP server. Range is 1 through 10 seconds. Default is 5. 3. To configure LDAP over TLS/SSL, enter the following: <ol style="list-style-type: none"> a. Start TLS— Enable to configure LDAP over StartTLS. b. Peer name— Enter peer hostname in FQDN format. c. Timeout— Enter the number of of seconds to wait for the secure handshake to be initiated and to complete. Range is 3 through 90 seconds. Default is 5. |

Table 297: Fields on the Access Profile Page (Continued)

| Field | Description |
|-------------------------|--|
| | <p>d. Minimum version— Select the minimum version of TLS protocol enabled in connections to negotiate the TLS connection with the LDAP server. Default is v1.2.</p> <p>e. Certification check— Enable certification check to validate LDAP server's certificate.</p> <p>4. Click OK to save changes.</p> <p>To edit, select the LDAP server configuration and click the pencil icon.</p> <p>To delete, select the LDAP server configuration and click the delete icon.</p> |
| LDAP Options | |
| Base Distinguished Name | <p>Enter the base distinguished name that defines user's basic properties.</p> <p>For example, in the base distinguished name o=juniper, c=us, where c stands for country, and o for organization.</p> |
| Revert Interval | <p>Specifies the amount of time that elapses before the primary server is contacted if a backup server is being used.</p> <p>Use top/bottom arrows to provide the revert interval.</p> <p>Range is 60 through 4294967295.</p> |
| LDAP Option Type | <p>Select an LDAP option from the list:</p> <ul style="list-style-type: none"> • None—No user LDAP distinguished name (DN). • Assemble—Indicates that a user's LDAP DN is assembled through the use of a common name identifier, the username, and base distinguished name. • Search—Indicates that a search is used to get a user's LDAP DN. The search is performed based on the search filter and the search text typed in by the user during authentication. |
| Common Name | <p>Enter a common name identifier used as a prefix for the username during the assembly of the users distinguished name.</p> <p>This option is available when you select Assemble LDAP option type.</p> |

Table 297: Fields on the Access Profile Page (Continued)

| Field | Description |
|--------------------|---|
| Search Filter | <p>Enter the name of the filter to find the users LDAP distinguished name.</p> <p>This option is available when you select Search LDAP option type.</p> |
| Admin Search | <p>Enable this option to perform an LDAP administrator search. By default, the search is an anonymous search.</p> <p>This option is available when you select Search LDAP option type.</p> |
| Distinguished Name | <p>Enter the distinguished name of an administrative user. The distinguished name is used in the bind for performing the LDAP search.</p> <p>This option is available when you select Admin Search is enabled.</p> |
| Secret | <p>Enter the plain-text password for the administrative user.</p> <p>This option is available when you select Admin Search is enabled.</p> |

Table 297: Fields on the Access Profile Page (Continued)

| Field | Description |
|----------------|--|
| Allowed groups | <p>NOTE: Starting in Junos OS Release 23.2R1, J-Web supports Allowed Groups option for Access Profile page. This option is not supported for SRX300 line of Firewalls and SRX550HM Firewall.</p> <p>Configure groups that are allowed to sign in. Users can configure maximum of 32 groups and group lists are limited to 255 bytes.</p> <p>The order in which the membership attribute is received from the LDAP server determines how a user is associated with the configured (allowed) groups. To match the user, the first group in the list received from the LDAP server that matches any of the configured groups is used.</p> <p>Any user who is a member of more than one group can obtain resources from either group, depending on the order of the LDAP server's response. To ensure that the user is assigned the intended resource with certainty, it is recommended that the user belong to only one group.</p> <p>To configure allowed groups:</p> <ol style="list-style-type: none"> 1. Click + available above the allowed groups grid. 2. Enter a group name. 3. Select an address pool from the list. If you want to create a new address pool, click Create Address Pool. See "Add an Address Pool" on page 1089 . <p>NOTE: This step is optional if you have already selected an address pool in the Address Assignment option.</p> <ol style="list-style-type: none"> 4. Click the tick icon to save changes. If you want to discard changes, click X instead. <p>You can also edit and delete allowed groups using the edit icon and delete icon respectively.</p> |

Authentication Order

Table 297: Fields on the Access Profile Page (Continued)

| Field | Description |
|---------|--|
| Order 1 | <p>Select one or more of the following authentication methods:</p> <ul style="list-style-type: none"> • NONE—No authentication for the specified user. • Local—Use local authentication services. • LDAP—Use LDAP. The SRX Series Firewall uses this protocol to get user and group information necessary to implement the integrated user firewall feature. • Radius—Use RADIUS authentication services. <p>If RADIUS servers fail to respond or return a reject response, try local authentication, because it is explicitly configured in the authentication order.</p> |
| Order 2 | Select the authentication method from the list. |

RELATED DOCUMENTATION

[About the Access Profile Page | 1076](#)

[Edit an Access Profile | 1085](#)

[Delete an Access Profile | 1086](#)

Edit an Access Profile

You are here: **Security Services > Firewall Authentication > Access Profile.**

To edit an access profile:

1. Select an existing access profile that you want to edit on the Access Profile page.
2. Click the pencil icon available on the upper-right corner of the page.
The Edit Access Profiles page appears with editable fields. For more information on editing the fields, see ["Add an Access Profile" on page 1078](#).
3. Click **OK** to save the changes or click **Cancel** to discard the changes.

RELATED DOCUMENTATION

[About the Access Profile Page | 1076](#)

[Add an Access Profile | 1078](#)

[Delete an Access Profile | 1086](#)

Delete an Access Profile

You are here: **Security Services > Firewall Authentication > Access Profile.**

To delete an access profile:

1. Select an access profile that you want to delete on the Access Profiles page.
2. Click the delete icon available on the upper-right corner of the page.
3. Click **Yes** to delete access profiles or click **No** to retain access profiles.

RELATED DOCUMENTATION

[About the Access Profile Page | 1076](#)

[Add an Access Profile | 1078](#)

[Edit an Access Profile | 1085](#)

Firewall Authentication—Address Pools

IN THIS CHAPTER

- [About the Address Pools Page | 1087](#)
- [Add an Address Pool | 1089](#)
- [Edit an Address Pool | 1092](#)
- [Delete Address Pool | 1093](#)
- [Search for Text in an Address Pools Table | 1093](#)

About the Address Pools Page

IN THIS SECTION

- [Tasks You Can Perform | 1087](#)
- [Field Descriptions | 1088](#)

You are here: **Security Services** > **Firewall Authentication** > **Address Pools**.

Use this page to get configure Address Pools.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add Address Pool. See ["Add an Address Pool" on page 1089](#) .
- Edit Address Pool. See ["Edit an Address Pool" on page 1092](#) .
- Delete Address Pool. See ["Delete Address Pool" on page 1093](#) .

- Search for Text in an Address Pools table. See ["Search for Text in an Address Pools Table"](#) on page 1093 .
- View the details of an address pool—To do this, select the address pool for which you want to view the details and follow the available options:
 - Click **More** and select **Detailed View**.
 - Right-click on the selected address pool and select **Detailed View**.
 - Mouse over to the left of the selected address pool and click **Detail_View**.
- Filter the address pool based on select criteria. To do this, select the filter icon at the upper-right corner of the address pool 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 address pool table. To do this, use the Show Hide Columns icon in the upper-right corner of the page and select the options you want to show or deselect to hide options on the page.

Field Descriptions

[Table 298 on page 1088](#) describes the fields on the Address Pools page.

Table 298: Fields on the Address Pools Page

| Field | Description |
|----------------|---|
| Identifier | Specifies the name of the address pool. |
| Subnet | Specifies the IPv4 or IPv6 subnet configured. |
| Primary DNS | Specifies the primary-dns IP address. |
| Secondary DNS | Specifies the secondary-dns IP address. |
| Primary WINS | Specifies the primary-wins IP address. |
| Secondary WINS | Specifies the secondary-wins IP address. |

Table 298: Fields on the Address Pools Page (Continued)

| Field | Description |
|------------------------|--|
| Named Address Ranges | Specifies the name of the address range. |
| Excluded Address Range | Specifies the range of address excluded for the address pool. |
| Static Address Range | Specifies the static address range for the address pool, |
| Linked Address Pool | Specifies the secondary address pool that is linked to the primary address pool. |

RELATED DOCUMENTATION

[Add an Address Pool | 1089](#)

[Edit an Address Pool | 1092](#)

[Delete Address Pool | 1093](#)

[Search for Text in an Address Pools Table | 1093](#)

Add an Address Pool

You are here: **Security Services > Firewall Authentication > Address Pools.**

To add an address pool:

1. Click **+** on the upper-right corner of the Address Pools page.
The Create Address Pool page appears.
2. Complete the configuration according to the guidelines provided in [Table 299 on page 1089](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 299: Fields on the Create Address Pool Page

| Field | Description |
|--------|--|
| Subnet | Enter the subnet for IPv4 or IPv6 address. |

Table 299: Fields on the Create Address Pool Page (Continued)

| Field | Description |
|-------------|---|
| Identifier | Enter the address pool name. |
| DNS servers | Enter the primary, secondary, or both DNS IP address. |
| WINS server | Enter the primary, secondary, or both WINS IP address. NOTE: This option will not be available if you enter an IPv6 subnet address. |

Named Address Ranges**NOTE:** Named Address Range is not available for IPsec VPN.

| | |
|--------------|--|
| Add | Click + to add a new named address range for the address pool. |
| Name | Enter a name for the IP address range. |
| From address | Enter the lower limit of the address range. |
| To address | Enter the upper limit of the address range and click the tick icon to save the changes. If you want to discard, click X. |
| Delete | Click the delete icon to delete the address range for the address pool. |

Excluded Address Ranges

| | |
|--------------|---|
| Add | Click + to add a new excluded address range for the address pool. |
| From address | Enter the lower limit of the address range. |
| To address | Enter the upper limit of the address range and click the tick icon to save the changes. If you want to discard, click X. NOTE: You can add up to maximum of 20 excluded addresses and 16 excluded address ranges. |

Table 299: Fields on the Create Address Pool Page (Continued)

| Field | Description |
|---------------------------------------|--|
| Delete | Click the delete icon to delete the excluded address range for the address pool. |
| Static Address Binding | |
| Assign static IP address for username | Enable to assign a static IP address for username. Disabled by default. NOTE: By default, this option will be enabled and hidden for IPsec VPN. |
| Add | Click + to add a new static address for the address pool. |
| Hostname | Enter a unique string that must begin with an alphanumeric character and can include periods, dashes, and underscores; no spaces allowed; 63-character maximum. NOTE: <ul style="list-style-type: none"> • Hostname should not be a duplicate. • Hostname field will be available only if you enable Assign static IP address for username. |
| Username | Enter a unique string that must begin with an alphanumeric character and can include periods, dashes, and underscores; no spaces allowed. NOTE: <ul style="list-style-type: none"> • Username should not be a duplicate. • Username field will be available only if you enable Assign static IP address for username. |
| IP address | Enter an IP address within the subnet entered. NOTE: IP address should not duplicate with other host name IP address. |

Table 299: Fields on the Create Address Pool Page (Continued)

| Field | Description |
|---------------------|--|
| MAC address | <p>Enter a valid MAC address and click the tick icon to save the changes. If you want to discard, click X.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • MAC address should not duplicate with other host name MAC address. • MAC address field will not be available if you enable Assign static IP address for username. |
| Delete | Click the delete icon to delete static address binding. |
| Linked address pool | <p>Select an option from the list. To add a new secondary address pool, do the following:</p> <ol style="list-style-type: none"> 1. Click Add. The Create Address Pool page appears. 2. Complete the configuration according to the guidelines provided in Table 299 on page 1089. 3. Click OK to save the changes. If you want to discard your changes, click Cancel. <p>NOTE: You must link an IPv4/IPv6 subnet address pool with another IPv4/IPv6 address respectively.</p> |

RELATED DOCUMENTATION

[About the Address Pools Page | 1087](#)

[Edit an Address Pool | 1092](#)

[Delete Address Pool | 1093](#)

[Search for Text in an Address Pools Table | 1093](#)

Edit an Address Pool

You are here: **Security Services > Firewall Authentication > Address Pools.**

To edit an address pool:

1. Select an existing address pool that you want to edit on the Address Pools page.
2. Click the pencil icon available on the upper-right corner of the page.

The Edit Address Pool page appears with editable fields. For more information on the options, see ["Add an Address Pool" on page 1089](#) .

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[About the Address Pools Page | 1087](#)

[Add an Address Pool | 1089](#)

[Delete Address Pool | 1093](#)

[Search for Text in an Address Pools Table | 1093](#)

Delete Address Pool

You are here: **Security Services > Firewall Authentication > Address Pools.**

To delete an address pool:

1. Select an address pool that you want to delete on the Address Pools page.
2. Click the delete icon available on the upper-right corner of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the Address Pools Page | 1087](#)

[Add an Address Pool | 1089](#)

[Edit an Address Pool | 1092](#)

[Search for Text in an Address Pools Table | 1093](#)

Search for Text in an Address Pools Table

You are here: **Security Services > Firewall Authentication > Address Pools.**

You can use the search icon in the upper-right corner of the Address Pools page to search for text containing letters and special characters on that page.

To search for text:

1. Click the search icon and enter partial text or full text of the keyword in the search bar.
The search results are displayed.
2. Click **X** next to a search keyword or click **Clear All** to clear the search results.

RELATED DOCUMENTATION

[About the Address Pools Page | 1087](#)

[Add an Address Pool | 1089](#)

[Edit an Address Pool | 1092](#)

[Delete Address Pool | 1093](#)

Firewall Authentication Settings

IN THIS CHAPTER

- [About the Authentication Settings Page | 1095](#)

About the Authentication Settings Page

IN THIS SECTION

- [Field Description | 1095](#)

You are here: **Security Services > Firewall Authentication > Authentication Settings.**

Use this page to configure firewall authentication. You can click the arrow pointing outwards icon to expand all the options or click the arrow pointing inwards to collapse or hide all the options.

To edit this page, configure minimum one access profile under **Security Services > Firewall Authentication > Access Profile.**

Field Description

To configure a firewall authentication:

1. Complete the configuration according to the guidelines provided in [Table 300 on page 1096](#) .
2. Click **Save** to save the changes.

[Table 300 on page 1096](#) describes the fields on the Firewall Authentication page.

Table 300: Fields on the Firewall Authentication Page

| Field | Description |
|------------------------------|--|
| Pass-through Settings | |
| Default Profile | Select a profile from the list that the policies use to authenticate users. |
| FTP Banners | |
| Login | Displays the login prompt for users logging in using FTP. Maximum characters are 250. |
| Success | Displays a successful login prompt for users logging in using FTP. Maximum characters are 250. |
| Fail | Displays failed login prompt for users logging in using FTP. Maximum characters are 250. |
| Telnet Banners | |
| Login | Displays the login prompt for users logging in using telnet. Maximum characters are 250. |
| Success | Displays a successful login prompt for users logging in using telnet. Maximum characters are 250. |
| Fail | Displays failed login prompt for users logging in using telnet. Maximum characters are 250. |
| HTTP Banner | |
| Login | Displays the login prompt for users logging in using HTTP. |

Table 300: Fields on the Firewall Authentication Page (Continued)

| Field | Description |
|--------------------------|---|
| Success | Displays a successful login prompt for users logging in using HTTP. |
| Fail | Displays failed login prompt for users logging in using HTTP. |
| Web-auth-settings | |
| Default Profile | Select a profile that the policies use to authenticate users. |
| Success | Displays a successful login prompt for users logging in using Web authentication banner. |
| Logo Image Upload | |
| Logo File | 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 | Click the button to navigate to the logo image on the user's local disk. |
| Sync | Click the button to sync the logo image. |
| Restore | Click the button to restore the Web authentication logo. |

RELATED DOCUMENTATION

| [About the UAC Settings Page](#) | 1098

Firewall Authentication—UAC Settings

IN THIS CHAPTER

- [About the UAC Settings Page | 1098](#)

About the UAC Settings Page

IN THIS SECTION

- [Field Description | 1098](#)

You are here: **Security Services > Firewall Authentication > UAC Settings.**

Use this page to configure UAC Settings.

Field Description

To configure UAC settings:

1. Complete the configuration according to the guidelines provided in [Table 301 on page 1098](#).
2. Click **Save** to save the changes.

[Table 301 on page 1098](#) describes the fields on the UAC Setting page.

Table 301: Fields on the UAC Setting Page

| Field | Description |
|-------|-------------|
|-------|-------------|

Global Settings

Table 301: Fields on the UAC Setting Page (Continued)

| Field | Description |
|----------------------------|--|
| Certificate Verification | <p>Determines whether server certificate verification is required when initiating a connection between a device and an Access Control Service in a UAC configuration.</p> <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 | <p>Specifies the value in seconds that the device should expect to receive a heartbeat signal from the IC Series device.</p> <p>Enter the heartbeat interval in seconds. Range: 1 through 9999.</p> |
| Test Only Mode | <p>Allows all traffic and log enforcement result.</p> <p>Enable the Test Only Mode option.</p> |
| Timeout | <p>Specifies (in seconds) that the device should wait to get a heartbeat response from an IC Series UAC Appliance.</p> <p>Enter the timeout in seconds. Range: 2 through 10000.</p> |
| Timeout Action | <p>Specifies the action to be performed when a timeout occurs and the device cannot connect to an Infranet Enforcer.</p> <p>Select the timeout action from the list.</p> |
| Infranet Controller | |

Table 301: Fields on the UAC Setting Page (Continued)

| Field | Description |
|----------------------------|---|
| Infranet Controller | <p>Click + to add an infranet controller.</p> <p>Click pencil icon to edit a selected infranet controller.</p> <p>Click delete icon to delete the selected infranet controller.</p> |
| Name | Enter a name for the Infranet Controller. |
| IP address | Enter an IP address for the Infranet Controller. |
| Interface | Select an interface used for the Infranet Controller. |
| Interface | Enter the password to use for the Infranet Controller |
| CA Profiles | <p>Select a CA from the list in the CA Profiles column and then click the right arrow to move them to the Selected column.</p> <p>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.</p> |
| Port | <p>Specifies the port number to be associated with this Infranet Controller for data traffic.</p> <p>Enter a value from 1 through 65,535.</p> |
| Server Certificate Subject | Enter the server certificate subject name of the Infranet Controller certificate to match. |
| Captive Portal | |
| Captive Portal | <p>Specifies the preconfigured security policy for captive portal on the Junos OS Enforcer.</p> <p>Click + to add a captive portal.</p> <p>Click pencil icon to edit a selected captive portal.</p> <p>Click delete icon to delete the selected captive portal.</p> |

Table 301: Fields on the UAC Setting Page (Continued)

| Field | Description |
|------------------|---|
| Name | Enter a name for the captive portal. |
| Redirect Traffic | Select a traffic type to be redirected. |
| Redirect URL | Enter the URL to which the captive portal should be directed. |

RELATED DOCUMENTATION

| [About the Application Tracking Page](#) | 835

Firewall Authentication—Active Directory

IN THIS CHAPTER

- [About the Active Directory Page | 1102](#)

About the Active Directory Page

You are here: **Security Services** > **Firewall Authentication** > **Active Directory**.

You can configure Active directory.

[Table 302 on page 1102](#) describes the fields on the Active Directory page.

Table 302: Fields on the Active Directory Page

| Field | Description |
|----------------------------|--|
| 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 Firewall to retrieve address-to-user mapping information. |
| Timeout | |

Table 302: Fields on the Active Directory Page (Continued)

| Field | Description |
|--|---|
| 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>Enter the number of seconds that the domain PC has to respond to the SRX Series Firewall'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>Enter a value. The range is 10 through 1440 minutes. 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>Enter a value. The range is 10 through 1440 minutes. 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> |
| Filter | |

Table 302: Fields on the Active Directory Page (Continued)

| Field | Description |
|------------------------|---|
| Include | <p>Enable to include IP addresses from the Available column.</p> <p>Click + 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 + 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 Virtual Firewall devices, 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 Firewalls, you can create only one domain. Starting in Junos OS Release 23.4R1, for SRX1600 and SRX2300 Firewalls, you can configure the integrated user firewall in a maximum of two domains. <p>You can select the pencil icon to edit the domain or select delete icon to delete the domain.</p> |
| General | |

Table 302: Fields on the Active Directory Page (*Continued*)

| Field | Description |
|----------------------------------|---|
| Domain Name | <p>Enter the name of the domain.</p> <p>The range for the domain name is 1 through 64 characters.</p> |
| Username | <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) | |
| Domain Controller(s) | <p>Click + 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. <p>You can configure up to maximum of 10 domain controllers.</p> <ul style="list-style-type: none"> IP Address—Enter the IP address of the domain controller. |
| User Group Mapping (LDAP) | |
| User Group Mapping (LDAP) | <p>Click +:</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. <p>Default value is port 443.</p> |
| Base Distinguish Name | <p>Enter the LDAP base distinguished name (DN).</p> <p>Example: DC=example,DC=net</p> |

Table 302: Fields on the Active Directory Page (Continued)

| Field | Description |
|-----------------------------|---|
| Username | 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 | Enable this option to specify the algorithm used while the SRX Series Firewall 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 Firewall scans the event log on the domain controller. The range is 5 through 60 seconds.</p> <p>Default value is 60 seconds.</p> |
| Initial Event Log TimeSpan | <p>Enter the time of the earliest event log on the domain controller that the SRX Series Firewall will initially scan. This scan applies to the initial deployment only. After WMIC and the user identification start working, the SRX Series Firewall scans only the latest event log.</p> <p>The range is 1 through 168 hours. Default value is 1 hour.</p> |

Change History Table

Feature support is determined by the platform and release you are using. Use [Feature Explorer](#) to determine if a feature is supported on your platform.

| Release | Description |
|---------|--|
| 19.2R1 | Starting in Junos OS Release 19.2R1, the default value is 60 minutes. |
| 19.2R1 | Starting in Junos OS Release 19.2R1, for SRX4200, SRX1500, SRX550M, and vSRX Virtual Firewall devices, 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 Firewalls, you can create only one domain. |

RELATED DOCUMENTATION

| [About the Authentication Priority Page](#) | 1111

Firewall Authentication—Local Authentication

IN THIS CHAPTER

- [About the Local Authentication Page | 1108](#)
- [Add a Local Authentication Entry | 1109](#)
- [Delete a Local Authentication Entry | 1110](#)

About the Local Authentication Page

IN THIS SECTION

- [Tasks You Can Perform | 1108](#)
- [Field Descriptions | 1109](#)

You are here: **Security Services > Firewall Authentication > Local Authentication.**

Use this page to enable or disable authentication priority configuration options.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a local auth entry. See "[Add a Local Authentication Entry](#)" on page 1109 .
- Delete a local auth entry. See "[Delete a Local Authentication Entry](#)" on page 1110 .
- Clear all the local auth entry. To do this, select the local auth entries you want to clear and click **Clear All** at the upper-right corner of the table.

Field Descriptions

Table 303 on page 1109 describes the fields on the Local Auth page.

Table 303: Fields on the Local Auth Page

| Field | Description |
|-----------|---|
| Filter by | Displays the local authentication configuration based on the selected filter. |
| IP | Displays the IP address. |
| Username | Displays the name of the user. |
| Role Name | Displays the list of roles assigned to the username. |
| Search | Select the filter you want and enter your inputs based on the filter type. Then, click the search icon to display the output based on your selected filter. |

RELATED DOCUMENTATION

[Add a Local Authentication Entry | 1109](#)

[Delete a Local Authentication Entry | 1110](#)

Add a Local Authentication Entry

You are here: **Security Services > Firewall Authentication > Local Authentication.**

To add a local authentication entry:

1. Click **+** on the upper-right corner of the Local Authentication page.
The Add Local Auth Entry page appears.
2. Complete the configuration according to the guidelines provided in [Table 304 on page 1110](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 304: Fields on the Add Local Auth Page

| Field | Action |
|------------|---|
| IP Address | Enter an IP address for the local authentication. |
| Username | Enter a username for the local authentication. |
| Role List | <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 the delete (X) icon.</p> <p>To edit a role, hover over the role name and click the pencil icon.</p> <p>NOTE: You can configure only maximum of 200 roles for a local authentication entry.</p> |

RELATED DOCUMENTATION

[About the Local Authentication Page | 1108](#)

[Delete a Local Authentication Entry | 1110](#)

Delete a Local Authentication Entry

You are here: **Security Services > Firewall Authentication > Local Authentication.**

To delete a local authentication entry:

1. Select a local authentication entry that you want to delete on the Local Authentication page.
2. Click the delete icon available on the upper-right corner of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the Local Authentication Page | 1108](#)

[Add a Local Authentication Entry | 1109](#)

Firewall Authentication—Authentication Priority

IN THIS CHAPTER

- [About the Authentication Priority Page | 1111](#)

About the Authentication Priority Page

You are here: **Security Services** > **Firewall Authentication** > **Authentication Priority**.

Use this page to enable or disable authentication priority configuration options.

[Table 305 on page 1111](#) describes the fields on the Authentication Priority page.

Table 305: Fields on the Authentication Priority Page

| Field | Description |
|--------------------------------|--|
| Enable local authentication | Select the Enable local authentication check box to enable local authentication. |
| Priority | Enter a priority value (1 through 65,535) in the Priority field. NOTE: The default local authentication priority value is 100. |
| Enable firewall authentication | Select the check box to enable firewall authentication. |
| Priority | Enter a priority value (1 through 65,535) in the Priority field. NOTE: The default firewall authentication priority value is 150. |
| Enable unified access control | Select the check box to enable UAC authentication. |

Table 305: Fields on the Authentication Priority Page (*Continued*)

| Field | Description |
|-------------------------|---|
| Priority | Enter a priority value (1 through 65,535) in the Priority field. NOTE: The default local authentication priority value is 200. |
| Enable active directory | Select the check box to enable UAC authentication. |
| Priority | Enter a priority value (1 through 65,535) in the Priority field. NOTE: The default local authentication priority value is 125. |
| OK | Click OK to save the configuration changes. |
| Reset | Click Reset to set the priority values and enable options to the default configuration. |

RELATED DOCUMENTATION

| [About the Local Authentication Page | 1108](#)

Firewall Authentication—JIMS

IN THIS CHAPTER

- [About the Juniper Identity Management Service Page | 1113](#)
- [Add a Juniper Identity Management Service Profile | 1114](#)
- [Edit a Juniper Identity Management Service Profile | 1118](#)
- [Delete a Juniper Identity Management Service Profile | 1119](#)

About the Juniper Identity Management Service Page

IN THIS SECTION

- [Tasks You Can Perform | 1113](#)

You are here: **Security Services > Firewall Authentication > JIMS.**

You can add, edit or delete a Juniper Identity Management Services (JIMS) profile. You can also view the connection status of this SRX Series Firewall with the JIMS.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a Juniper Identity Management Service profile. See ["Add a Juniper Identity Management Service Profile" on page 1114](#) .
- Edit a Juniper Identity Management Service profile. See ["Edit a Juniper Identity Management Service Profile" on page 1118](#) .

- Delete a Juniper Identity Management Service profile. See "[Delete a Juniper Identity Management Service Profile](#)" on page 1119 .

RELATED DOCUMENTATION

[Add a Juniper Identity Management Service Profile](#) | 1114

Add a Juniper Identity Management Service Profile

You are here: **Security Services** > **Firewall Authentication** > **JIMS**.

To add a Juniper Identity Management Service (JIMS) profile:

1. Click **Configure** on the Juniper Identity Management Service page.
The Configure Juniper Identity Management Service Profile page appears.
2. Complete the configuration according to the guidelines provided in [Table 306 on page 1114](#) .
3. Click **Finish** to save the changes. If you want to discard your changes, click **Cancel**.

Table 306: Fields on the Configure Juniper Identity Management Service Profile Page

| Field | Action |
|---|---|
| General Information | |
| Connection for Primary and Secondary Juniper Identity Management Service | |
| Connection Type | Select a connection type from the list. The options available are: HTTPS and HTTP. |
| Port | 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 | Enter a primary IP address of JIMS server. |

Table 306: Fields on the Configure Juniper Identity Management Service Profile Page (Continued)

| Field | Action |
|--|--|
| Primary CA Certificate | <p>Specifies the primary certificate of the JIMS. SRX Series Firewall will use it to verify JIMS's certificate for SSL connection.</p> <p>Select Upload CA certificate to device or specify the path of the file on device.</p> |
| Primary CA Certificate file upload | <p>Enables you to locate and upload the CA certificate.</p> <p>Click Browse to locate the CA certificate on your device and click Upload the selected CA certificate.</p> |
| Primary CA Certificate file path | <p>Enter a file path of the primary CA certificate.</p> |
| Primary Client ID | <p>Enter a primary client ID of the SRX Series Firewall to obtain access token. It must be consistent with the configuration of the API client created on JIMS.</p> |
| Primary Client Secret | <p>Enter a password which enables you to access the primary identity management server.</p> <p>Specifies the client secret of the SRX Series Firewall to obtain access token. It must be consistent with the configuration of the API client created on JIMS.</p> |
| Secondary Juniper Identity Management Service Server | <p>Enables a secondary JIMS server, its IP address, CA certificate, client ID, and client secret.</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> |

Table 306: Fields on the Configure Juniper Identity Management Service Profile Page (Continued)

| Field | Action |
|--------------------------|--|
| Token API | <p>Enter the token API to specify the path of the URL for acquiring access token.</p> <p>Default is 'oauth_token/oauth'.</p> |
| Query API | <p>Enter the path where the URL for querying user identities 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 | <p>Specifies the maximum number of items in one batch query.</p> <p>Enter the number of items. Range is 100 to 1000 and the default number is 200.</p> |
| Query Interval | <p>Specifies the interval for querying the newly generated user identities.</p> <p>Enter the number of seconds you need between each query. The range is 1 through 60 (seconds), and the default value is 5.</p> |
| IP Query | |
| Query Delay Time | <p>Specifies the time delay to send individual IP query.</p> <p>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.</p> |
| No IP Query | <p>Select the check box if you want to disable the IP query function that is enabled by default.</p> |

Table 306: Fields on the Configure Juniper Identity Management Service Profile Page (Continued)

| Field | Action |
|---|--|
| Authentication Timeout | |
| Authentication Entry Timeout | <p>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.</p> <p>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.</p> |
| Invalid Authentication Entry Timeout | <p>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.</p> <p>Specifies the timeout value of invalid auth entry in the SRX Series authentication table for either Windows active directory or Aruba ClearPass.</p> |
| Filter | |
| NOTE: You can select address set with maximum of 20 IP addresses and address set with wild card addresses. | |
| Include IP Address Book | <p>Select an IP address book from the predefined address book in which an address set must be selected as IP filter.</p> |
| Include IP Address Set | <p>Specifies the predefined address set selected as IP filter.</p> <p>Select an IP address set from the list.</p> <p>To add a new address set for the IP address book, click Add New Address Set.</p> |
| Exclude IP Address Book | <p>Select an IP address book that you want identity management profile to exclude.</p> |

Table 306: Fields on the Configure Juniper Identity Management Service Profile Page (Continued)

| Field | Action |
|------------------------|---|
| Exclude IP Address Set | Select the predefined address set that you want identity management profile to exclude. |
| Filter to Domain | Enter one or more active directory domains, to the SRX Series Firewall. You can specify up to twenty domain names for the filter. |

RELATED DOCUMENTATION

[About the Juniper Identity Management Service Page | 1113](#)

[Edit a Juniper Identity Management Service Profile | 1118](#)

[Delete a Juniper Identity Management Service Profile | 1119](#)

Edit a Juniper Identity Management Service Profile

You are here: **Security Services** > **Firewall Authentication** > **JIMS**.

To edit a Juniper Identity Management Service (JIMS) profile:

1. Select the existing JIMS profile that you want to edit on the Juniper Identity Management Service page.
2. Click the pencil icon available on the upper-right corner of the page.

The Edit a Juniper Identity Management Service Profile page appears with editable fields. For more information on the options, see "[Add a Juniper Identity Management Service Profile](#)" on page 1114 .

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[About the Juniper Identity Management Service Page | 1113](#)

[Add a Juniper Identity Management Service Profile | 1114](#)

[Delete a Juniper Identity Management Service Profile | 1119](#)

Delete a Juniper Identity Management Service Profile

You are here: **Security Services** > **Firewall Authentication** > **JIMS**.

To delete a Juniper Identity Management Service (JIMS) profile:

1. Click the delete icon available on the upper-right corner of the Juniper Identity Management Service page.
2. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the Juniper Identity Management Service Page | 1113](#)

[Add a Juniper Identity Management Service Profile | 1114](#)

[Edit a Juniper Identity Management Service Profile | 1118](#)

ICAP Redirect

IN THIS CHAPTER

- [About the ICAP Redirect Profile Page | 1120](#)
- [Add an ICAP Redirect Profile | 1122](#)
- [Edit an ICAP Redirect Profile | 1125](#)
- [Delete ICAP Redirect Profile | 1125](#)

About the ICAP Redirect Profile Page

IN THIS SECTION

- [Tasks You Can Perform | 1120](#)
- [Field Descriptions | 1121](#)

You are here: **Security Services** > **ICAP Redirect**.

You can configure ICAP Redirect Profile.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create an ICAP redirect profile. See ["Add an ICAP Redirect Profile" on page 1122](#) .
- Edit an ICAP redirect profile. See ["Edit an ICAP Redirect Profile" on page 1125](#) .
- Delete an ICAP redirect profile. See ["Delete ICAP Redirect Profile" on page 1125](#) .

- Filter the ICAP redirect profiles based on select criteria. To do this, select the filter icon at the upper-right corner of the ICAP redirect profiles 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 ICAP redirect profiles table. To do this, click the Show Hide Columns icon in the upper-right corner of the ICAP redirect profiles table and select the options you want to view or deselect the options you want to hide on the page.
- Advance search for ICAP redirect profiles. To do this, use the search text box present above the table grid. The search includes the logical operators as part of the filter string. In the search text box, when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.

For an advanced search:

1. Enter the search string in the text box.

Based on your input, a list of items from the filter context menu appears.

2. Select a value from the list and then select a valid operator based on which you want to perform the advanced search operation.

NOTE: Press Spacebar to add an AND operator or OR operator to the search string. Press backspace at any point of time while entering a search criteria, only one character is deleted.

3. Press Enter to display the search results in the grid.

Field Descriptions

[Table 307 on page 1121](#) describes the fields on the ICAP Redirect Profile page.

Table 307: Fields on the ICAP Redirect Profile Page

| Field | Description |
|---------|---|
| Name | Displays the ICAP Service profile name. |
| Timeout | Displays the server response timeout in milliseconds. |
| Server | Displays the ICAP Redirection Server. |

Table 307: Fields on the ICAP Redirect Profile Page (Continued)

| Field | Description |
|-----------------|--|
| Fallback Option | Specifies the request timeout action when the request is sent to the server. |
| HTTP Redirect | Enables redirect service on HTTP request/HTTP response. |

RELATED DOCUMENTATION

[Add an ICAP Redirect Profile | 1122](#)

[Edit an ICAP Redirect Profile | 1125](#)

[Delete ICAP Redirect Profile | 1125](#)

Add an ICAP Redirect Profile

You are here: **Security Services > ICAP Redirect.**

To add an ICAP redirect profile:

1. Click **+** on the upper-right corner of the ICAP Redirect Profiles page.
The Create ICAP Redirect Profile page appears.
2. Complete the configuration according to the guidelines provided in [Table 308 on page 1122](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 308: Fields on the Create ICAP Redirect Profile Page

| Field | Action |
|---------|--|
| Name | Enter a unique ICAP Service profile name. The string must contain alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed; maximum length is 63 characters. |
| Timeout | Enter the server response timeout in milliseconds. The range is between 100 milliseconds to 50000 milliseconds. |

Table 308: Fields on the Create ICAP Redirect Profile Page (Continued)

| Field | Action |
|---|---|
| HTTP Redirect Option | |
| Request | Select to enable redirect service on HTTP request. |
| Response | Select to enable redirect service on HTTP response. |
| ICAP Server | |
| You can configure ICAP Redirection server by the following options: | |
| Add —Create an ICAP Redirect server. Enter information as specified in Table 309 on page 1123 . | |
| Edit —Edit an ICAP Redirect server configuration. Enter information as specified in Table 309 on page 1123 . | |
| Fallback Option | |
| Timeout Action | Select the timeout action from the list. The available options are: None, Permit, Log Permit, and Block. |
| Connectivity Action | Select the connectivity action from the list that the request cannot be sent out due to connection issues. |
| Default Action | Select a default action from the list to be taken when there are scenarios other than the above two mentioned ones. |

Table 309: Fields on the Create ICAP Redirect Server Page

| Field | Action |
|------------|---|
| Name | Enter an ICAP Redirect server name. The string must contain alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed; maximum length is 63 characters. |
| Host Type* | Select Name or IP address. |

Table 309: Fields on the Create ICAP Redirect Server Page (Continued)

| Field | Action |
|------------------------|--|
| Host | Enter the host name or host IP address depending on what host type you choose. |
| 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 1025 through 65534. |
| Sockets | Specifies the number of connections to be created. Enter the number of connections. The range is 1 through 64. |
| Authentication | |
| Authorization Type | Specifies the type of authentication. |
| Credentials Type | Select the credential type as ASCII or Base64. Based on the Credential Type that you choose, enter the ASCII string or Base64 string. |
| URL | |
| Request MOD | Enter the reqmod uri that can be configured for ICAP server only. |
| Response MOD | Enter the respmod uri that can be configured for ICAP server only. |
| Routing Instance | Specifies the virtual router that is used for launching. Select a routing instance from the list. |
| SSL Initiation Profile | Select an SSL initiation profile from the list. |

RELATED DOCUMENTATION

[About the ICAP Redirect Profile Page | 1120](#)

[Edit an ICAP Redirect Profile | 1125](#)

[Delete ICAP Redirect Profile | 1125](#)

Edit an ICAP Redirect Profile

You are here: **Security Services** > **ICAP Redirect**.

To edit an ICAP redirect profile:

1. Select the existing ICAP redirect profile that you want to edit on the ICAP Redirect page.
2. Click the pencil icon available on the upper-right corner of the page.

The Edit ICAP Redirect Profile page appears with editable fields. For more information on the options, see "[Add an ICAP Redirect Profile](#)" on page 1122 .

3. Click **OK** to save the changes.

RELATED DOCUMENTATION

[About the ICAP Redirect Profile Page | 1120](#)

[Delete ICAP Redirect Profile | 1125](#)

Delete ICAP Redirect Profile

You are here: **Security Services** > **ICAP Redirect**.

To delete ICAP redirect profile:

1. Select one or more ICAP redirect profile that you want to delete on the ICAP Redirect page.
2. Click the delete icon available on the upper-right corner of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the ICAP Redirect Profile Page | 1120](#)

[Add an ICAP Redirect Profile | 1122](#)

[Edit an ICAP Redirect Profile | 1125](#)