

J-Web User Guide for SRX Series Devices

Published
2020-11-13

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 Devices

Copyright © 2020 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 the Documentation | xxxi

Documentation and Release Notes | xxxi

Documentation Conventions | xxxi

Documentation Feedback | xxxiv

Requesting Technical Support | xxxiv

Self-Help Online Tools and Resources | xxxv

Creating a Service Request with JTAC | xxxv

1

Juniper Web Device Manager

Getting Started | 2

Juniper Web Device Manager Overview | 2

What is J-Web? | 2

Benefits of J-Web | 2

Start J-Web | 3

Prerequisites for Using J-Web | 3

Log On to J-Web | 4

Configure SRX Devices Using the J-Web Setup Wizard | 5

J-Web First Look | 26

Explore J-Web | 27

J-Web Launch Pad | 27

J-Web Top Pane | 28

J-Web Side Pane | 30

J-Web Main Pane | 33

J-Web Workflow Wizards | 36

Summary | 36

2

Dashboard

J-Web Dashboard | 38

Dashboard Overview | 38

What is J-Web Dashboard | 38

Chassis View | 39

Work with Widgets | 40

Monitor

Interfaces | 47

Monitor Ports | 47

Monitor PPPoE | 49

Access | 53

Monitor Address Pools | 53

Multi Tenancy | 55

Monitor Logical Systems | 55

Monitor Tenants | 58

Alarms | 62

Monitor Alarms | 62

Monitor Policy Log | 63

Events | 65

Monitor All Events | 65

Monitor Firewall Events | 70

Monitor Web Filtering Events | 75

Monitor IPsec VPNs Events | 79

Monitor Content Filtering Profiles Events | 83

Monitor Antispam Events | 87

Monitor Antivirus Events | 91

Monitor IPS Events | 95

Monitor Screen Events | 99

Monitor Security Intelligence Events | 101

Monitor ATP Events | 103

Monitor System Events | 105

Users | 108

Monitor Users | 108

Device | 110

Monitor Chassis Information | 110

Monitor Cluster Status | 112

Monitor Cluster Statistics | 113

Monitor Ethernet Switching | 115

Monitor Voice ALGs—Summary | 117

Monitor Voice ALGs—H323 | 118

Monitor Voice ALGs—MGCP | 120

Monitor Voice ALGs—SCCP | 123

Monitor Voice ALGs—SIP | 125

Monitor DS-Lite | 129

Routing | 131

Monitor Route Information | 131

Monitor RIP Information | 134

Monitor OSPF Information | 135

Monitor BGP Information | 138

Class of Service (CoS) | 140

Monitor CoS Interfaces | 140

Monitor Classifiers | 141

Monitor CoS Value Aliases | 142

Monitor RED Drop Profiles | 142

Monitor Forwarding Classes | 143

Monitor Rewrite Rules | 144

Monitor Scheduler Maps | 145

MPLS | 148

Monitor MPLS Interfaces | 148

Monitor LSP Information | 149

Monitor LSP Statistics | 150

Monitor RSVP Sessions | 151

Monitor RSVP Interfaces | 153

DHCP | 154

Monitor DHCP Server | 154

Monitor DHCP Relay | 156

NAT | 158

Monitor Source NAT | 158

Monitor Destination NAT | 164

Monitor Static NAT | 166

Monitor Interface NAT Ports | 168

Authentication | 170

Monitor Firewall Authentication | 170

Monitor Local Authentication | 171

Monitor UAC Authentication | 172

Security Services | 174

Monitor Policy Activities | 174

Monitor Shadow Policies | 177

Monitor Screen Counters | 180

Monitor UTM—Antivirus | 181

Monitor UTM—Web Filtering | 183

Monitor UTM—Antispam | 184

Monitor UTM—Content Filtering Profiles | 185

Monitor ICAP Redirect | 186

Monitor IPS Attacks | 187

Monitor IPS Status | 189

Monitor Application Firewalls | 190

Monitor Applications | 192

Monitor Application Tracking | 193

Monitor AppQoS | 196

Monitor Advanced Threat Prevention—Statistics | 198

VPN | 200

Monitor VPN—Phase I | 200

Monitor VPN—Phase II | 201

Flow Session | 204

Monitor Flow Session | 204

Flow Gate | 207

Monitor Flow Gate | 207

VLAN | 209

Monitor VLAN | 209

Wireless LAN | 211

Monitor Wireless LAN | 211

Threats Map (Live) | 215

Monitor Threats Map (Live) | 215

Field Descriptions | 216

Threat Types | 217

Tasks You Can Perform | 218

4**Device Administration****Basic Settings | 223**

Configure Basic Settings | 223

Setup | 238

Configure Setup Wizard | 238

Configure Cluster (HA) Mode | 262

Cluster Management | 275

About the Cluster Configuration Page | 275

Tasks You Can Perform | 275

Field Descriptions | 276

Edit Node Settings | 277

Add an HA Cluster Interface | 278

Edit an HA Cluster Interface | 280

Delete HA Cluster Interface | 280

Add a Redundancy Group | 281

Edit a Redundancy Group | 283

Delete Redundancy Group | 283

User Management | 284

About the User Management Page | 284

Tasks You Can Perform | 284

Field Descriptions | 284

Add a User | 287

Edit a User | 289

Delete User | 289

Certificate Management—Device Certificates | 290

About the Device Certificates Page | 290

Import a Device Certificate | 291

Export a Device Certificate | 293

Add a Device Certificate | 294

Delete Device Certificate | 296

View Details of a Device Certificate | 297

Search Text in the Device Certificates Table | 300

Certificate Management—Trusted Certificate Authority | 302

About the Trusted Certificate Authority Page | 302

Generate Default Trusted Certificate Authorities | 303

Enroll a CA Certificate | 304

Import a CA Certificate | 305

Add a Certificate Authority Profile | 306

Edit a Certificate Authority Profile | 310

Delete Certificate Authority Profile | 310

Search Text in the Trusted Certificate Authority Table | 311

Certificate Management—Certificate Authority Group | 313

About the Certificate Authority Group Page | 313

Import a Trusted CA Group | 314

Add a CA Group | 315

Edit a CA Group | 316

Delete CA Group | 317

Search Text in the Certificate Authority Group Table | 317

Multi Tenancy—Resource Profiles | 319

About the Resource Profiles Page | 319

Tasks You Can Perform | 319

Field Descriptions | 320

Global Settings | 321

Add a Resource Profile | 322

Edit a Resource Profile | 325

Delete Resource Profile | 325

Multi Tenancy—Interconnecting Ports | 327

About the Interconnecting Ports Page | 327

Tasks You Can Perform | 327

Field Descriptions | 328

Add a LT Logical Interface | 329

Edit a LT Logical Interface | 335

Delete Logical Interface | 335

Search for Text in an Interconnect Ports Table | 336

Multi Tenancy—Logical Systems | 337

About the Logical Systems Page | 337

Tasks You Can Perform | 337

Field Descriptions | 338

Add a Logical System | 339

Edit a Logical System | 349

Delete Logical System | 349

Search Text in Logical Systems Table | 350

Multi Tenancy—Tenants | 351

About the Tenants Page | 351

Tasks You Can Perform | 351

Field Descriptions | 352

Add a Tenant | 353

Edit a Tenant | 360

Delete Tenant | 360

Search Text in Tenants Table | 361

License Management | 362

Manage Your Licenses | 362

About License Management Page | 362

Add License | 363

Delete Installed Licenses | 364

Update Installed Licenses | 364

Update Trial Licenses | 364

Display License Keys | 364

Download License Keys | 364

Software Feature Licenses | 365

ATP Management | 367

Enroll Your Device with Juniper ATP Cloud | 367

About the Diagnostics Page | 370

Operations | 372

Maintain Files | 372

About Files Page | 372

Clean Up Files | 372

Download and Delete Files | 373

Delete Backup JUNOS Package | 374

Maintain Reboot Schedule | 375

Maintain System Snapshots | 377

Software Management | 379

Upload Software Packages | 379

Install Software Packages | 380

Rollback Software Package Version | 381

Configuration Management | 382

Manage Upload Configuration Files | 382

Manage Configuration History | 383

Manage Rescue Configuration | 385

Alarm Management | 386

Monitor Chassis Alarm | 386

 About Chassis Alarm Page | 386

 Create Chassis Alarm Definition | 386

 Edit Chassis Alarm Definition | 390

Monitor System Alarm | 391

 About System Alarm Page | 391

 Create System Alarm Configuration | 391

 Edit System Alarm Configuration | 394

RPM | 395

Setup RPM | 395

View RPM | 402

Tools | 407

Troubleshoot Ping Host | 407

 About Ping Host Page | 407

Troubleshoot Ping MPLS | 410

 About Ping MPLS Page | 411

Troubleshoot Traceroute | 415

 About Traceroute Page | 415

Troubleshoot Packet Capture | 418

 About Packet Capture Page | 418

Access CLI | 424

 About CLI Terminal Page | 424

 CLI Terminal Requirements | 424

 CLI Overview | 424

View CLI Configuration | 425

 About CLI Viewer Page | 426

Edit CLI Configuration | 427

 About CLI Editor Page | 427

Point and Click CLI | 428

 About Point and Click CLI Page | 428

Network

Connectivity—Ports | 435

About the Ports Page | 435

 Tasks You Can Perform | 435

 Field Descriptions | 435

Add a Logical Interface | 438

Edit a Logical Interface | 444

Delete Logical Interface | 445

Connectivity—VLAN | 446

About the VLAN Page | 446

 Tasks You Can Perform | 446

 Field Descriptions | 447

Add a VLAN | 447

Edit a VLAN | 449

Delete VLAN | 450

Assign an Interface to VLAN | 450

Connectivity—Link Aggregation | 452

About the Link Aggregation Page | 452

 Tasks You Can Perform | 452

 Field Descriptions | 453

Link Aggregation Global Settings | 453

Add a Logical Interface to Link Aggregation | 454

Add a Link Aggregation | 456

Edit an Aggregated Interface | 457

Delete Link Aggregation | 458

Search for Text in the Link Aggregation Table | 458

Connectivity—PPPoE | 459

Configure PPPoE | 459

Connectivity—Wireless LAN | 461

About the Settings Page | 461

Tasks You Can Perform | 461

Field Descriptions | 462

Create an Access Point | 462

Edit an Access Point | 463

Delete Access Point | 464

Create an Access Point Radio Settings | 465

Edit an Access Point Radio Settings | 467

Delete Access Point Radio Settings | 468

DHCP Client | 469

About the DHCP Client Page | 469

Tasks You Can Perform | 469

Field Descriptions | 469

Add DHCP Client Information | 470

Delete DHCP Client Information | 471

DHCP Server | 473

About the DHCP Server Page | 473

Tasks You Can Perform | 473

Field Descriptions | 474

Add a DHCP Pool | 475

Edit a DHCP Pool | 478

Delete DHCP Pool | 479

DHCP Groups Global Settings | 479

Add a DHCP Group | 480

Edit a DHCP Group | 480

Delete DHCP Group | 481

Firewall Filters—IPv4 | 482

About the IPv4 Page | 482

Tasks You Can Perform | 482

Field Descriptions | 482

Add IPv4 Firewall Filters | 483

Firewall Filters—IPv6 | 497

About the IPv6 Page | 497

Tasks You Can Perform | 497

Field Descriptions | 497

Add IPv6 Firewall Filters | 498

Firewall Filters—Assign to Interfaces | 509

About the Assign to Interfaces Page | 509

Field Descriptions | 509

Source NAT | 511

About the Source Page | 511

Tasks You Can Perform | 511

Field Descriptions | 512

Global Settings | 514

Add a Source Rule Set | 515

Edit a Source Rule Set | 518

Delete Source Rule Set | 519

Add a Source NAT Pool | 519

Edit a Source NAT Pool | 521

Delete Source NAT Pool | 521

Destination NAT | 523

About the Destination Page | 523

Tasks You Can Perform | 523

Field Descriptions | 524

Add a Destination Rule Set | 525

Edit a Destination Rule Set | 528

Delete Destination Rule Set | 528

Add a Destination NAT Pool | 529

Edit a Destination NAT Pool | 531

Delete Destination NAT Pool | 532

Static NAT | 533

About the Static Page | 533

Tasks You Can Perform | 533

Field Descriptions | 534

Add a Static Rule Set | 535

Edit a Static Rule Set | 538

Delete Static Rule Set | 539

NAT Proxy ARP/ND | 540

About the Proxy ARP/ND Page | 540

Tasks You Can Perform | 540

Field Descriptions | 541

Add a Proxy ARP | 541

Edit a Proxy ARP | 542

Delete a Proxy ARP | 543

Add a Proxy ND | 544

Edit a Proxy ND | 545

Delete Proxy ND | 545

Static Routing | 547

About the Static Routing Page | 547

Tasks You Can Perform | 547

Field Descriptions | 547

Add a Static Route | 548

Edit a Static Route | 549

Delete Static Route | 550

RIP Routing | 551

About the RIP Page | 551

Tasks You Can Perform | 551

Field Descriptions | 551

Add a RIP Instance | 552

Edit a RIP Instance | 554

Delete RIP Instance | 555

Edit RIP Global Settings | 555

Delete RIP Global Settings | 558

OSPF Routing | 559

About the OSPF Page | 559

Tasks You Can Perform | 559

Field Descriptions | 560

Add an OSPF | 561

Edit an OSPF | 568

Delete OSPF | 569

BGP Routing | 570

About the BGP Page | 570

Tasks You Can Perform | 570

Field Descriptions | 570

Add a BGP Group | 572

Edit a BGP Group | 577

Delete a BGP Group | 578

Edit Global Information | 578

Routing Instances | 583

About the Routing Instances Page | 583

Tasks You Can Perform | 583

Field Descriptions | 584

Add a Routing Instance | 584

Edit a Routing Instance | 585

Delete Routing Instance | 586

Routing—Policies | 587

About the Policies Page | 587

Tasks You Can Perform | 587

Field Descriptions | 588

Global Options | 588

Add a Policy | 590

Clone a Policy | 598

Edit a Policy | 599

Delete Policy | 599

Test a Policy | 600

Routing—Forwarding Mode | 601

About the Forwarding Mode Page | 601

Field Descriptions | 601

CoS—Value Aliases | 603

About the Value Aliases Page | 603

Tasks You Can Perform | 603

Field Descriptions | 603

Add a Code Point Alias | 604

Edit a Code Point Alias | 605

Delete Code Point Alias | 605

CoS—Forwarding Classes | 607

About the Forwarding Classes Page | 607

Tasks You Can Perform | 607

Field Descriptions | 607

Add a Forwarding Class | 608

Edit a Forwarding Class | 609

Delete Forwarding Class | 609

CoS Classifiers | 610

About the Classifiers Page | 610

Tasks You Can Perform | 610

Field Descriptions | 610

Add a Classifier | 611

Edit a Classifier | 613

Delete Classifier | 613

CoS—Rewrite Rules | 615

About the Rewrite Rules Page | 615

Tasks You Can Perform | 615

Field Descriptions | 615

Add a Rewrite Rule | 616

Edit a Rewrite Rule | 618

Delete Rewrite Rule | 618

CoS—Schedulers | 619

About the Schedulers Page | 619

Tasks You Can Perform | 619

Field Descriptions | 619

Add a Scheduler | 620

Edit a Scheduler | 622

Delete Scheduler | 622

CoS—Scheduler Maps | 623

About the Scheduler Maps Page | 623

Tasks You Can Perform | 623

Field Descriptions | 623

Add a Scheduler Map | 624

Edit a Scheduler Map | 625

Delete Scheduler Map | 626

CoS—Drop Profile | 627

About the Drop Profile Page | 627

Tasks You Can Perform | 627

Field Descriptions | 627

Add a Drop Profile | 628

Edit a Drop Profile | 629

Delete Drop Profile | 630

CoS—Virtual Channel Groups | 631

About the Virtual Channel Groups Page | 631

Tasks You Can Perform | 631

Field Descriptions | 631

Add a Virtual Channel | 632

Edit a Virtual Channel | 633

Delete Virtual Channel | 634

CoS—Assign To Interface | 635

About the Assign To Interface Page | 635

Tasks You Can Perform | 635

Field Descriptions | 635

Edit a Port | 636

Add a Logical Interface | 637

Edit a Logical Interface | 639

Delete Logical Interface | 639

Application QoS | 641

About the Application QoS Page | **641**

Tasks You Can Perform | **641**

Field Descriptions | **642**

Add an Application QoS Profile | **643**

Edit an Application QoS Profile | **645**

Clone an Application QoS Profile | **646**

Delete Application QoS Profile | **646**

Add a Rate Limiter Profile | **647**

Edit a Rate Limiter Profile | **648**

Clone a Rate Limiter Profile | **649**

Delete Rate Limiter Profile | **649**

Security Policies and Objects

Security Policies | 652

About the Security Policies Page | **652**

Tasks You Can Perform | **652**

Field Descriptions | **655**

Global Options | **657**

Add a Rule | **659**

Clone a Rule | **671**

Edit a Rule | **671**

Delete Rules | **672**

Zones/Screens | 673

About the Zones/Screens Page | **673**

Tasks You Can Perform | **673**

Field Descriptions | **673**

Add a Zone | **674**

Edit a Zone | **677**

Delete Zone | **677**

Add a Screen | **678**

Edit a Screen | **686**

Delete Screen | **686**

Zone Addresses | 687

About the Zone Addresses Page | 687

Tasks You Can Perform | 687

Field Descriptions | 688

Add Zone Addresses | 689

Clone Zone Addresses | 690

Edit Zone Addresses | 691

Delete Zone Addresses | 691

Search Text in a Zone Addresses Table | 692

Global Addresses | 693

About the Global Addresses Page | 693

Tasks You Can Perform | 693

Field Descriptions | 693

Add an Address Book | 694

Edit an Address Book | 697

Delete Address Book | 697

Services | 698

About the Services Page | 698

Tasks You Can Perform | 698

Field Descriptions | 698

Add a Custom Application | 700

Edit a Custom Application | 702

Delete Custom Application | 703

Add an Application Group | 703

Edit an Application Group | 704

Delete Application Group | 705

Dynamic Applications | 706

About the Dynamic Applications Page | 706

Tasks You Can Perform | 707

Field Descriptions | 708

Global Settings | 709

Add Application Signatures | 711

Clone Application Signatures | 715

Add Application Signatures Group | 716

Edit Application Signatures | 717

Delete Application Signatures | 718

Search Text in an Application Signatures Table | 718

Application Tracking | 720

About the Application Tracking Page | 720

Field Description | 720

Schedules | 722

About the Schedules Page | 722

Tasks You Can Perform | 722

Field Descriptions | 723

Add a Schedule | 723

Clone a Schedule | 725

Edit a Schedule | 726

Delete Schedule | 726

Search Text in Schedules Table | 727

Proxy Profiles | 728

About the Proxy Profiles Page | 728

Tasks You Can Perform | 728

Field Descriptions | 729

Add a Proxy Profile | 729

Edit a Proxy Profile | 730

Delete Proxy Profile | 731

Security Services

UTM Default Configuration | 734

About the Default Configuration Page | 734

Tasks You Can Perform | 734

Field Descriptions | 735

Edit a Default Configuration | 735

Delete Default Configuration | 736

UTM Antivirus Profiles | 738

About the Antivirus Profiles Page | 738

Tasks You Can Perform | 738

Field Descriptions | 739

Add an Antivirus Profile | 740

Clone an Antivirus Profile | 744

Edit an Antivirus Profile | 745

Delete Antivirus Profile | 745

UTM Web Filtering Profiles | 747

About the Web Filtering Profiles Page | 747

Tasks You Can Perform | 747

Field Descriptions | 748

Add a Web Filtering Profile | 749

Clone a Web Filtering Profile | 755

Edit a Web Filtering Profile | 756

Delete Web Filtering Profile | 756

UTM Web Filtering Category Update | 758

About the Category Update Page | 758

Tasks You Can Perform | 758

Field Descriptions | 759

Category Update Settings | 760

Download and Install Settings | 763

UTM Antispam Profiles | 764

About the Antispam Profiles Page | 764

Tasks You Can Perform | 764

Field Descriptions | 765

Add an Antispam Profile | 766

Clone an Antispam Profile | 767

Edit an Antispam Profile | 768

Delete Antispam Profile | 768

UTM Content Filtering Profiles | 770

About the Content Filtering Profiles Page | 770

Tasks You Can Perform | 770

Field Descriptions | 771

Add a Content Filtering Profile | 772

Clone a Content Filtering Profile | 775

Edit a Content Filtering Profile | 776

Delete Content Filtering Profile | 776

UTM Custom Objects | 778

About the Custom Objects Page | 778

Tasks You Can Perform | 778

Field Descriptions | 779

Add a MIME Pattern List | 781

Add a File Extension List | 782

Add a Protocol Command List | 783

Add a URL Pattern List | 784

Add a URL Category List | 785

Add a Custom Message List | 787

Clone Custom Objects | 788

Edit Custom Objects | 789

Delete Custom Objects | 789

UTM Policies | 791

About the UTM Policies Page | 791

Tasks You Can Perform | 791

Field Descriptions | 792

Add a UTM Policy | 793

Clone a UTM Policy | 795

Edit a UTM Policy | 796

Delete UTM Policy | 797

IPS Signature Update | 798

About the Signature Update Page | 798

Tasks You Can Perform | 798

Field Descriptions | 798

Download an IPS Signature | 799

Install an IPS Signature | 800

Check Status of the IPS Signature | 801

IPS Signature Download Setting | 802

IPS Sensor | 804

About the Sensor Page | 804

Field Descriptions | 804

IPS Policy | 810

About the Policy Page | 810

Tasks You Can Perform | 810

Field Descriptions | 811

IDP Policy Template | 812

Check Status of the IDP Policy | 813

Add an IDP Policy | 813

Clone an IDP Policy | 816

Edit an IDP Policy | 817

Delete IDP Policy | 817

ALG | 819

About the ALG Page | 819

Field Descriptions | 819

Advanced Threat Prevention | 828

About the Advanced Threat Prevention Page | 828

Tasks You Can Perform | 828

Field Descriptions | 829

Add a Threat Prevention Policy | 830

Edit a Threat Prevention Policy | 831

Delete Threat Prevention Policy | 832

SSL Initiation Profiles | 833

About the SSL Initiation Profile Page | 833

Tasks You Can Perform | 833

Field Descriptions | 834

Add an SSL Initiation Profile | 835

Edit an SSL Initiation Profile | 837

Delete SSL Initiation Profile | 838

SSL Proxy Profiles | 839

About the SSL Proxy Page | 839

Tasks You Can Perform | 839

Field Descriptions | 840

Add an SSL Proxy Profile | 841

Clone an SSL Proxy Profile | 848

Edit an SSL Proxy Profile | 849

Delete SSL Proxy Profile | 849

Firewall Authentication—Access Profile | 851

About the Access Profile Page | 851

Tasks You Can Perform | 851

Field Descriptions | 852

Add an Access Profile | 853

Edit an Access Profile | 858

Delete an Access Profile | 858

Firewall Authentication—Address Pools | 860

About the Address Pools Page | 860

Tasks You Can Perform | 860

Field Descriptions | 861

Add an Address Pool | 861

Edit an Address Pool | 863

Delete Address Pool | 863

Search for Text in an Address Pools Table | 864

Firewall Authentication Settings | 865

About the Authentication Settings Page | 865

Field Description | 865

Firewall Authentication—UAC Settings | 868

About the UAC Settings Page | 868

Field Description | 868

Firewall Authentication—Active Directory | 871

About the Active Directory Page | 871

Firewall Authentication—Local Authentication | 876

About the Local Authentication Page | 876

Tasks You Can Perform | 876

Field Descriptions | 876

Add a Local Auth Entry | 877

Delete a Local Auth Entry | 878

Firewall Authentication—Authentication Priority | 879

About the Authentication Priority Page | 879

Firewall Authentication—Identity Management | 881

About the Identity Management Page | 881

Tasks You Can Perform | 881

Add an Identity Management Profile | 881

Edit an Identity Management Profile | 885

Delete Identity Management Profile | 886

ICAP Redirect | 887

About the ICAP Redirect Profile Page | 887

Tasks You Can Perform | 887

Field Descriptions | 888

Add an ICAP Redirect Profile | 889

Edit an ICAP Redirect Profile | 891

Delete ICAP Redirect Profile | 891

VPN

IPsec VPN | 894

About the IPsec VPN Page | 894

Tasks You Can Perform | 894

Field Descriptions | 895

IPsec VPN Global Settings | 896

Field Descriptions | 896

Create a Site-to-Site VPN | 899

Create a Remote Access VPN—Juniper Secure Connect | 914

Create a Remote Access VPN—NCP Exclusive Client | 929

Edit an IPsec VPN | 939

Delete an IPsec VPN | 940

Manual Key VPN | 942

About the Manual Key VPN Page | 942

Tasks You Can Perform | 942

Field Descriptions | 942

Add a Manual Key VPN | 943

Edit a Manual Key VPN | 945

Delete Manual Key VPN | 946

Dynamic VPN | 947

About the Dynamic VPN Page | 947

Tasks You Can Perform | 947

Field Descriptions | 948

Global Settings | 948

IPsec Template | 950

Add a Dynamic VPN | 951

Edit a Dynamic VPN | 953

Delete Dynamic VPN | 953

9

Reports

Reports | 956

About Reports Page | 956

Overview | 957

Generate Reports | 959

Threat Assessment Report | 961

Application and User Usage | 961

Top Talkers | 961

IPS Threat Environment | 962

Viruses Blocked | 962

URL Report | 962

Virus: Top Blocked | 963

Top Firewall Events | 963

Top Firewall Deny Destinations | 963

Top Firewall Service Deny | 963

Top Firewall Denies | 963

Top IPS Events | 963

Top Anti-spam Detected | 964

Top Screen Attackers | 964

Top Screen Victims | 964

Top Screen Hits | 964

Top Firewall Rules | 964

| | |
|--|-----|
| Top Firewall Deny Sources | 964 |
| Top IPS Attack Sources | 964 |
| Top IPS Attack Destinations | 964 |
| Top IPS Rules | 965 |
| Top Web Apps | 965 |
| Top Roles | 965 |
| Top Applications Blocked | 965 |
| Top URLs by User | 965 |
| Top Source Zone by Volume | 966 |
| Top Applications by User | 966 |
| Top Botnet Threats By Source Address via IDP Logs | 966 |
| Top Botnet Threats by Destination Address via IDP Logs | 966 |
| Top Botnet Threats by Threat Severity via IDP Logs | 966 |
| Top Malware Threats by Source Address via IDP Logs | 967 |
| Top Malware Threats by Destination Address via IDP Logs | 967 |
| Top Malware Threats by Threat Severity via IDP Logs | 967 |
| Top Blocked Applications via Webfilter Logs | 967 |
| Top Permitted Application Subcategories by Volume via Webfilter Logs | 967 |
| Top Permitted Application Subcategories by Count via Webfilter Logs | 968 |

About the Documentation

IN THIS SECTION

- Documentation and Release Notes | xxxi
- Documentation Conventions | xxxi
- Documentation Feedback | xxxiv
- Requesting Technical Support | xxxiv

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

Documentation and Release Notes

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

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

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

Documentation Conventions

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

Table 1: Notice Icons







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

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

Table 2: Text and Syntax Conventions

| Convention | Description | Examples |
|------------------------------|---|--|
| Bold text like this | Represents text that you type. | To enter configuration mode, type the configure command: user@host> configure |
| Fixed-width text like this | Represents output that appears on the terminal screen. | user@host> show chassis alarms No alarms currently active |
| <i>Italic text like this</i> | <ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. | <ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i> |

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

| Convention | Description | Examples |
|--------------------------------|--|--|
| <i>Italic text like this</i> | Represents variables (options for which you substitute a value) in commands or configuration statements. | Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i> |
| Text like this | Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components. | <ul style="list-style-type: none"> To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE. |
| < > (angle brackets) | Encloses optional keywords or variables. | stub <default-metric <i>metric</i> >; |
| (pipe symbol) | Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity. | broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>) |
| # (pound sign) | Indicates a comment specified on the same line as the configuration statement to which it applies. | rsvp { # Required for dynamic MPLS only |
| [] (square brackets) | Encloses a variable for which you can substitute one or more values. | community name members [<i>community-ids</i>] |
| Indentation and braces ({ }) | Identifies a level in the configuration hierarchy. | [edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } } |
| ; (semicolon) | Identifies a leaf statement at a configuration hierarchy level. | |

GUI Conventions

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

| Convention | Description | Examples |
|------------------------------|--|---|
| Bold text like this | Represents graphical user interface (GUI) items you click or select. | <ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel. |
| > (bold right angle bracket) | Separates levels in a hierarchy of menu selections. | In the configuration editor hierarchy, select Protocols>Ospf . |

Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

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



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

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are

covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net>

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

Creating a Service Request with JTAC

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

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

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

1

PART

Juniper Web Device Manager

[Getting Started](#) | 2

Getting Started

IN THIS CHAPTER

- [Juniper Web Device Manager Overview | 2](#)
- [Start J-Web | 3](#)
- [Explore J-Web | 27](#)

Juniper Web Device Manager Overview

IN THIS SECTION

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

What is J-Web?

Juniper Networks SRX Series Services Gateways 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. You can also use Hypertext Transfer Protocol (HTTP) to access J-Web.

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

[Start J-Web | 3](#)

[Explore J-Web | 27](#)

Start J-Web

IN THIS SECTION

- [Prerequisites for Using J-Web | 3](#)
- [Log On to J-Web | 4](#)
- [Configure SRX Devices Using the J-Web Setup Wizard | 5](#)
- [J-Web First Look | 26](#)

Prerequisites for Using J-Web

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

- Supported browsers—Mozilla Firefox, Google Chrome, and Microsoft Internet Explorer.

NOTE: By default, you establish a J-Web session through an HTTPS-enabled Web browser.

- Language support— English-version browsers.

Log On to J-Web

To log into the J-Web interface:

1. Connect the network port of your device to the Ethernet port on the management device (laptop or PC), using an RJ-45 cable.

NOTE: Following are the networks that you can use for your respective device:

- For SRX300 and SRX320 devices, use network ports numbered **0/1** through **0/6**.
- For SRX550M, use network ports numbered **0/1** through **0/5**.
- For other SRX devices, use the management port labelled **MGMT**.

2. Ensure that the management device acquires an IP address from the device.

NOTE: The services gateway functions as a DHCP server and will assign an IP address to the management device. This is applicable only for SRX300 line of devices and SRX550M devices. If an IP address is not assigned to the management device, manually configure an IP address.

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

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

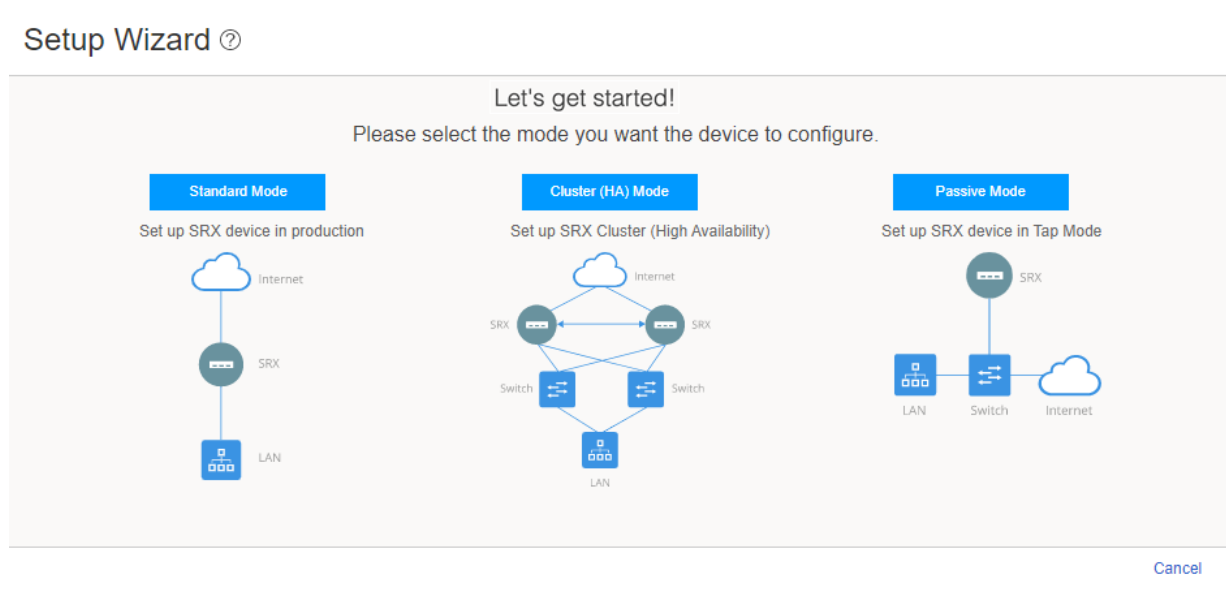
NOTE: The J-Web browser tab title displays the device model and hostname. These details are also displayed when you hover over the J-Web browser tab.

For example, when you access J-Web for an SRX320 device with a host name *srx320-xyz*, the J-Web browser tab displays the title as *J-Web (srx320 - srx320-xyz)*.

If the hostname isn't configured, the J-Web browser tab title displays the host URL or IP address; for example, *J-Web (srx320 - <device IP address>)*.

The J-Web Setup Wizard page opens. See [Figure 1 on page 5](#).

Figure 1: Setup Wizard Page



Configure SRX Devices 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.

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

- **Standard mode**—Configure your SRX Series device to operate in a standard mode. In this mode, you can configure basic settings such as device and users, time and DNS Servers, also management interface, zones and interfaces, and security policies.
- **Cluster (HA) mode**—Configure your SRX Series device 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 Standard or Passive mode when your device is in the HA mode.

- **Passive mode**—Configure your SRX Series device to operate in a TAP mode. TAP mode allows you to passively monitor traffic flows across a network. If IDP 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 devices does not support the passive mode configuration.

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 Devices using the J-Web Setup wizard:

1. Click on the configuration mode that you want to setup.

The Setup Wizard page appears.

NOTE:

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

- a. Click **Skip**.

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. We recommend that you do NOT use the root account to manage your SRX device as a best practice. You can add user accounts below in user management section.

Username: root

Password* ⓘ

Confirm Password*

Cancel OK

- b. Enter the root password and reenter it to confirm.

- 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 > Setup through the J-Web menu to configure the SRX device.

2. For standard mode and passive mode, complete the configuration according to the guidelines provided in [Table 3 on page 8](#).

NOTE:

- If you select Cluster (HA) Mode, for the configuration information see [“Configure Cluster \(HA\) Mode” on page 262](#).
- In the Setup wizard, root password is mandatory and all the other options are optional. In the passive mode, management interface, TAP interface, and services are mandatory.

3. Click **Finish**.

A successful message appears, and the device configuration mode of your choice is set up.

NOTE:

- Once the configuration is complete, the entire configuration is committed to the device and a successful message appears. If the commit fails, the CLI displays an error message and you remain at the wizard's last page. If required, you can change the configuration until the commit is successful.
- If the connectivity is lost during commit or if commit takes more than a minute, a message will be displayed with configured IP address to access J-Web again.
- For SRX300 line of devices and SRX550M devices, an additional message will be displayed about the device reboot if you have enabled Juniper Sky ATP or Security Intelligence services. For other SRX devices, the device will not reboot.

Table 3: Setup Wizard Configuration

| Field | Action |
|---------------------------|--|
| Device & Users | |
| System Identity | |
| Hostname | <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> |
| Allow root user SSH login | Enable this option to allow the root login (to the device) using SSH. |
| Device Password | |

Table 3: Setup Wizard Configuration (continued)

| Field | Action |
|-------------------------------|--|
| 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> |
| Confirm Password | Reenter the password. |
| User Management | <p>You can create additional user accounts in addition to root user account.</p> <p>NOTE: We recommend that you do not use root user account as a best practice to manage your devices.</p> <p>To add additional user accounts and to assign them a role:</p> <ol style="list-style-type: none"> 1. Click +. 2. Enter the details in the following fields: <ul style="list-style-type: none"> • Username—Enter a username. Do not use space or symbols. • Password—Enter a password. You can use alphanumeric characters and special characters; the minimum length is six characters. • Confirm Password—Reenter the password. • Role—Select a role from the list. Available options are: Super User, Operator, Read-Only, and Unauthorized. 3. Click the tick mark. <p>You can edit the user details using the pencil icon or select the existing user and delete it using the delete icon.</p> |
| Time & DNS Servers | |
| Set Date & Time | |
| Set system time | Select either NTP server or Manual to configure the system time. |

Table 3: Setup Wizard Configuration (*continued*)

| Field | Action |
|---|--|
| Date and Time | Select the date and time (in DD-MM-YYYY and HH:MM:SS 24-hour or AM/PM formats) to configure the system time manually. |
| NTP Server | <p>Enter a hostname or IP address of the NTP server.</p> <p>Once the system is connected to the network, the system time is synced with the NTP server time.</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> |
| Time zone | Select an option from the list. By default, device current time (UTC) is selected. |
| DNS Servers | |
| DNS Server 1 | <p>By default, 8.8.8.8 is displayed.</p> <p>NOTE: Entering a new IP address for the DNS server will remove the default IP address.</p> |
| DNS Server 2 | <p>Enter an IP address for the DNS server. By default, 8.8.4.4 is displayed.</p> <p>NOTE: Entering a new IP address for the DNS server will remove the default IP address.</p> |
| Management Interface | |
| Management Interface | |
| <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 Port | <p>Select an option 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 TAP mode, it is mandatory to configure a management port. J-Web needs a management port for viewing generated report. |

IPv4

NOTE: Click **Email it to self** to get the newly configured IPv4 address to your inbox. This is useful if you lose connectivity when you change the management IP address to another network.

| | |
|--------------------------|---|
| 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 | Enter a subnet mask for the IPv4 address. |
| Static Route | Enter an IPv4 address for the static route to route to the other network devices. |
| Static Route Subnet Mask | Enter a subnet mask for the static route IPv4 address. |
| 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 to route to the other network devices. |

Table 3: Setup Wizard Configuration (*continued*)

| Field | Action |
|----------------------------|---|
| 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 not available if the management port is fxp0. If the management port is not fxp0, a new dedicated functional management zone is created and the configures access protocols are added to the zone.
- In the Setup wizard, you cannot add any additional protocols.

| | |
|---------|---|
| HTTPS | Select this option for the web management using HTTP secured by SSL. NOTE: By default, this option is selected. |
| SSH | Select this option for the SSH service. NOTE: By default, this option is selected. |
| Ping | Select this option for the internet control message protocol. NOTE: By default, this option is selected. |
| DHCP | Select this option for the Dynamic Host Configuration Protocol. |
| Netconf | Select this option for the NETCONF Service. |

Zones & Interfaces—For Standard Mode

Zones & Interfaces

| | |
|-------------|--|
| Zone Name | View the zone name populated from your device factory default settings. NOTE: For Standard mode, trust and untrust zones are created by default even if these zones are not available in the factory default settings. |
| Interfaces | View the interfaces name populated from your device factory default settings. |
| Description | Enter the description for zone and interfaces. |

Table 3: Setup Wizard Configuration (*continued*)

| Field | Action |
|--|---|
| Edit | <p>Select a zone and click the pencil icon at the right corner of the table to modify the configuration.</p> <p>For more information on editing zones, see Table 4 on page 17 and Table 5 on page 22.</p> |
| Search | Click the search icon at the right corner of the table to quickly locate a zone or an interface. |
| Detailed View | <p>Hover over the zone name and click the Detailed View icon to view the zone and interface details.</p> <p>You can also click More and select Detailed View for the selected zone.</p> |
| Zones & Interfaces—For Passive Mode | |
| TAP Interface | |
| Physical Interface | <p>Select an interface from the list.</p> <p>For Passive mode, untrust zone will be displayed.</p> |
| Internet Connectivity | |
| <p>NOTE: Your device must have internet connectivity to use IPS, AppSec, Web filtering, Juniper Sky ATP, and Security threat intelligence services.</p> | |
| Name | <p>View the zone name populated from your device factory default settings.</p> <p>NOTE: For Passive mode, untrust zone is created by default.</p> |
| Interfaces | View the interfaces name populated from your device factory default settings. |
| Description | Enter the description for zone and interfaces. |
| Edit | <p>Select a zone and click the pencil icon at the right corner of the table to modify the configuration.</p> <p>For more information on editing zones, see Table 4 on page 17 and Table 5 on page 22.</p> |

Table 3: Setup Wizard Configuration (continued)

| Field | Action |
|--------------------------|---|
| Search | Click the search icon at the right corner of the table to quickly locate a zone or an interface. |
| Detailed View | <p>Hover over the zone name and click the Detailed View icon to view the zone and interface details.</p> <p>You can also click More and select Detailed View for the selected zone.</p> |
| Default Gateway | |
| Default Gateway (IPv4) | Enter the IPv4 address of the default gateway. |
| Default Gateway (IPv6) | Enter the IPv6 address of the default gateway. |
| Security Policies | |
| Reporting | |
| On-Box Reporting | <p>Enable this option to generate on-box reports.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • We recommend you use Stream mode logging to syslog server. • This option is supported only for the TAP mode. |
| Services | |
| UTM | Enable this option for configuring UTM services. |
| License | <p>Enter UTM 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 UTM services, your device must have internet connectivity from a revenue interface. |
| UTM Type | <p>Select an option to configure UTM features:</p> <ul style="list-style-type: none"> • Web Filtering • Antivirus • Antispam |

Table 3: Setup Wizard Configuration (*continued*)

| Field | Action |
|-----------------------|---|
| 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 | <p>Enable this option to install the IPS signatures.</p> <ul style="list-style-type: none"> IPS Policy—Displays the IPS policy wizard name. License—Enter the license key and click Install License to add a new license. <p>NOTE: The installation process may take few minutes.</p> <ul style="list-style-type: none"> IPS Signature—Click Browse to navigate to the IPS signature package folder and select it. Click Install to install the selected IPS signature package. <p>NOTE: You can download the IPS signature offline package at https://support.juniper.net/support/downloads/.</p> |
| Sky ATP | <p>Enable this option to use Juniper Sky ATP services.</p> <p>NOTE: After the Juniper Sky ATP configuration is pushed, only the SRX300 line of devices and SRX550M devices are rebooted. Your device must have internet connectivity to enable Juniper Sky ATP enrollment process through J-Web.</p> |
| 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 Sky ATP enrollment process through J-Web.</p> |
| User Firewall | <p>Enable this option to use user firewall services.</p> <ul style="list-style-type: none"> 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 3: Setup Wizard Configuration (*continued*)

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

Inspect Pass-through Tunnel

NOTE: This option is supported only for the TAP mode.

| | |
|-------|--|
| IP-IP | Enable this option for the SRX Series device to inspect pass through traffic over an IP-IP tunnel. |
| GRE | Enable this option for the SRX Series device to inspect pass through traffic over a GRE tunnel. |

Security Policy

NOTE: The table lists the security policy along with the selected advanced security settings.

| | |
|---------------------|--|
| Policy Name | Name of the policy. NOTE: <ul style="list-style-type: none"> If you are in Standard mode, trust-to-untrust policy is created by default. If you are in TAP mode, tap-policy is created by default. |
| From Zone | Name of the source zone. NOTE: <ul style="list-style-type: none"> If you are in Standard mode, permits all traffic from the trust zone. If you are in TAP mode, permits all traffic from the tap zone. |
| To Zone | Name of the destination zone. <ul style="list-style-type: none"> If you are in Standard mode, permits all traffic from the trust zone to the untrust zone. If you are in TAP mode, permits all traffic from the TAP zone to the TAP zone. |
| Source Address | Name of the source address (not the IP address) of a policy. |
| Destination Address | 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. |

Table 3: Setup Wizard Configuration (*continued*)

| Field | Action |
|-------------------|--|
| Advanced Security | Name of the configured advanced security settings. |

Table 4: Edit Trust Zone

| Field | Action |
|----------------------------|--|
| General Information | |
| Name | Displays the zone name. |
| Description | Enter the description for the zone. |
| Application Tracking | Enables this option to provide application tracking support to the zone. |
| Source Identity Log | Enables this option to trigger user identity logging when that zone is used as the source zone in a security policy. |
| Services | By default, this option is enabled. You can disable if required. all—Specifies all system services. |
| Protocols | By default, this option is enabled. You can disable if required. all—Specifies all protocol. |
| Interfaces | |
| Name | Displays the name of the interface |
| Description | Displays the description of the interface. |
| IP Address | Displays the IP address of the interface. |
| VLAN | Displays the VLAN name. |
| Services | Displays the system service option selected. |
| Protocols | Displays the protocol option selected. |

Table 4: Edit Trust Zone (continued)

| Field | Action |
|-------|---|
| Add | <p>To add a switching or a routing interface:</p> <ol style="list-style-type: none"> Click +. The Add Interface page appears. Enter the following details: <ul style="list-style-type: none"> General (fields for switching interface): <ul style="list-style-type: none"> Type (family)—Select Switching. NOTE: This option will be available for only SRX300 line of devices, SRX550M, and SRX1500 devices. For SRX5000 line of devices, SRX4100, SRX4200, SRX4600, and vSRX devices, the Type (family) field is not available. Routing Interface (IRB) Unit—Enter the IRB unit. Description—Enter the description for the interface. General (fields for routing interface): <ul style="list-style-type: none"> Type (family)—Select Routing. For SRX5000 line of devices, SRX4100, SRX4200, SRX4600, and vSRX devices, the Type (family) field is not available. Interface Name—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. |

Table 4: Edit Trust Zone (continued)

| Field | Action |
|-------|--|
| | <ul style="list-style-type: none"> • Interfaces—Select an interface from the Available column and move it to the Selected column. <p>NOTE: This option is available only for the Switching family type.</p> <ul style="list-style-type: none"> • IPv4: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • IPv6 Address—Enter a valid IPv6 address for the switching or the routing interface. • Subnet Prefix—Enter a subnet prefix for the IPv6 address. • VLAN Details: <p>NOTE: This option is available only for the Switching family type.</p> <ul style="list-style-type: none"> • VLAN Name—Enter a unique name for the VLAN. • VLAN ID—Enter the VLAN ID. • DHCP Local Server: <ul style="list-style-type: none"> • DHCP Local Server—Enable this option to configure the switch to function as an extended DHCP local server. • DHCP Pool Name—Enter the DHCP pool name. • DHCP Pool Range (Low)—Enter an IP address that is the lowest address in the IP address pool range. • DHCP Pool Range (High)—Enter an IP address that is the highest address in the IP address pool range. <p>NOTE: This address must be greater than the address specified in DHCP Pool Range (Low).</p> <ul style="list-style-type: none"> • Propagate Settings from—Select an interface on the router through which the resolved DHCP queries are propagated to the DHCP pool. |

Table 4: Edit Trust Zone (continued)

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

Table 4: Edit Trust Zone (continued)

| Field | Action |
|-------|--|
| | <ul style="list-style-type: none"> • 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. <p>• Protocols—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 4: Edit Trust Zone (continued)

| Field | Action |
|--------|--|
| Edit | <p>Select an interface and click the edit icon at the top right corner of the table.</p> <p>The Edit Interface page appears with editable fields.</p> <p>NOTE: As interface name is prepopulated, you cannot edit it.</p> |
| Delete | <p>Select an interface and click the delete icon at the top 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 | <p>Click the search icon at the top right corner of the table and enter partial text or full text of the keyword in the search bar.</p> <p>The search results are displayed.</p> |

Table 5: Edit Untrust Zone

| Field | Action |
|----------------------------|--|
| General Information | |
| Name | Displays the zone name as untrust. |
| Description | Enter the description for the zone. |
| Application Tracking | Enables this option to provide application tracking support to the zone. |
| Source Identity Log | Enables this option for system services. |
| Interfaces | |
| Name | Displays the name of the physical interface |
| Description | Displays the description of the interface. |
| Address Mode | Displays the type of address mode. |
| IP Address | Displays the IP address of the interface. |
| Services | Displays the system service option selected. |

Table 5: Edit Untrust Zone *(continued)*

| Field | Action |
|-----------|--|
| Protocols | Displays the protocol option selected. |

Table 5: Edit Untrust Zone *(continued)*

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

Table 5: Edit Untrust Zone (continued)

| Field | Action |
|-------|---|
| | <p>To add an interface to the untrust zone:</p> <ol style="list-style-type: none"> Click +. The Add Interface page appears. Enter the following details: <ul style="list-style-type: none"> General: <ul style="list-style-type: none"> Interface Name—Select an interface from the list. Interface Unit—By default 0 will be populated. You can change the unit value if required. 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 line of devices 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. <ul style="list-style-type: none"> IPv4 Address—Enter a valid IPv4 address for the interface. Subnet Mask—Enter a subnet mask for the IPv4 address. IPv6: NOTE: This option is available only for the Static IP address mode. <ul style="list-style-type: none"> IPv6 Address—Enter a valid IPv6 address for the interface. Subnet Prefix—Enter a subnet prefix for the IPv6 address. |

Table 5: Edit Untrust Zone (continued)

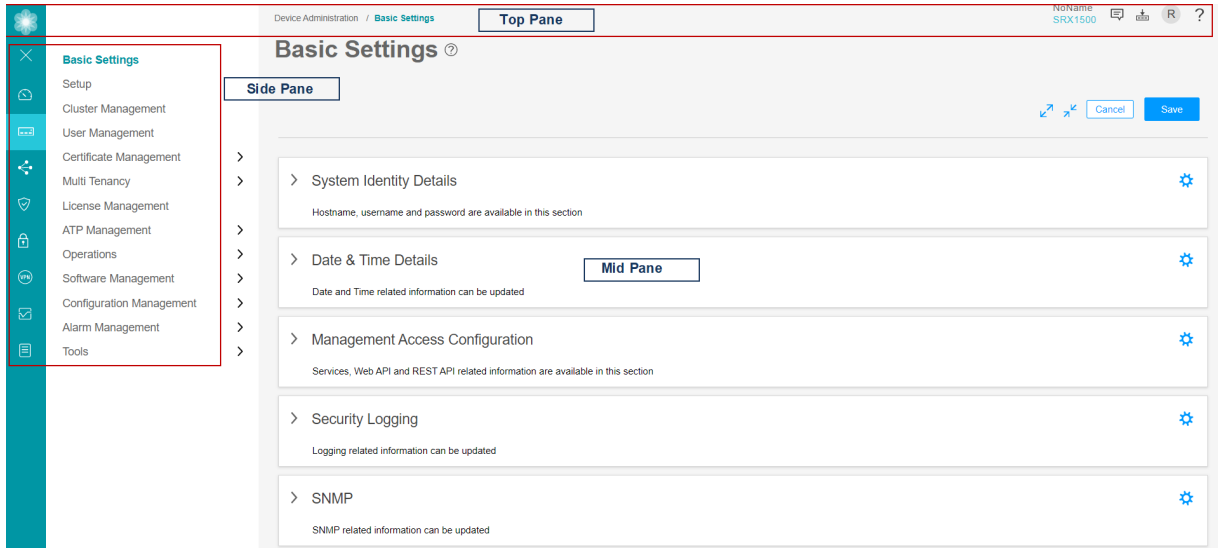
| Field | Action |
|--------|--|
| | <ul style="list-style-type: none"> • System Services—Select system services from the list in the Available column and then click the right arrow to move it to the Selected column. • Protocols—Select protocols from the list in the Available column and then click the right arrow to move it to the Selected column. |
| Edit | <p>Select an interface and click the edit icon at the top right corner of the table.</p> <p>The Edit Interface page appears with editable fields.</p> <p>NOTE: As interface name is prepopulated, you cannot edit it.</p> |
| Delete | <p>Select an interface and click the delete icon at the top 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 | <p>Click the search icon at the top right corner of the table and enter partial text or full text of the keyword in the search bar.</p> <p>The search results are displayed.</p> |

J-Web First Look

Each page of the J-Web interface is divided into the following panes (see [Figure 3 on page 27](#)):

- **Launch pad**—Displays high level details of the system identification, active users, and interface status.
- **Top pane**—Displays identifying information and links.
- **Side pane**—Displays subtasks of the Dashboard, Monitor, Device, Administration, Network, Security Policies and Objects, Security Services, VPN, and Reports task 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.

Figure 3: J-Web First Look



Explore J-Web

IN THIS SECTION

- J-Web Launch Pad | 27
- J-Web Top Pane | 28
- J-Web Side Pane | 30
- J-Web Main Pane | 33
- J-Web Workflow Wizards | 36
- Summary | 36

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 4 on page 28 shows the launch pad screen and its elements.

Figure 4: 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 29 provides the details of the J-Web top pane elements.

Table 6: J-Web Top Pane Elements

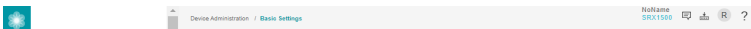





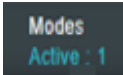

| Element | Description |
|--|--|
| <p>Banner</p>  | <p>Location—The gray bar at the top of the screen.</p> <p>You can access device details, feedback button, commit options, a profile management access menu, and a help button.</p> |
| <p>Device details</p>  | <p>Location—To the upper right of the banner.</p> <p>Provides details of the device you have accessed.</p> |
| <p>Feedback Button</p>  | <p>Location—To the right of the device details.</p> <p>You can provide feedback (jweb-feedback@juniper.net) if you are having an issue with the product.</p> |
| <p>Commit Configuration Menu</p>  | <p>Location—To the right of the Feedback button.</p> <p>Provides options to commit, compare, confirm, discard, or commit the changes in your preferred way.</p> |
| <p>User Functions Menu</p>  | <p>Location—To the right of the Commit Configuration menu.</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> |

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

| Element | Description |
|--|--|
| <div>Help Button</div> <div></div> | <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> |
| <div>Mode</div> <div></div> | <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> |
| <div>Tenant or Logical System User Name</div> <div></div> | <p>Location—To the left of the device details.</p> <p>Displays the name of the tenant user or logical system user when root user enters as a Tenant or a logical systems. Click on the username and select Exit to go back to the root user role.</p> |

J-Web Side Pane

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

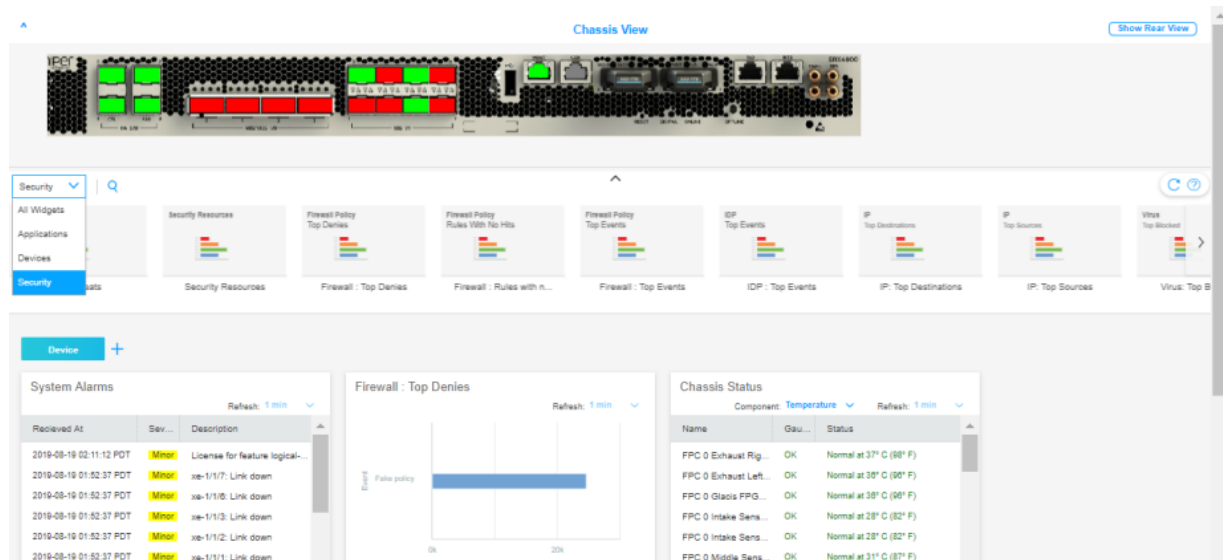
The following tabs across the side pane of the J-Web GUI provide workspaces in which an administrator can perform specific tasks:

- **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 5 on page 31 shows an example of the J-Web Dashboard tab.

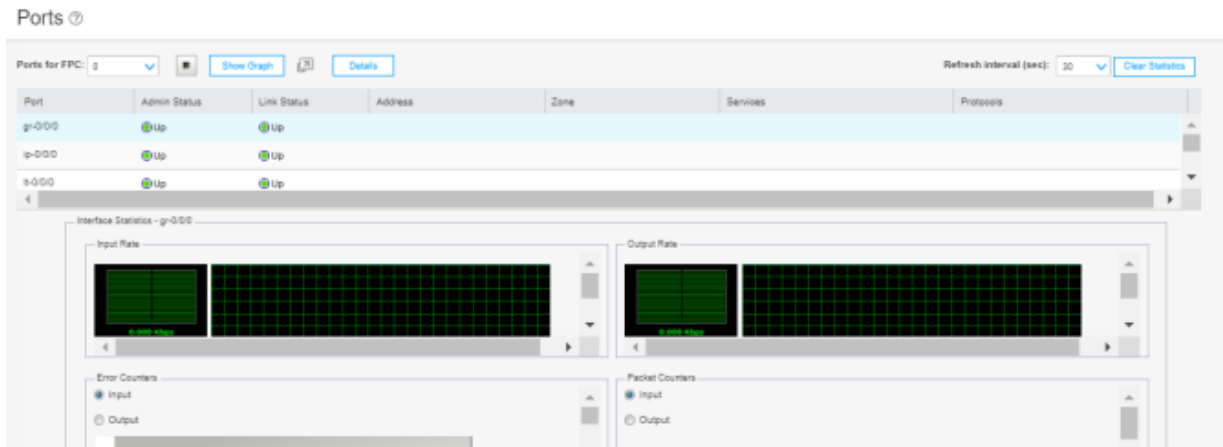
Figure 5: J-Web Dashboard Tab



- **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 6 on page 32 shows an example of the J-Web Monitor tab.

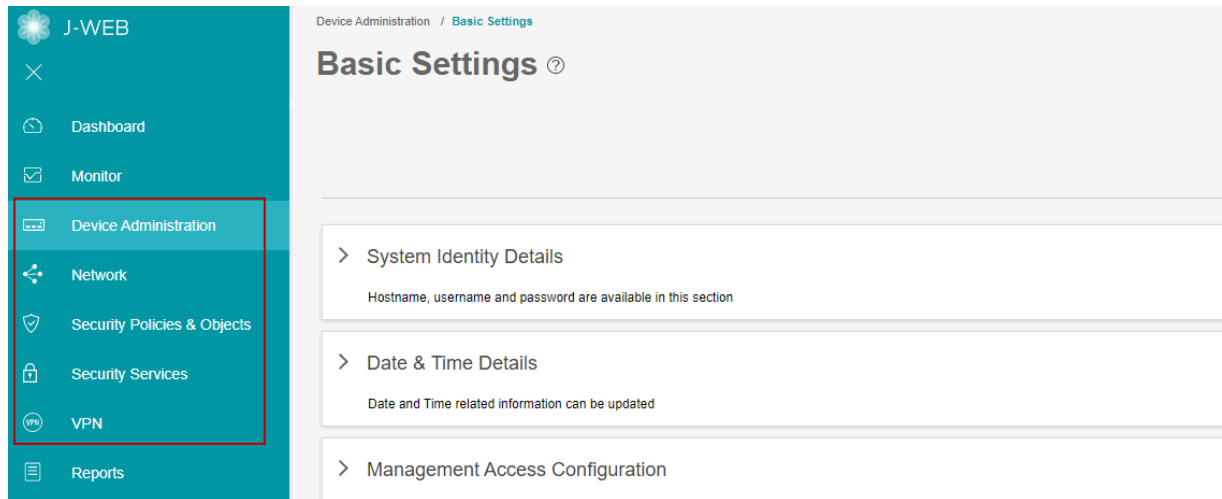
Figure 6: J-Web Monitor Tab



- **Configure**—The highlighted workspace in [Figure 7 on page 33](#) is where all of the SRX Series device configuration happens. Starting in Junos OS 20.3R1 Release, you can configure the following features for managing your network security:
 - **Device administration**—Such as basic settings, Setup wizard, operations, RPM, and tools. You can also manage cluster, user, certificates, licenses, ATP, software, configuration, and alarms.
 - **Network**—Such as connectivity, DHCP, firewall filters, NAT, routing, Class of Services (CoS), and Application QoS.
 - **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 UTM, IPS, ALG, ATP, SSL profiles, firewall authentication, and ICAP redirect.
 - **VPN**—Such as IPsec VPN, manual key VPN, and dynamic VPN.

[Figure 7 on page 33](#) shows an example of the J-Web configuration menus.

Figure 7: J-Web Configure Menus



- **Reports**—The Reports tab provides a workspace in which you can generate reports on demand. J-Web comes with a predefined set of reports. The generated report is displayed in HTML format. You can group multiple reports and generate a consolidated report.

Figure 8 on page 33 shows an example of the J-Web Reports tab.

Figure 8: J-Web Reports Tab

Reports

Reports ⓘ

Generate Report 🔍

| <input type="checkbox"/> | Name | Report Content | Type |
|--------------------------|--------------------------------|---|------|
| <input type="checkbox"/> | Threat Assessment Report | Executive Summary, Application Risk Assessment, Threat & Malware Assessment ⓘ | Log |
| <input type="checkbox"/> | Application and User Usage | Top High Risk Applications by Bandwidth, Top High Risk Applications By Count, Top Categories By Bandwidth ⓘ | Log |
| <input type="checkbox"/> | Top Talkers | Top Source IPs by Bandwidth, Top Destination IPs by Bandwidth, Top Source IPs by Session ⓘ | Log |
| <input type="checkbox"/> | IPS Threat Environment | IPS Attacks by Severity Over Time, Total IPS Attacks by Severity, Top IPS Categories Blocked ⓘ | Log |
| <input type="checkbox"/> | Viruses Blocked | Total Viruses Blocked Over Time, Top Viruses Blocked | Log |
| <input type="checkbox"/> | URL Report | Top URLs by Bandwidth, Top URLs by Count, Top URL Categories by Bandwidth ⓘ | Log |
| <input type="checkbox"/> | Virus: Top Blocked | Virus: Top Blocked | Log |
| <input type="checkbox"/> | Top Firewall Events | Top Firewall Events | Log |
| <input type="checkbox"/> | Top Firewall Deny Destinations | Top Firewall Deny Destinations | Log |
| <input type="checkbox"/> | Top Firewall Service Deny | Top Firewall Service Deny | Log |
| <input type="checkbox"/> | Top Firewall Denies | Top Firewall Denies | Log |

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 34 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





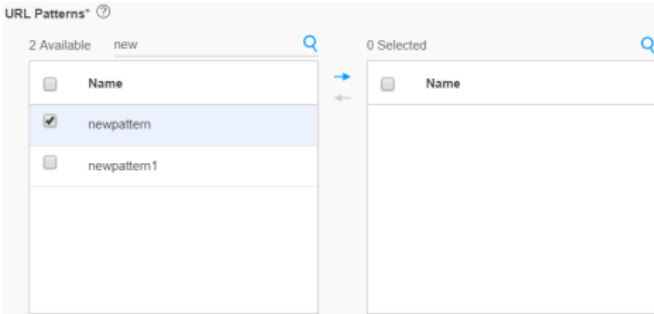

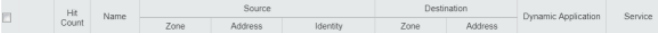





| Element | Description |
|---|---|
| <p>Breadcrumbs</p>  | <p>Location—Upper left part of main screen. Not visible on the Dashboard.</p> <p>Trace your location in the GUI. The breadcrumbs provide a path back to one of the five tabs: Dashboard, Monitor, Configure, Reports, and Administration.</p> |
|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

Table 7: J-Web Main Pane Elements (*continued*)

| Element | Description |
|--|---|
| <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> |
| <p>Filter</p>  | <p>Location—Upper right corner of tabular views.</p> <p>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.</p> |
| <p>Success message</p>  | <p>Location—At the top of the main pane.</p> <p>A message is displayed with this icon to state that your task is successful.</p> |
| <p>Information message</p>  | <p>Location—At the top of the main pane.</p> <p>A message is displayed with this icon to state you have some pending actions, but you can continue with the task.</p> |
| <p>Alert message</p>  | <p>Location—At the top of the main pane.</p> <p>A message is displayed with this icon to state you have some pending actions which you must complete to proceed with the required task.</p> |
| <p>Warning message</p>  | <p>Location—At the top of the main pane.</p> <p>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.</p> |

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 devices more easily.

Release History Table

| Release | Description |
|------------------------|---|
| 20.3R1 | Starting in Junos OS 20.3R1 Release, you can configure the following features for managing your network security: |

2

PART

Dashboard

J-Web Dashboard | 38

J-Web Dashboard

IN THIS CHAPTER

- [Dashboard Overview | 38](#)

Dashboard Overview

IN THIS SECTION

- [What is J-Web Dashboard | 38](#)
- [Chassis View | 39](#)
- [Work with Widgets | 40](#)

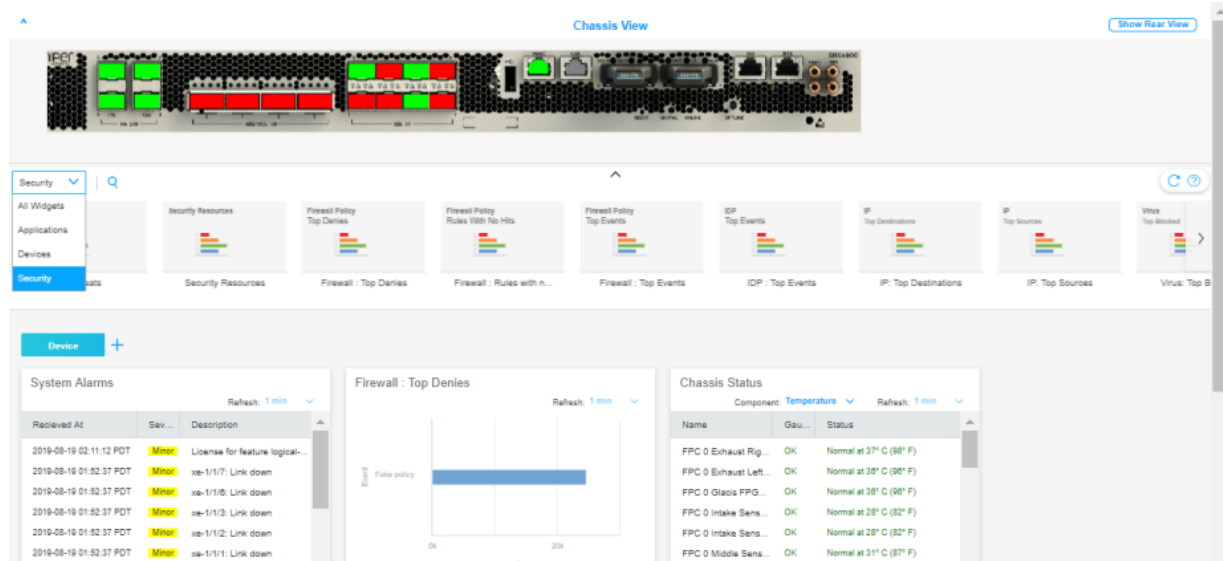
What is J-Web Dashboard

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

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

[Figure 9 on page 39](#) shows an example of the Dashboard page of SRX4600 Services Gateway.

Figure 9: SRX4600 Dashboard



Chassis View

You can view the image of the chassis and its component parts using the Dashboard. The ports reflect the most real-time status and are colored to indicate the port link status. For example, the ge port LED is green when the port is up and red when the port is down. Major or minor alarm indicators appear in red. When you insert or remove a card, the chassis view reflects the change immediately.

NOTE: To use the Chassis View, you must install a recent version of Adobe Flash that supports ActionScript and AJAX (Version 9).

Using the chassis view, you can:

- Mouse over a port to view the port name and help tips.
- Use the Show Front View and Show Rear View buttons at the top right corner to toggle between front and rear views of the chassis.
- Use the arrow button at the left top corner to hide or show the chassis view.
- Right-click on each of the component to view the chassis information, switch to front or back view of the chassis, and configure or monitor ports.
- Use the zoom option on the left side of the chassis to zoom in or out for SRX5000 line of devices.

NOTE:

- J-Web supports I/O card (IOC4) and Routing Engine (RE3) line cards for SRX5000 line of devices and Switch Control Board (SCB4) line cards for SRX5600 and SRX5800 devices.
- J-Web supports Wi-Fi Mini-Physical Interface Module (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.

Table 8 on page 40 summarizes the fields in Chassis View.

Table 8: Fields in Dashboard Chassis View

| Field | Description |
|-----------------|--|
| Chassis View | <ul style="list-style-type: none">• Provides a graphical representation of the hardware chassis.• Displays the front or rear panel view of the device and shows which slots are occupied. When you insert or remove a card, the Chassis View reflects the change immediately.• Changes color to indicate the port link status. For example, the ge port LED is green and steadily on when the port is up and red when the port is down.• Displays help tips when you hover the mouse over a port. <p>NOTE: You can also view the sub-ports details configured on any or all ports of the SRX5K-IOC4-MRATE line card.</p> |
| Show Front View | Displays the front view of the chassis and its components. |
| Show Rear View | Displays the rear view of the chassis and its components. |
| Zoom | Available on the left side of the chassis to zoom in or zoom out the chassis view. |
| Reset | Available on the left side of the chassis to set the chassis view for the default size. |

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 top right-hand 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:

- The Threat Activity pane is not available on SRX5400, SRX5600, and SRX5800 devices.
- For SRX Series devices configured for logical systems, the Logical System Identification and Logical System Profile panes are displayed when you log in as a user logical system administrator. These are the only logical system panes available in Dashboard Preferences.
- 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.

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 9 on page 41 provides the dashboard widgets options based on the selected device.

Table 9: 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 9: 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 also supports RE3 line cards for SRX5000 line of devices.</p> |
| Applications | Displays top 10 applications based on sessions or bandwidth. |
| Threats | Displays top 10 IPS sources, antispam sources, and antivirus name, sorted by count. |
| 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 also supports RE3 line cards for SRX5000 line of devices.</p> |
| Firewall: Top Denies | Displays top requests denied by the firewall based on their source IP addresses, sorted by count. |
| Firewall Policy: Rules With No Hits | Displays firewall policies with the most rules not hit, sorted by count. |
| Threat Activity | Provides the most current threats received on the device. |
| Firewall: Top Events | Displays all top 10 firewall events of the network traffic, sorted by count. |
| IDP: Top Events | Displays top 10 IDP events grouped by event-type, sorted by count. |
| 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. |
| Interface: Most Sessions | Displays top 10 interfaces with most sessions. |
| IP: Top Destinations | Displays top 10 destination-address, sorted by count or volume. |
| IP: Top Sources | Displays top 10 source-address of the network traffic, sorted by count or volume. |
| Virus: Top Blocked | Displays top 10 blocked viruses, sorted by count. |

Table 9: Dashboard Widgets Options (continued)

| Field | Description |
|--|---|
| Zones: Top Bandwidth by Packets | Displays top 10 zones with maximum throughput rate in packets. |
| Web Filtering: Top Web Blocked | Displays top 5 WebBlocked based on the CLI response. |
| Web Filtering: Top Source Address | Displays top 4 Source Address Web Filter based on the CLI response. |
| Web Filtering: Top Destination Address | Displays top 4 Destination Address Web Filter based on the CLI response. |
| Application & Users: High Risk Applications Blocked Per User | Displays top 4 High Risk Applications Blocked per user based on the CLI response. |
| Application & Users: High Risk Applications Allowed Per User | Displays High Risk Applications allowed per user. |
| Security Resources | Provides the maximum, configured, and activated number of sessions, firewall/VPN policies, and IPsec VPNs. |
| Chassis Status | Provides the component temperature and fan tray details of the system. Select Monitor > Device > Chassis Information for more information. NOTE: Chassis Status widget also supports RE3 line cards for SRX5000 line of devices and SCB4 line cards for SRX5600 and SRX5800 devices. |
| Content Filtering: Top Content Filters | Displays top 10 Protocol, Reason, and Source-address. |
| Web Filtering: Top Web Categories | Displays top 10 Web categories, Security risk, Productivity loss, Legal-liability and Blocked. |
| Threat Monitoring | Displays top Malwares identified, Threats and Infected categories. |
| Top Users of High Risk Applications by Volume/Count | Displays top users of High Risk Applications by volume. |
| Application & Users: Top Categories | Displays top 4 Categories of Application & Users sorted by count and volume. |
| Application & Users: Top Users | Displays top 4 Users sorted by count and volume. |
| Application & Users: Top IPs | Displays top 4 IPs of Application & Users sorted by count and volume. |
| Application & Users: Top High Risk Applications | Displays top 4 High Risk Applications sorted by risk, count and volume. |

Table 9: Dashboard Widgets Options (*continued*)

| Field | Description |
|---|--|
| Anti Spam: Top Source Address | Displays top 4 Antispam group by source address and sorted by count. |
| Application & Users: Application Usage by Category/Type | Displays top 5 Application Usage by Category group. |
| Application & Users: Users with the Most Critical Application Usage | Displays top 5 Users with the Most Critical Application Usage volume. |
| 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. |

3

PART

Monitor

[Interfaces](#) | **47**

[Access](#) | **53**

[Multi Tenancy](#) | **55**

[Alarms](#) | **62**

[Events](#) | **65**

[Users](#) | **108**

[Device](#) | **110**

[Routing](#) | **131**

[Class of Service \(CoS\)](#) | **140**

[MPLS](#) | **148**

[DHCP](#) | **154**

[NAT](#) | **158**

[Authentication](#) | **170**

[Security Services](#) | **174**

[VPN](#) | **200**

[Flow Session](#) | **204**

[Flow Gate](#) | **207**

[VLAN](#) | **209**

[Wireless LAN](#) | **211**

[Threats Map \(Live\)](#) | **215**

Interfaces

IN THIS CHAPTER

- [Monitor Ports | 47](#)
- [Monitor PPPoE | 49](#)

Monitor Ports

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

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

NOTE:

- J-Web also 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 also 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.

[Table 10 on page 47](#) describes the fields on the Ports page.

Table 10: Fields on the Ports Page

| Field | Description |
|-------------------|---|
| Start/Stop button | Starts or stops monitoring the selected interfaces. |
| Port | Displays the interface name. |
| Admin Status | Displays whether the interface is enabled (Up) or disabled (Down). |
| Link Status | Displays whether the interface is linked (Up) or not linked (Down). |

Table 10: Fields on the Ports Page (*continued*)

| Field | Description |
|-----------------------------|---|
| Address | Displays the IP address of the interface. |
| Zone | Displays whether the zone is an untrust zone or a trust zone. |
| Services | Displays services that are enabled on the device, such as HTTP and SSH. |
| Protocols | Displays protocols that are enabled on the device, such as BGP and IGMP. |
| Interface Statistics | |
| Input Rate | Displays interface bandwidth utilization. Input rates are shown in bytes per second. |
| Output Rate | Displays interface bandwidth utilization. Output rates are shown in bytes per second. |
| Error Counters | Displays input and output error counters in the form of a bar chart. |
| Packet Counters | Displays the number of broadcast, unicast, and multicast packet counters in the form of a pie chart. (Packet counter charts are supported only for interfaces that support MAC statistics). |

[Table 11 on page 48](#) shows the options to change the Interface display on the Ports page.

Table 11: Options to change the Interface Display

| Field | Description |
|---------------|---|
| Port for FPC | Controls the member for which information is displayed. |
| Show Graph | Displays input and output packet counters and error counters in the form of charts. |
| Pop-up button | Displays the interface graphs in a separate pop-up window. |
| Details | Displays extensive statistics about the selected interface, including its general status, traffic information, IP address, I/O errors, class-of-service data, and statistics. |

Table 11: Options to change the Interface Display (*continued*)

| Field | Description |
|------------------|---|
| Refresh Interval | Indicates the duration of time after which you want the data on the page to be refreshed. |
| Clear Statistics | Clears the statistics for the selected interface. |

Alternatively, you can enter the following show commands in the CLI to view interface status and traffic statistics:

- **show interfaces terse**

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

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

RELATED DOCUMENTATION

| [Monitor PPPoE](#) | 49

Monitor PPPoE

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

Use this page to view information on the session status for PPPoE interfaces, cumulative statistics for all PPPoE interfaces on the device, and the PPPoE version configured on the device.

NOTE: This option is not available in SRX5000 line of devices, SRX4200, and SRX4600 devices.

To view interface-specific properties in the J-Web interface, select the interface name on the PPPoE page.

[Table 12 on page 50](#) describes the fields on the PPPoE page.

Table 12: Fields on the PPPoE Page

| Field | Description |
|-------------------------|---|
| Interface | <p>Name of the PPPoE interface.</p> <p>Click the interface name to display PPPoE information for the interface.</p> |
| State | State of the PPPoE session on the interface. |
| Session ID | <p>Unique session identifier for the PPPoE session.</p> <p>To establish a PPPoE session, first the device acting as a PPPoE client obtains the Ethernet address of the PPPoE server or access concentrator, and then the client and the server negotiate a unique session ID. This process is referred to as PPPoE active discovery and is made up of four steps:</p> <ul style="list-style-type: none"> • initiation • offer • request • session confirmation. <p>The access concentrator generates the session ID for session confirmation and sends it to the PPPoE client in a PPPoE Active Discovery Session-Confirmation (PADS) packet.</p> |
| Service Name | <p>Type of service required from the access concentrator.</p> <p>Service Name identifies the type of service provided by the access concentrator, such as the name of the Internet service provider (ISP), class, or quality of service.</p> |
| Configured AC Name | Configured access concentrator name. |
| Session AC Names | Name of the access concentrator. |
| AC MAC Address | Media access control (MAC) address of the access concentrator. |
| Session Uptime | Number of seconds the current PPPoE session has been running. |
| Auto-Reconnect Time-out | Number of seconds to wait before reconnecting after a PPPoE session is terminated. |
| Idle Time-out | Number of seconds a PPPoE session can be idle without disconnecting. |
| Underlying Interface | Name of the underlying logical Ethernet or ATM interface on which PPPoE is running—for example, ge-0/0/0.1. |
| PPPoE Statistics | |

Table 12: Fields on the PPPoE Page (*continued*)

| Field | Description |
|-----------------------|---|
| Active PPPoE Sessions | Total number of active PPPoE sessions. |
| Packet Type | <p>Packets sent and received during the PPPoE session, categorized by packet type and packet error:</p> <ul style="list-style-type: none"> • PADI—PPPoE Active Discovery Initiation packets. • PADO—PPPoE Active Discovery Offer packets. • PADR—PPPoE Active Discovery Request packets. • PADS—PPPoE Active Discovery Session - Confirmation packets. • PADT—PPPoE Active Discovery Terminate packets. • Service Name Error—Packets for which the Service-Name request could not be honored. • AC System Error—Packets for which the access concentrator experienced an error in processing the host request. For example, the host had insufficient resources to create a virtual circuit. • Generic Error—Packets that indicate an unrecoverable error occurred. • Malformed Packet—Malformed or short packets that caused the packet handler to disregard the frame as unreadable. • Unknown Packet—Unrecognized packets. |
| Sent | Number of the specific type of packet sent from the PPPoE client. |
| Received | Number of the specific type of packet received by the PPPoE client. |
| Timeout | <p>Information about the timeouts that occurred during the PPPoE session.</p> <ul style="list-style-type: none"> • PADI—Number of timeouts that occurred for the PADI packet. • PADO—Number of timeouts that occurred for the PADO packet. (This value is always 0 and PADO is not supported). • PADR—Number of timeouts that occurred for the PADR packet. |
| Sent | Number of the timeouts that occurred for PADI, PADO, and PADR packets. |
| PPPoE Version | |
| Maximum Sessions | Maximum number of active PPPoE sessions the device can support. The default is 256 sessions. |

Table 12: Fields on the PPPoE Page (*continued*)

| Field | Description |
|-------------------------------|---|
| PADI Resend Timeout | <p>Initial time, (in seconds) the device waits to receive a PADO packet for the PADI packet sent. For example, 2 seconds. This timeout doubles for each successive PADI packet sent.</p> <p>The PPPoE Active Discovery Initiation (PADI) packet is sent to the access concentrator to initiate a PPPoE session. Typically, the access concentrator responds to a PADI packet with a PPPoE Active Discovery Offer (PADO) packet. If the access concentrator does not send a PADO packet, the device sends the PADI packet again after timeout period is elapsed. The PADI Resend Timeout doubles for each successive PADI packet sent. For example, if the PADI Resend Timeout is 2 seconds, the second PADI packet is sent after 2 seconds, the third after 4 seconds, the fourth after 8 seconds, and so on.</p> |
| PADR Resend Timeout | <p>Initial time (in seconds) the device waits to receive a PADS packet for the PADR packet sent. This timeout doubles for each successive PADR packet sent.</p> <p>The PPPoE Active Discovery Request (PADR) packet is sent to the access concentrator in response to a PADO packet, and to obtain the PPPoE session ID. Typically, the access concentrator responds to a PADR packet with a PPPoE Active Discovery Session-Confirmation (PADS) packet, which contains the session ID. If the access concentrator does not send a PADS packet, the device sends the PADR packet again after the PADR Resend Timeout period is elapsed. The PADR Resend Timeout doubles for each successive PADR packet sent.</p> |
| Maximum Resend Timeout | Maximum value (in seconds) that the PADI or PADR resend timer can accept. For example, 64 seconds. The maximum value is 64. |
| Maximum Configured AC Timeout | Time (in seconds), within which the configured access concentrator must respond. |

Alternatively, enter the following CLI commands:

- **show pppoe interfaces**
- **show pppoe statistics**
- **show pppoe version**

You can also view status information about the PPPoE interface by entering the `show interfaces pp0` command in the CLI editor.

RELATED DOCUMENTATION

Access

IN THIS CHAPTER

- [Monitor Address Pools](#) | 53

Monitor Address Pools

You are here: **Monitor** > **Access** > **Address Pools**.

Use this page to view the properties and assignments of the address pool.

NOTE: This option is not available in SRX5000 line of devices and SRX4000 line of devices.

[Table 13 on page 53](#) describes the fields on the Address Pools page.

Table 13: Fields on the Address Pools Page

| Field | Description |
|--------------------------------|---|
| Address Pool Properties | |
| Address Pool | Select an address pool to view its properties and assignments. |
| Refresh Button | Refreshes the data of the address pool assignment. |
| Address Pool Name | Displays the name of the address pool. |
| Network Address | Displays the IP network address of the address pool. |
| Address Ranges | Displays the name, the lower limit, and the upper limit of the address range. |
| Primary DNS | Displays the primary-dns IP address. |
| Secondary DNS | Displays the secondary-dns IP address. |

Table 13: Fields on the Address Pools Page *(continued)*

| Field | Description |
|--|--|
| Primary WINS | Displays the primary-wins IP address. |
| Secondary WINS | Displays the secondary-wins IP address. |
| Address Pool Address Assignment | |
| IP Address | Displays the IP address of the address pool. |
| Hardware Address | Displays the hardware MAC address of the address pool. |
| Host/User | Displays the user name using the address pool. |
| Type | Displays the authentication type used by the address pool NOTE: The authentication types can be extended authentication (XAuth) or IKE Authentication. |

RELATED DOCUMENTATION

| [Monitor Ports](#) | 47

Multi Tenancy

IN THIS CHAPTER

- [Monitor Logical Systems | 55](#)
- [Monitor Tenants | 58](#)

Monitor Logical Systems

You are here: **Monitor** > **Multi Tenancy** > **Logical System**.

An SRX Series device with a multitenant logical systems device, provides various departments, organizations, customers, and partners a private use of the portion of its resource and a private view of the device.

[Table 14 on page 55](#) describes the fields on the logical system page.

Table 14: Fields on the Logical Systems Page

| Field | Description |
|--------------------|--|
| Name | Displays the logical systems configured on the device. |
| Resource Profile | Displays the logical system profile assigned to each logical system. |
| Zone Usage | Displays the used and reserved number of zones that user logical system administrators and primary logical system administrators have configured for their logical systems if the security profile is bound to the logical systems. |
| Scheduler Usage | Displays the number of schedulers that user logical system administrators and primary logical system administrators have configured for their logical systems if the security profile is bound to the logical systems. |
| Policy Count Usage | Displays the number of security policies with a count that user logical system administrators and primary logical system administrators have configured for their logical systems if the security profile is bound to the logical systems. |

Table 14: Fields on the Logical Systems Page (*continued*)

| Field | Description |
|----------------------------------|--|
| Policy Without Count Usage | Displays the number of security policies without a count that user logical system administrators and primary logical system administrators have configured for their logical systems if the security profile is bound to the logical systems. |
| Nat Static Rule Usage | Displays the number of NAT static rule configurations that user logical system administrators and primary logical system administrators have configured for their logical systems if the security profile is bound to the logical systems. |
| Nat Source Rule Usage | Displays the NAT source rule configurations that user logical system administrators and primary logical system administrators have configured for their logical systems if the security profile is bound to the logical systems. |
| Nat Source Pool Usage | Displays the NAT source pool configurations that logical system administrators and primary logical system administrators have configured for their logical systems if the security profile is bound to the logical systems. |
| Nat Rule Referenced Prefix Usage | Displays the security NAT rule referenced IP prefix quota of a logical system. |
| Nat Port-ol IP Number Usage | Displays the number of NAT port overloading IP number configurations that user logical system administrators and primary logical system administrators have configured for their logical systems if the security profile is bound to the logical systems. |
| Nat Pat Portnum Usage | Displays the used quantity and the reserved quantity of ports for the logical system as part of the security profile. |
| Nat Pat Address Usage | Displays the number of NAT with port address translation (PAT) configurations that user logical system administrators and primary logical system administrators have configured for their logical systems if the security profile is bound to the logical systems. |
| Nat Address Usage | Displays the number of NAT without port address translation configurations that user logical system administrators and primary logical system administrators have configured for their logical systems if the security profile is bound to the logical systems. |
| Nat Interface Port-ol IP Usage | Displays the security NAT interface port overloading quota of a logical system. |
| Nat Destination Rule Usage | Displays the number of NAT destination rule configurations that user logical system administrators and primary logical system administrators have configured for their logical systems if the security profile is bound to the logical systems. |

Table 14: Fields on the Logical Systems Page (*continued*)

| Field | Description |
|---------------------------------|--|
| Nat Destination Pool Usage | Displays the number of NAT destination pools that user logical system administrators and primary logical system administrators have configured for their logical systems if the security profile is bound to the logical systems. |
| Nat Cone Binding Usage | Displays the number of NAT cone binding configurations that user logical system administrators and primary logical system administrators have configured for their logical systems if the security profile is bound to the logical systems. |
| Flow Session Usage | Displays the number of flow sessions that user logical system administrators and primary logical system administrators have configured for their logical systems if the security profile is bound to the logical systems. |
| Flow Gate Usage | Displays the number of flow gates, also known as pinholes, that user logical system administrators and primary logical system administrators have configured for their logical systems if the security profile is bound to the logical systems. |
| DsLite Software Initiator Usage | <p>Displays the number of IPv6 dual-stack lite (DS-Lite) software initiators that can connect to the software concentrator configured in either a user logical system or the primary logical system.</p> <p>NOTE: This statement is configured in the security profile that is bound to the logical system.</p> |
| CPU on SPU Usage | <p>Displays the CPU utilization and average utilization of all SPUs is shown</p> <p>NOTE: The detail option shows CPU utilization on each SPU.</p> |
| Auth Entry Usage | Displays the number of firewall authentication entries that user logical system administrators and primary logical system administrators have configured for their logical systems if the security profile is bound to the logical systems. |
| Appfw Rule Set Usage | Displays the number of application firewall rule set configurations that a primary administrator has configured for a primary logical system or user logical system when the security profile is bound to the logical systems. |
| Appfw Rule Usage | Displays the number of application firewall rule configurations that a primary administrator have configured for a primary logical system or user logical system when the security profile is bound to the logical systems. |

Table 14: Fields on the Logical Systems Page (*continued*)

| Field | Description |
|---------------------|--|
| appfw-profile-count | Displays the application firewall profile quota of a logical system NOTE: As a primary administrator, you can create a security profile and specify the kinds and amounts of resources to allocate to a logical system to which the security profile is bound. |
| address-book-count | Displays the number of address books that user logical system administrators and primary logical system administrators have configured for their logical systems if the security profile is bound to the logical systems. |

RELATED DOCUMENTATION

| [Monitor Tenants](#) | 58

Monitor Tenants

You are here: **Monitor** > **Multi Tenancy** > **Tenants**.

An SRX Series device with a multitenant systems device, provides various departments, organizations, customers, and partners, depending on your environment, private and logically separated use of system resources and tenant-specific views of security configuration and KPIs.

[Table 15 on page 58](#) describes the fields on the Tenants page.

Table 15: Fields on the Tenants Page

| Field | Description |
|-----------------------|---|
| View Details | Displays the grid view or graph view of all the resources for the tenant you have selected. |
| Search icon | Enables you to search for a tenant system in the grid. |
| Filter icon | Enables you to filter and display the list of tenants based on a column in the grid. |
| Show Hide Column icon | Enables you to show or hide a column in the grid. |
| Name | Displays the tenants configured on the device. |

Table 15: Fields on the Tenants Page (continued)

| Field | Description |
|----------------------------------|--|
| Resource Profile | Displays the resource profile assigned to each tenant. |
| Zone Usage | Displays the used and reserved number of zones for the given tenant. |
| Scheduler Usage | Displays the number of schedulers that primary administrators have configured for their tenants. |
| Policy Count Usage | Displays the number of security policies with a count primary administrators have configured for their tenants if the security profile is bound to the tenants. |
| Policy Without Count Usage | Displays the number of security policies without a count that primary administrators have configured for their tenants if the security profile is bound to the tenants. |
| Nat Static Rule Usage | Displays the number of NAT static rule configurations that primary administrators have configured for their tenants if the security profile is bound to the tenants. |
| Nat Source Rule Usage | Displays the NAT source rule configurations that primary administrators have configured for their tenants if the security profile is bound to the tenants. |
| Nat Source Pool Usage | Displays the NAT source pool configurations that primary administrators have configured for their tenants if the security profile is bound to the tenants. |
| Nat Rule Referenced Prefix Usage | Displays the security NAT rule referenced IP prefix quota of a tenant. |
| Nat Port-OI IP Number Usage | Displays the number of NAT port overloading IP number configurations that primary administrators have configured for their tenants if the security profile is bound to the tenants. |
| Nat Pat Portnum Usage | Displays the used quantity and the reserved quantity of ports for the tenant as part of the security profile. |
| Nat Pat Address Usage | Displays the number of NAT with port address translation (PAT) configurations that primary administrators have configured for their tenants if the security profile is bound to the tenants. |
| Nat No Pat Address Usage | Displays the number of NAT without port address translation configurations that primary administrators have configured for their tenants if the security profile is bound to the tenants. |
| Nat Interface Port-OI IP Usage | Displays the security NAT interface port overloading quota of a tenant. |

Table 15: Fields on the Tenants Page (*continued*)

| Field | Description |
|---------------------------------|---|
| Nat Destination Rule Usage | Displays the number of NAT destination rule configurations that primary administrators have configured for their tenants if the security profile is bound to the tenants. |
| Nat Destination Pool Usage | Displays the number of NAT destination pools that primary administrators have configured for their tenants if the security profile is bound to the tenants. |
| Nat Cone Binding Usage | Displays the number of NAT cone binding configurations that primary administrators have configured for their tenants if the security profile is bound to the tenants. |
| Flow Session Usage | Displays the number of flow sessions that primary administrators have configured for their tenants if the security profile is bound to the tenants. |
| Flow Gate Usage | Displays the number of flow gates, also known as pinholes, that primary administrators have configured for their tenants if the security profile is bound to the tenants. |
| DsLite Software Initiator Usage | <p>Displays the number of IPv6 dual-stack lite (DS-Lite) software initiators that can connect to the software concentrator configured in either a user tenant or the primary tenant</p> <p>NOTE: This statement is configured in the security profile that is bound to the tenant.</p> |
| CPU on SPU Usage | <p>Displays the CPU utilization and average utilization of all SPUs</p> <p>NOTE: The detail option shows CPU utilization on each SPU.</p> |
| Auth Entry Usage | Displays the number of firewall authentication entries that primary administrators have configured for their tenants if the security profile is bound to the tenants. |
| Appfw Rule Set Usage | Displays the number of application firewall rule set configurations that a primary administrator has configured for a tenant when the security profile is bound to the tenants. |
| Appfw Rule Usage | Displays the number of application firewall rule configurations that a primary administrator have configured for a primary tenant or user tenant when the security profile is bound to the tenants. |

Table 15: Fields on the Tenants Page (*continued*)

| Field | Description |
|---------------------|--|
| appfw-profile-count | <p>Displays the application firewall profile quota of a tenant</p> <p>NOTE: As a primary administrator, you can create a security profile and specify the kinds and amount of resources to allocate to a tenant to which the security profile is bound.</p> |
| address-book-count | Displays the number of address books that primary administrators have configured for their tenants if the security profile is bound to the tenants. |

RELATED DOCUMENTATION

| [Monitor Logical Systems](#) | 55

Alarms

IN THIS CHAPTER

- [Monitor Alarms | 62](#)
- [Monitor Policy Log | 63](#)

Monitor Alarms

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

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

[Table 16 on page 62](#) describes the fields on the Alarms page.

Table 16: Fields on the Alarms Page

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

Table 16: Fields on the Alarms Page (*continued*)

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

RELATED DOCUMENTATION

| [Monitor Policy Log](#) | 63

Monitor Policy Log

You are here: **Monitor** > **Alarms** > **Policy Log**.

Use the monitoring functionality to view the Policy Log page.

[Table 17 on page 63](#) describes the fields on the Policy Log page.

Table 17: Fields on the Policy Log Page

| Field | Description |
|---------------------|--|
| Log file name | Name of the event log files to search. |
| Policy name | Name of the policy of the events to be retrieved. |
| Source address | Source address of the traffic that triggered the event. |
| Destination address | Destination address of the traffic that triggered the event. |
| Event type | Type of event that was triggered by the traffic. |

Table 17: Fields on the Policy Log Page (*continued*)

| Field | Description |
|-------------------------|---|
| Application | Application of the traffic that triggered the event. |
| Source port | Source port of the traffic that triggered the event. |
| Destination port | Destination port of the traffic that triggered the event. |
| Source zone | Source zone of the traffic that triggered the event. |
| Destination zone | Destination zone of the traffic that triggered the event. |
| Source NAT rule | Source NAT rule of the traffic that triggered the event. |
| Destination NAT rule | Destination NAT rule of the traffic that triggered the event. |
| Is global policy | Specifies that the policy is a global policy. |
| Timestamp | Time when the event occurred. |
| Policy name | Policy that triggered the event. |
| Record type | Type of event log providing the data. |
| Source IP/Port | Source address (and port, if applicable) of the event traffic. |
| Destination IP/Port | Destination address (and port, if applicable) of the event traffic. |
| Service name | Service name of the event traffic. |
| NAT source IP/Port | NAT source address (and port, if applicable) of the event traffic. |
| NAT destination IP/Port | NAT destination address (and port, if applicable) of the event traffic. |

RELATED DOCUMENTATION

[Monitor Alarms](#) | 62

Events

IN THIS CHAPTER

- Monitor All Events | 65
- Monitor Firewall Events | 70
- Monitor Web Filtering Events | 75
- Monitor IPsec VPNs Events | 79
- Monitor Content Filtering Profiles Events | 83
- Monitor Antispam Events | 87
- Monitor Antivirus Events | 91
- Monitor IPS Events | 95
- Monitor Screen Events | 99
- Monitor Security Intelligence Events | 101
- Monitor ATP Events | 103
- Monitor System Events | 105

Monitor All Events

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

Use this page to view the summary of all the events, threat severity, attacks, graphs, and grid elements for all types of events.

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

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

- Grid View—View the comprehensive details of events in a tabular format that includes sortable columns. You can group the events using the Group By option. For example, you can group the events based on source country, Source IP etc. The table includes information such as the event name, Source country, source IP address, and so on. [Table 18 on page 66](#) describes the fields on the Grid View page.

- **Chart View**—View a brief summary of all the events in your network. The top of the page has a swim lane graph of all the all events. You can use the widgets at the bottom of the page to view critical information such as, top sources, top source countries, top destinations, and top destination countries. [Table 19 on page 69](#) describes the widgets on the Chart View page.

Table 18: All Events—Fields on the Grid View Page

| Field | Description |
|---------------------------|---|
| Grid View | Displays information in grids that are lazy loaded with infinite scrolling. You can narrow down your search to a particular event based on IP address, description, or attack name. |
| Filters | Displays the filters list that are displayed above the grids. |
| First filter list | <p>Displays the options available in the first filter list are: Firewall, Webfilter, ContentFilter, Antispam, Antivirus, IPsec VPN, IPS, Screens, Security Intelligence, and ATP.</p> <p>Select the event that you want to filter in the first filter list.</p> |
| Second filter list | <p>Displays the options available in the second filter list are: Event-name, Source-address, Destination-address, Source name, User, Role, Reason, Profile, Protocol, and Category.</p> <p>Select the next criteria of the event on which you want to filter from the second filter list.</p> |

Table 18: All Events—Fields on the Grid View Page (continued)

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

Table 18: All Events—Fields on the Grid View Page (*continued*)

| Field | Description |
|----------------------------|--|
| UTM Category or Virus Name | Displays the UTM category of the log. |
| Event Category | Displays the event category of the log. |
| Source Country | Displays the source country of the event. |
| Source IP | Displays the source IP address from where the event occurred. |
| Source Port | Displays the source port of the event. |
| Destination Country | Displays the destination country of the event. |
| Destination IP | Displays the destination IP address of the event. |
| Destination Port | Displays the destination port of the event. |
| Application | Displays the application name from which the events or logs are generated. |
| Username | Displays the username from whom the log is generated. |
| Hostname | Displays the host name in the log. |
| Service Name | Displays the name of the application service. For example, FTP, HTTP, SSH, and so on. |
| Protocol ID | Displays the protocol ID in the log. |
| Policy Name | Displays the Policy name in the log. |
| Source Zone | Displays the User traffic received from the zone. |
| Destination Zone | Displays the destination zone of the log. |
| Nested Application | Displays the nested application in the log. |
| Roles | Displays the role names associated with the event. |
| Reason | Displays the reason for the log generation. For example, a connection tear down may have an associated reason such as authentication failed. |
| NAT Source Port | Displays the translated source port. |

Table 18: All Events—Fields on the Grid View Page (continued)

| Field | Description |
|---------------------------|---|
| NAT Destination Port | Displays the translated destination port. |
| NAT Source Rule Name | Displays the NAT source rule name. |
| NAT Destination Rule Name | Displays the NAT destination rule name. |
| NAT Source IP | Displays the translated (or natted) source IP address. It can contain IPv4 or IPv6 addresses. |
| NAT Destination IP | Displays the translated (also called natted) destination IP address. |
| Traffic Session ID | Displays the traffic session ID of the log. |
| URL | Displays the accessed URL name that triggered the event. |
| Object Name | Displays the object name of the log. |
| Path Name | Displays the path name of the log. |
| Logical System Name | Displays the name of the logical system. |
| Rule Name | Displays the rule name of the log. |
| Action | Displays the action taken for the event: warning, allow, and block. |
| Time | Displays the time when the log was received. |

Table 19: All Events—Widgets on the Chart View Page

| Field | Description |
|-------------------|--|
| Chart View | Displays the trend analysis, displayed in the Time Range graph, in numbers. |
| Total Events | Displays the total number of events that occurred in the specified time range. |
| Virus Instances | Displays the number of virus instances that occurred in the specified time range. |
| Attacks | Displays the number of IDP or IPS attacks that occurred in the specified time range. |
| Interface Down | Displays the total number of interfaces that are down. |

Table 19: All Events—Widgets on the Chart View Page (continued)

| Field | Description |
|-----------------------|---|
| Sessions | Displays the total number of firewall events or sessions that occurred during the time period specified in the Time Range graph. |
| Graphs | The graphs display the trend analysis in swim lane chart for the time range that you specified in the Time Range graph. |
| Firewall | Mouse over at any point in the swim lane chart to view further details at that point. |
| Web Filtering | |
| IPsec VPNs | The legend in each graph shows the colors and its related interpretation. |
| Content Filtering | For example, in the Firewall graph, blue color represents all firewall events and black represents blocked firewall events. Similarly, in the IPS graph, orange, amber, and yellow represent critical, high, and medium IPS attacks respectively. |
| Antispam | |
| Antivirus | |
| IPS | |
| Screen | |
| Security Intelligence | |
| ATP | |

RELATED DOCUMENTATION

[Monitor Firewall Events](#) | 70

Monitor Firewall Events

You are here: **Monitor** > **Events** > **Firewall**.

Use this page to view information about the security events based on Event name, Source address, Destination address, Applications, User, Service, Policy, Nested application, Source interface and Source zone.

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

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

- **Grid View**—View the comprehensive details of firewall events in a tabular format that includes sortable columns. You can group the events using the Group By option. For example, you can group the events based on source country. The table includes information such as the event name, source IP, destination country, and so on. [Table 20 on page 71](#) describes the fields on the Grid View page.
- **Chart View**—View a brief summary of all the firewall events in your network. The top of the page has a swim lane graph of all the firewall events. You can use the widgets at the bottom of the page to view critical information such as, top sources, top destinations, and top users. [Table 21 on page 74](#) describes the widgets on the Chart View page.

Table 20: Firewall—Fields on the Grid View Page

| Field | Description |
|---|---|
| The filter that is displayed above the grids. | <p>Displays the options available in the filter list are:</p> <ul style="list-style-type: none"> • Event Name—Displays the event name of the log. • Source Address—Displays the source addresses to be used as match criteria for the policy. Address sets are resolved to their individual names. • Destination Address—Displays the destination addresses (or address sets) to be used as match criteria for the policy. Addresses are entered as specified in the destination zone's address book. • Application—Displays the application name from which the events or logs are generated. • User—Displays the user name from whom the log is generated. • Service—Displays the name of the application service. For example, FTP, HTTP, SSH, and so on. • Policy—Displays the Policy name in the log. • Nested Application—Displays the nested application in the log. • Source Interface—Specify the source interface for ICMP requests. If no source interface is specified, the device automatically uses the local tunnel endpoint interface. • Source Zone—Displays the User traffic received from the zone. <p>Select the criteria or parameter on which you want to construct the filter statement.</p> |

Table 20: Firewall—Fields on the Grid View Page (*continued*)

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

Table 20: Firewall—Fields on the Grid View Page (*continued*)

| Field | Description |
|---------------------------|--|
| Event Category | Displays the event category of the log. |
| Source IP | Displays the source IP address from where the event occurred. |
| Source Port | Displays the source port of the event. |
| Application | Displays the application name from which the events or logs are generated. |
| User Name | Displays the user name from whom the log is generated. |
| Host Name | Displays the host name in the log. |
| Service Name | Displays the name of the application service. For example, FTP, HTTP, SSH, and so on. |
| Protocol ID | Displays the protocol ID in the log. |
| Policy Name | Displays the policy name in the log. |
| Destination Zone | Displays the destination zone of the log. |
| Roles | Displays the role names associated with the event. |
| Reason | Displays the reason for the log generation. For example, a connection tear down may have an associated reason such as authentication failed. |
| NAT Source Port | Displays the translated source port. |
| NAT Destination Port | Displays the translated destination port. |
| NAT Source Rule Name | Displays the NAT source rule name. |
| NAT Destination Rule Name | Displays the NAT destination rule name. |
| NAT Source IP | Displays the translated (or natted) source IP address. It can contain IPv4 or IPv6 addresses. |
| NAT Destination IP | Displays the translated (also called natted) destination IP address. |
| Traffic Session ID | Displays the traffic session ID of the log. |

Table 20: Firewall—Fields on the Grid View Page (*continued*)

| Field | Description |
|---------------------|--|
| URL | Displays the accessed URL name that triggered the event. |
| Object Name | Displays the object name of the log. |
| Path Name | Displays the path name of the log. |
| Logical System Name | Displays the name of the logical system. |
| Rule Name | Displays the rule name of the log. |
| Action | Displays the action taken for the event: warning, allow, and block. |
| Profile Name | Displays the profile name in the log. |
| Time | Displays the time when the log was received. |
| Source IP | Displays the source IP address from where the event occurred. |
| Destination Country | Displays the destination country name from where the event occurred. |
| Destination IP | Displays the destination IP address of the event. |
| Destination Port | Displays the destination port of the event. |

Table 21: Firewall—Widgets on the Chart View Page

| Field | Description |
|------------------|---|
| Top Sources | Displays the top five source IP addresses of the network traffic; sorted by event count. |
| Top Destinations | Displays the top five destination IP addresses of the network traffic; sorted by event count. |
| Top Users | Displays the top five users of the network traffic; sorted by event count. |

RELATED DOCUMENTATION

Monitor Web Filtering Events

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

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

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

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

- **Grid View**—View the comprehensive details of web filtering events in a tabular format that includes sortable columns. You can group the events using the Group By option. For example, you can group the events based on source country. The table includes information such as the event name, time, source IP, source country, and so on. [Table 22 on page 75](#) describes the fields on the Grid View page.
- **Chart View**—View a brief summary of all the web filtering events in your network. The top of the page has a swim lane graph of all the screen events. You can use the widgets at the bottom of the page to view critical information such as, top sources, Top URLs blocked, and Top URL Categories Blocked. [Table 23 on page 78](#) describes the widgets on the Chart View page.

Table 22: Web Filtering—Fields on the Grid View Page

| Field | Description |
|--|--|
| The filter list that is displayed above the grids. | <p>Options available in the filter list are:</p> <ul style="list-style-type: none"> • Event Name—Displays the event name of the log. • Source Address—Displays the source addresses to be used as match criteria for the policy. Address sets are resolved to their individual names. • Destination Address—Displays the destination addresses (or address sets) to be used as match criteria for the policy. Addresses are entered as specified in the destination zone's address book. • Source Name—Displays the source name of the log. • User—Displays the user name from whom the log is generated. • Role—Displays the role names associated with the event. • Reason—Displays the reason for the log generation. For example, a connection tear down may have an associated reason such as authentication failed. • Profile—Displays the profile name in the log. • Protocol—Displays the protocol in the log. • Category—Displays the category of the log. <p>Select the criteria or parameter on which you want to construct the filter statement.</p> |

Table 22: Web Filtering—Fields on the Grid View Page (continued)

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

Table 22: Web Filtering—Fields on the Grid View Page (*continued*)

| Field | Description |
|----------------------------|--|
| UTM Category or Virus Name | Displays the UTM category or name of the virus. |
| Event Category | Displays the event category of the log. |
| Source Country | Displays the source country of the log. |
| Source IP | Displays the source IP address from where the event occurred. |
| Source Port | Displays the source port of the event. |
| Destination Country | Displays the destination country of the log. |
| Destination IP | Displays the destination IP address of the event. |
| Destination Port | Displays the destination port of the event. |
| Application | Displays the application name from which the events or logs are generated. |
| User name | Displays the user name from whom the log is generated. |
| Hostname | The host name in the log. |
| Service Name | The name of the application service. For example, FTP, HTTP, SSH, and so on. |
| Protocol ID | Displays the protocol ID in the log. |
| Policy name | Displays the policy name in the log. |
| Source Zone | User traffic received from the zone. |
| Destination Zone | Displays the destination zone of the log. |
| Nested Application | Displays the nested application in the log. |
| Roles | Role names associated with the event. |
| Reason | Displays the reason for the log generation. For example, a connection tear down may have an associated reason such as authentication failed. |
| NAT Source Port | Displays the translated source port. |

Table 22: Web Filtering—Fields on the Grid View Page (continued)

| Field | Description |
|---------------------------|---|
| NAT Destination Port | Displays the translated destination port. |
| NAT Source Rule Name | Displays the NAT source rule name. |
| NAT Destination Rule Name | Displays the NAT destination rule name. |
| NAT Source IP | Displays the translated (or natted) source IP address. It can contain IPv4 or IPv6 addresses. |
| NAT Destination IP | Displays the translated (also called natted) destination IP address. |
| Traffic Session ID | Displays the traffic session ID of the log. 32 |
| URL | Displays the accessed URL name that triggered the event. |
| Object Name | Displays the object name of the log. |
| Path Name | Displays the path name of the log. |
| Logical System Name | Displays the name of the logical system. |
| Rule Name | Displays the rule name of the log. |
| Action | Displays the action taken for the event: warning, allow, and block. |
| Profile Name | Displays the profile name in the log. |
| Time | Displays the time when the log was received. |
| Description | Displays the description of the log. |
| Action | Action taken for the event: warning, allow, and block |

Table 23: Web Filtering—Widgets on the Chart View Page

| Field | Description |
|----------------------------|---|
| Top URLs Blocked | Displays the top URLs that are blocked. |
| Top URL Categories Blocked | Displays the top URL categories that are blocked. |

Table 23: Web Filtering—Widgets on the Chart View Page (*continued*)

| Field | Description |
|-------------|--|
| Top Sources | Displays the top five source IP addresses of the network traffic; sorted by event count. |

RELATED DOCUMENTATION

[Monitor IPsec VPNs Events](#) | 79

Monitor IPsec VPNs Events

You are here: **Monitor** > **Events** > **IPsec VPNs**.

Use the monitoring functionality to view the Policy Log page.

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

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

- **Grid View**—View the comprehensive details of IPsec events in a tabular format that includes sortable columns. You can group the events using the Group By option. For example, you can group the events based on source country. The table includes information such as the event name, UTM category, destination country, source IP address, source country, and so on. [Table 24 on page 79](#) describes the fields on the Grid View page.
- **Chart View**—View a brief summary of all the IPsec events in your network. The top of the page has a swim lane graph of all the IPsec events. You can use the widgets at the bottom of the page to view critical information such as, top sources, top source countries, top destinations, and top destination countries. [Table 25 on page 82](#) describes the widgets on the Chart View page.

Table 24: IPsec VPNs—Fields on the Grid View Page

| Field | Description |
|--|--|
| The filter list that is displayed above the grids. | Displays the options available in the filter: <ul style="list-style-type: none"> • Event name—The event name of the log. |

Table 24: IPsec VPNs—Fields on the Grid View Page (*continued*)

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

Table 24: IPsec VPNs—Fields on the Grid View Page *(continued)*

| Field | Description |
|----------------------------|--|
| UTM Category or Virus Name | Displays the UTM category of the log. |
| Event Category | Displays the event category of the log. |
| Source Country | Displays the source country of the log. |
| Source IP | Displays the source IP address from where the event occurred. |
| Source Port | Displays the source port of the event. |
| Destination Country | Displays the destination country of the log. |
| Destination IP | Displays the destination IP address from where the event occurred. |
| Destination Port | The destination port of the event. |
| Application | Displays the application name from which the events or logs are generated. |
| User Name | Displays the user name from whom the log is generated. |
| Hostname | The host name in the log. |
| Service Name | Displays the name of the application service. For example, FTP, HTTP, SSH, and so on. |
| Protocol ID | Displays the protocol ID in the log. |
| Policy Name | Displays the policy name in the log. |
| Source Zone | Displays the user traffic received from the zone. |
| Destination Zone | Displays the destination zone of the log. |
| Nested Application | Displays the nested application in the log. |
| Roles | Displays the role names associated with the event. |
| Reason | Displays the reason for the log generation. For example, a connection tear down may have an associated reason such as authentication failed. |
| NAT Source Port | Displays the translated source port. |

Table 24: IPsec VPNs—Fields on the Grid View Page *(continued)*

| Field | Description |
|---------------------------|---|
| NAT Destination Port | Displays the translated destination port. |
| NAT Source Rule Name | Displays the NAT source rule name. |
| NAT Destination Rule Name | Displays the NAT destination rule name. |
| NAT Source IP | Displays the translated (or natted) source IP address. It can contain IPv4 or IPv6 addresses. |
| NAT Destination IP | Displays the translated (also called natted) destination IP address. |
| Traffic Session ID | Displays the traffic session ID of the log. |
| URL | Displays the accessed URL name that triggered the event. |
| Object Name | Displays the object name of the log. |
| Path Name | Displays the path name of the log. |
| Logical System Name | Displays the name of the logical system. |
| Rule Name | Displays the rule name of the log. |
| Action | Displays the action taken for the event: warning, allow, and block. |
| Profile Name | Displays the profile name in the log. |
| Time | Displays the time when the log was received. |

Table 25: IPsec VPNs—Widgets on the Chart View Page

| Field | Description |
|------------|--|
| IPsec VPNs | Gives a brief summary of all the IPsec VPN events in your network. |

RELATED DOCUMENTATION

[Monitor Content Filtering Profiles Events](#) | 83

Monitor Content Filtering Profiles Events

You are here: **Monitor** > **Events** > **Content Filtering Profiles**.

Use the monitoring functionality to view the Content Filtering page.

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

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

- **Grid View**—View the comprehensive details of content filtering events in a tabular format that includes sortable columns. You can group the events using the Group By option. For example, you can group the events based on source country. The table includes information such as the event name, UTM category, source IP address, source country, and so on. [Table 26 on page 83](#) describes the fields on the Grid View page.
- **Chart View**—View a brief summary of all the Content filtering events in your network. The top of the page has a swim lane graph of all the content filtering events. You can use the widgets at the bottom of the page to view critical information such as, top sources, top source countries, top destinations, and top destination countries. [Table 27 on page 86](#) describes the widgets on the Chart View page.

Table 26: Content Filtering—Fields on the Grid View Page

| Field | Description |
|--|--|
| The filter list that is displayed above the grids. | <p>Displays the options available in the filter list are:</p> <ul style="list-style-type: none"> • Event Name—Displays the event name of the log. • Source Address—Displays the source addresses to be used as match criteria for the policy. Address sets are resolved to their individual names. • Destination Address—Displays the destination addresses (or address sets) to be used as match criteria for the policy. Addresses are entered as specified in the destination zone's address book. • Source Name—Displays the source name of the log. • User— Displays the user name from whom the log is generated. • Role—Displays the role names associated with the event. • Reason —Displays the reason for the log generation. For example, a connection tear down may have an associated reason such as authentication failed. • Profile— Displays the profile name in the log. • Protocol—Displays the protocol ID in the log. • Category—Displays the category of the log. |

Table 26: Content Filtering—Fields on the Grid View Page (*continued*)

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

Table 26: Content Filtering—Fields on the Grid View Page *(continued)*

| Field | Description |
|----------------------|--|
| Source Country | Displays the source country of the log. |
| Source IP | Displays the source IP address from where the event occurred. |
| Source Port | Displays the source port of the event. |
| Application | Displays the application name from which the events or logs are generated. |
| Destination Country | Displays the destination country of the log. |
| Destination IP | Displays the destination IP of the log. |
| Destination Port | Displays the destination port of the log. |
| User Name | Displays the user name from whom the log is generated. |
| Host Name | Displays the host name in the log. |
| Service Name | Displays the name of the application service. For example, FTP, HTTP, SSH, and so on. |
| Protocol ID | Displays the protocol ID in the log. |
| Policy Name | Displays the policy name in the log. |
| Source Zone | Displays the source zone of the log. |
| Destination Zone | Displays the destination zone of the log. |
| Nested Application | Displays the nested application in the log. |
| Roles | Displays the role names associated with the event. |
| Reason | Displays the reason for the log generation. For example, a connection tear down may have an associated reason such as authentication failed. |
| NAT Source Port | Displays the translated source port. |
| NAT Destination Port | Displays the translated destination port. |
| NAT Source Rule Name | Displays the NAT source rule name. |

Table 26: Content Filtering—Fields on the Grid View Page *(continued)*

| Field | Description |
|---------------------------|---|
| NAT Destination Rule Name | Displays the NAT destination rule name. |
| NAT Source IP | Displays the translated (or natted) source IP address. It can contain IPv4 or IPv6 addresses. |
| NAT Destination IP | Displays the translated (also called natted) destination IP address. |
| Traffic Session ID | Displays the traffic session ID of the log. 32 |
| URL | Displays the accessed URL name that triggered the event. |
| Object Name | Displays the object name of the log. |
| Path Name | Displays the path name of the log. |
| Logical System Name | Displays the name of the logical system. |
| Rule Name | Displays the rule name of the log. |
| Action | Displays the action taken for the event: warning, allow, and block. |
| Profile Name | Displays the profile name in the log. |
| Time | Displays the time when the log was received. |

Table 27: Content Filtering—Widgets on the Chart View Page

| Field | Description |
|-------------------------------|---|
| Top Blocked Protocol Commands | Adds respective content for display column. |
| Top Reasons | Adds respective content for display column. |
| Top Sources | Top five source IP addresses of the network traffic; sorted by event count. |

RELATED DOCUMENTATION

Monitor Antispam Events

You are here: **Monitor** > **Events** > **Antispam**.

Use the monitoring functionality to view the Antispam page.

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

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

- **Grid View**—View the comprehensive details of Antispam events in a tabular format that includes sortable columns. You can group the events using the Group By option. For example, you can group the events based on source country. The table includes information such as the event name, UTM category, source IP address, source country, and so on. [Table 28 on page 87](#) describes the fields on the Grid View page.
- **Chart View**—View a brief summary of all the Antispam events in your network. The top of the page has a swim lane graph of all the screen events. You can use the widgets at the bottom of the page to view critical information such as, top sources, top source countries, top destinations, and top destination countries. [Table 29 on page 90](#) describes the widgets on the Chart View page.

Table 28: Antispam—Fields on the Grid View Page

| Field | Description |
|--|---|
| The filter list that is displayed above the grids. | <p>Displays the options available in the filter list are:</p> <ul style="list-style-type: none"> • Event Name—Displays the event name of the log. • Source Address—Displays the source addresses to be used as match criteria for the policy. Address sets are resolved to their individual names. • Destination Address—Displays the destination addresses (or address sets) to be used as match criteria for the policy. Addresses are entered as specified in the destination zone's address book. • Source Name—Displays the source name of the log. • User —Displays the user name from whom the log is generated. • Role—Displays the role names associated with the event. • Reason —Displays the reason for the log generation. For example, a connection tear down may have an associated reason such as authentication failed. • Profile—Displays the profile name in the log. • Protocol—Displays the protocol in the log. • Category—Displays the category of the log. <p>Select the criteria or parameter on which you want to construct the filter statement.</p> |

Table 28: Antispam—Fields on the Grid View Page (*continued*)

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

Table 28: Antispam—Fields on the Grid View Page (*continued*)

| Field | Description |
|----------------------|--|
| Source Country | Displays the source country of the log. |
| Source IP | Displays the source IP address from where the event occurred. |
| Source Port | Displays the source port of the log. |
| Destination Country | Displays the destination country of the log. |
| Destination IP | Displays the destination IP address of the event. |
| Destination Port | Displays the destination port of the event. |
| Application | Displays the application name from which the events or logs are generated. |
| User name | Displays the user name from whom the log is generated. |
| Hostname | The host name in the log. |
| Service Name | The name of the application service. For example, FTP, HTTP, SSH, and so on. |
| Protocol ID | Displays the protocol ID in the log. |
| Policy name | Displays the policy name in the log. |
| Source Zone | User traffic received from the zone. |
| Destination Zone | Displays the destination zone of the log. |
| Nested Application | Displays the nested application in the log. |
| Roles | Role names associated with the event. |
| Reason | Displays the reason for the log generation. For example, a connection tear down may have an associated reason such as authentication failed. |
| NAT Source Port | Displays the translated source port. |
| NAT Destination Port | Displays the translated destination port. |
| NAT Source Rule Name | Displays the NAT source rule name. |

Table 28: Antispam—Fields on the Grid View Page (continued)

| Field | Description |
|---------------------------|---|
| NAT Destination Rule Name | Displays the NAT destination rule name. |
| NAT Source IP | Displays the translated (or natted) source IP address. It can contain IPv4 or IPv6 addresses. |
| NAT Destination IP | Displays the translated (also called natted) destination IP address. |
| Traffic Session ID | Displays the traffic session ID of the log. 32 |
| URL | Displays the accessed URL name that triggered the event. |
| Object Name | Displays the object name of the log. |
| Path Name | Displays the path name of the log. |
| Logical System Name | Displays the name of the logical system. |
| Rule Name | Displays the rule name of the log. |
| Action | Displays the action taken for the event: warning, allow, and block. |
| Profile Name | Displays the profile name in the log. |
| Time | Displays the time when the log was received. |

Table 29: Antispam—Widgets on the Chart View Page

| Field | Description |
|-------------|---|
| Top Sources | Top five source IP addresses of the network traffic; sorted by event count. |

RELATED DOCUMENTATION

[Monitor Antivirus Events](#) | 91

Monitor Antivirus Events

You are here: **Monitor > Events > Antivirus.**

Use the monitoring functionality to view the Antivirus page.

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

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

- **Grid View**—View the comprehensive details of Antivirus events in a tabular format that includes sortable columns. You can group the events using the Group By option. For example, you can group the events based on source country. The table includes information such as the event name, UTM category, source IP address, source country, and so on. [Table 30 on page 91](#) describes the fields on the Grid View page.
- **Chart View**—View a brief summary of all the Antivirus events in your network. The top of the page has a swim lane graph of all the screen events. You can use the widgets at the bottom of the page to view critical information such as, top sources, top source countries, top destinations, and top destination countries. [Table 31 on page 94](#) describes the widgets on the Chart View page.

Table 30: Antivirus—Fields on the Grid View Page

| Field | Description |
|---------------|---|
| Search filter | <p>Select one of the filters from the list. Enter the relevant data for the search and click Go:</p> <ul style="list-style-type: none">• Event Name—Displays the event name of the log.• Source Address—Displays the source addresses to be used as match criteria for the policy. Address sets are resolved to their individual names.• Destination Address—Displays the destination addresses (or address sets) to be used as match criteria for the policy. Addresses are entered as specified in the destination zone’s address book.• Source Name—Displays the source name of the log.• User —Displays the user name from whom the log is generated.• Role—Displays the role names associated with the event.• Reason—Displays the reason for the log generation. For example, a connection tear down may have an associated reason such as authentication failed.• Profile—Displays the profile name in the log.• Protocol—Displays the protocol in the log.• Category—Displays the category of the log. <p>Select the criteria or parameter on which you want to construct the filter statement.</p> |

Table 30: Antivirus—Fields on the Grid View Page (*continued*)

| Field | Description |
|---|---|
| Text box | <p>Displays the filter parameter that you selected from the filter list.</p> <p>NOTE: In the filter statement the following limitation exists.</p> <ul style="list-style-type: none"> • You can use only one operator at a time. • You can use only one instance of the criteria or parameter in one filter statement. <p>For example, if you have used & operator and the parameter Event-Name once, I cannot use them again in the same filter statement</p> <p>CORRECT USAGE: Event-Name = rt_flow_session_close & application=TELNET</p> <p>WRONG USAGE: event name = rt_flow_session_close & event-name = rt_flow_session_create</p> <p>WRONG USAGE: event name = rt_flow_session_close & source-address = x.x.x.x & application = TELNET</p> <p>NOTE: The filter statement is NOT case-sensitive.</p> |
| Go | Executes the filter statement that is displayed in the text box. |
| X | Clears the filters. |
| Show Hide Column Filter icon represented by three vertical dots | Enables you to show or hide a column in the grid. |
| Threat Severity | Displays the severity level of the threat. |
| Event Name | Displays the event name of the log. |
| Description | Displays the description of the log. |
| Attack Name | Displays the attack name of the log. |
| UTM Category or Virus Name | Displays the UTM category or name of the virus. |
| Event Category | Displays the event category of the log. |
| Source Country | Displays the source country of the log. |
| Source IP | Displays the source IP address from where the event occurred. |

Table 30: Antivirus—Fields on the Grid View Page (*continued*)

| Field | Description |
|---------------------------|--|
| Source Port | Displays the source port of the event. |
| Destination Country | Displays the destination country of the log. |
| Destination IP | Displays the destination IP address of the event. |
| Destination Port | Displays the destination port of the event. |
| Application | Displays the application name from which the events or logs are generated. |
| User name | Displays the user name from whom the log is generated. |
| Host name | The host name in the log. |
| Service Name | The name of the application service. For example, FTP, HTTP, SSH, and so on. |
| Protocol ID | Displays the protocol ID in the log. |
| Policy name | Displays the policy name in the log. |
| Source Zone | User traffic received from the zone. |
| Destination Zone | Displays the destination zone of the log. |
| Nested Application | Displays the nested application in the log. |
| Roles | Role names associated with the event. |
| Reason | Displays the reason for the log generation. For example, a connection tear down may have an associated reason such as authentication failed. |
| NAT Source Port | Displays the translated source port. |
| NAT Destination Port | Displays the translated destination port. |
| NAT Source Rule Name | Displays the NAT source rule name. |
| NAT Destination Rule Name | Displays the NAT destination rule name. |
| NAT Source IP | Displays the translated (or natted) source IP address. It can contain IPv4 or IPv6 addresses. |

Table 30: Antivirus—Fields on the Grid View Page (*continued*)

| Field | Description |
|---------------------|--|
| NAT Destination IP | Displays the translated (also called natted) destination IP address. |
| Traffic Session ID | Displays the traffic session ID of the log. |
| URL | Displays the accessed URL name that triggered the event. |
| Object Name | Displays the object name of the log. |
| Path Name | Displays the path name of the log. |
| Logical System Name | Displays the name of the logical system. |
| Rule Name | Displays the rule name of the log. |
| Action | Displays the action taken for the event: warning, allow, and block. |
| Profile Name | Displays the profile name in the log. |
| Time | Displays the time when the log was received. |

Table 31: Antivirus—Widgets on the Chart View Page

| Field | Description |
|------------------|---|
| Top Sources | Displays the top five source IP addresses of the network traffic; sorted by event count. |
| Top Destinations | Displays the top five destination IP addresses of the network traffic; sorted by event count. |
| Top Viruses | Displays the top five viruses of the network traffic. |

RELATED DOCUMENTATION

[Monitor IPS Events](#) | 95

Monitor IPS Events

You are here: **Monitor > Events > IPS.**

Use the monitoring functionality to view the IPS page.

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

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

- **Grid View**—View the comprehensive details of IPS events in a tabular format that includes sortable columns. You can group the IPS events using the Group By option. For example, you can group the events based on source country. The table includes information such as the event name, UTM category, source IP address, source country, and so on. [Table 32 on page 95](#) describes the fields on the Grid View page.
- **Chart View**—View a brief summary of all the IPS events in your network. The top of the page has a swim lane graph of all the IPS events. You can use the widgets at the bottom of the page to view critical information such as, top sources, top source countries, top destinations, and top destination countries. [Table 33 on page 98](#) describes the widgets on the Chart View page.

Table 32: IPS—Fields on the Grid View Page

| Field | Description |
|--|---|
| The filter list that is displayed above the grids. | <p>Options available in the filter list are:</p> <ul style="list-style-type: none"> • Event Name—Displays the event name of the log. • Source Address—Displays the source addresses to be used as match criteria for the policy. Address sets are resolved to their individual names. • Destination Address—Displays the destination addresses (or address sets) to be used as match criteria for the policy. Addresses are entered as specified in the destination zone's address book. • Application—Displays the application name from which the events or logs are generated. • Rule Name—Displays the rule name of the log. • Threat Severity—Displays the severity level of the threat. • Attack Name—Displays the attack name of the log. <p>Select the criteria or parameter on which you want to construct the filter statement.</p> |

Table 32: IPS—Fields on the Grid View Page (*continued*)

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

Table 32: IPS—Fields on the Grid View Page (*continued*)

| Field | Description |
|----------------------|--|
| Source Country | Displays the source country of the log. |
| Source IP | Displays the source IP address from where the event occurred. |
| Source Port | Displays the source port of the event. |
| Destination Country | Displays the destination country of the log. |
| Destination IP | Displays the destination IP address of the event. |
| Destination Port | Displays the destination port of the event. |
| Application | Displays the application name from which the events or logs are generated. |
| User name | Displays the user name from whom the log is generated. |
| Hostname | The host name in the log. |
| Service Name | The name of the application service. For example, FTP, HTTP, SSH, and so on. |
| Protocol ID | Displays the protocol ID in the log. |
| Policy name | Displays the policy name in the log. |
| Source Zone | User traffic received from the zone. |
| Destination Zone | Displays the destination zone of the log. |
| Nested Application | Displays the nested application in the log. |
| Roles | Role names associated with the event. |
| Reason | Displays the reason for the log generation. For example, a connection tear down may have an associated reason such as authentication failed. |
| NAT Source Port | Displays the translated source port. |
| NAT Destination Port | Displays the translated destination port. |
| NAT Source Rule Name | Displays the NAT source rule name. |

Table 32: IPS—Fields on the Grid View Page (*continued*)

| Field | Description |
|---------------------------|---|
| NAT Destination Rule Name | Displays the NAT destination rule name. |
| NAT Source IP | Displays the translated (or natted) source IP address. It can contain IPv4 or IPv6 addresses. |
| NAT Destination IP | Displays the translated (also called natted) destination IP address. |
| Traffic Session ID | Displays the traffic session ID of the log. 32 |
| URL | Displays the accessed URL name that triggered the event. |
| Object Name | Displays the object name of the log. |
| Path Name | Displays the path name of the log. |
| Logical System Name | Displays the name of the logical system. |
| Rule Name | Displays the rule name of the log. |
| Action | Displays the action taken for the event: warning, allow, and block. |
| Profile Name | Displays the profile name in the log. |
| Time | Displays the time when the log was received. |

Table 33: IPS—Widgets on the Chart View Page

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

RELATED DOCUMENTATION

| [Monitor Screen Events](#) | 99

Monitor Screen Events

You are here: **Monitor** > **Events** > **Screen**.

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

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

- **Grid View**—View the comprehensive details of all screen events in a tabular format that includes sortable columns. You can group the events using the Group By option. For example, you can group the events based on source country. The table includes information such as the event name, source country, source address, destination country, attack name, and so on. [Table 34 on page 99](#) describes the fields on the Grid View page.
- **Chart View**—View a brief summary of all the screen events in your network. The top of the page has a swim lane graph of all the screen events. You can use the widgets at the bottom of the page to view critical information such as, top screen attackers, top screen victims, and top screen hits. [Table 35 on page 100](#) describes the widgets on the Chart View page.

Table 34: Screen—Fields on the Grid View Page

| Field | Description |
|--|---|
| The filter list that is displayed above the grids. | <p>Options available in the filter list are:</p> <ul style="list-style-type: none">• Event Name—Displays the event name of the log.• Source Address—Displays the source addresses to be used as match criteria for the policy. Address sets are resolved to their individual names.• Destination Address—Displays the destination addresses (or address sets) to be used as match criteria for the policy. Addresses are entered as specified in the destination zone's address book.• Attack Name—Displays the attack name of the log. <p>Select the criteria or parameter on which you want to construct the filter statement.</p> |
| Go | <p>Executes the filter statement that is displayed in the text box.</p> <p>Click Go.</p> |

Table 34: Screen—Fields on the Grid View Page (continued)

| Field | Description |
|---|--|
| X | Clears the filters. Click X. |
| Show Hide Column Filter icon represented by three vertical dots | Enables you to show or hide a column in the grid. |
| Timestamp | Displays the time when the log was received. |
| Event Name | Displays the event name of the log. |
| Source Country | Displays the source country of the log. |
| Source Address | Displays the source address from where the event occurred. |
| Destination Country | Displays the destination country of the log. |
| Destination Address | Displays the destination address of the event. |
| Destination Port | Displays the destination port of the event. |
| Source Port | Displays the source port of the event. |
| Description | Displays brief description of the event. |
| Source Zone Name | Displays the name of the source security zone of the traffic that triggered the event. |
| Host Name | Displays the host name of the device where the log was generated. |
| Action | Displays the action taken for the event. For example, warning, allow, and block. |
| Interface Name | Displays the name of the interface. |
| Domain | Displays the network or subnetwork to which the device belongs. |

Table 35: Screen—Widgets on the Chart View Page

| Field | Description |
|----------------------|--|
| Top Screen Attackers | Displays the top source countries from where the event source originated; sorted by the number of source IP addresses. |

Table 35: Screen—Widgets on the Chart View Page (*continued*)

| Field | Description |
|--------------------|---|
| Top Screen Victims | Displays the top destination countries targeted for the attack; sorted by the number of destination IP addresses. |
| Top Screen Hits | Displays the top source IP addresses of the network traffic; sorted by the number of event occurrences. |

RELATED DOCUMENTATION

[Monitor Security Intelligence Events](#) | 101

Monitor Security Intelligence Events

You are here: **Monitor** > **Events** > **Security Intelligence**.

Use the monitoring functionality to view the Security Intelligence page.

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

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

- **Grid View**—View the comprehensive details of security intelligence events in a tabular format that includes sortable columns. You can group the events using the Group By option. For example, you can group the events based on source country. The table includes information such as the event name, source address, source country, destination country, and so on. [Table 36 on page 102](#) describes the fields on the Grid View page.
- **Chart View**—View a brief summary of all the security intelligence events in your network. The top of the page has a swim lane graph of all the security intelligence events. You can use the widgets at the bottom of the page to view critical information such as, top compromised host and top C&C Servers. [Table 37 on page 103](#) describes the widgets on the Chart View page.

Table 36: Security Intelligence—Fields on the Grid View Page

| Field | Description |
|---|---|
| The filter is that is displayed above the grids. | <p>Options available in the filter list are:</p> <ul style="list-style-type: none"> • Event Name—Displays the event name of the log. • Source Address—Displays the source addresses to be used as match criteria for the policy. Address sets are resolved to their individual names. • Destination Address—Displays the destination addresses (or address sets) to be used as match criteria for the policy. Addresses are entered as specified in the destination zone's address book. <p>Select the criteria or parameter on which you want to construct the filter statement.</p> |
| Go | <p>Executes the filter statement that is displayed in the text box.</p> <p>Click Go.</p> |
| X | <p>Clears the filters.</p> <p>Click X.</p> |
| Show Hide Column Filter icon represented by three vertical dots | Enables you to show or hide a column in the grid. |
| Timestamp | Displays the time when the log was received. |
| Event Name | Displays the event name of the log. |
| Source Country | Displays the source country of the log. |
| Source Address | Displays the source address from where the event occurred. |
| Destination Country | Displays the destination country of the log. |
| Destination Address | Displays the destination address of the event. |
| Destination Port | Displays the destination port of the event. |
| Source Port | Displays the source port of the event. |
| Description | Displays the description of the log. |
| Source Zone Name | Displays the name of log source zone. |

Table 36: Security Intelligence—Fields on the Grid View Page (*continued*)

| Field | Description |
|----------------|--|
| Host name | Displays the host name in the log. |
| Action | Displays the action taken on the communication (permitted or blocked). |
| Interface Name | Displays the name of the interface. |
| Domain | Displays the network or subnetwork to which the device belongs. |

Table 37: Security Intelligence—Widgets on the Chart View Page

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

RELATED DOCUMENTATION

[Monitor ATP Events](#) | 103

Monitor ATP Events

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

Use the monitoring functionality to view the ATP page.

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

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

- **Grid View**—View the comprehensive details of all Juniper Sky ATP events in a tabular format that includes sortable columns. You can group the events using the Group By option. For example, you can group the events based on source country. The table includes information such as the event name, source country,

source address, destination country, malware information, and so on. [Table 38 on page 104](#) describes the fields on the Grid View page.

- **Chart View**—View a brief summary of all the Juniper Sky ATP events in your network. The top of the page has a swim lane graph of all the Juniper Sky ATP events. You can use the widgets at the bottom of the page to view critical information such as, Top malware source countries, top infected file categories, and top malwares identified. [Table 39 on page 105](#) describes the widgets on the Chart View page.

Table 38: ATP—Fields on the Grid View Page

| Field | Description |
|---|---|
| The filter list that is displayed above the grids. | <p>Options available in the filter list are:</p> <ul style="list-style-type: none"> • Event Name—Displays the event name of the log. • Source Address—Displays the source addresses to be used as match criteria for the policy. Address sets are resolved to their individual names. • Destination Address—Displays the destination addresses (or address sets) to be used as match criteria for the policy. Addresses are entered as specified in the destination zone's address book. <p>Select the criteria or parameter on which you want to construct the filter statement.</p> |
| Go | <p>Executes the filter statement that is displayed in the text box.</p> <p>Click Go.</p> |
| X | <p>Clears the filters.</p> <p>Click X.</p> |
| Show Hide Column Filter icon represented by three vertical dots | Enables you to show or hide a column in the grid. |
| Timestamp | The time when the log was received. |
| Event Name | Event name of the log. |
| Source Country | Source country name from where the event originated. |
| Source Address | Source IP address from where the event occurred. |
| Destination Country | Destination country name from where the event occurred. |
| Destination Address | Destination IP address of the event. |

Table 38: ATP—Fields on the Grid View Page (*continued*)

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

Table 39: ATP—Widgets on the Chart View Page

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

RELATED DOCUMENTATION

| [Monitor System Events](#) | 105

Monitor System Events

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

Use the monitoring functionality to view the System page.

[Table 40 on page 106](#) summarizes key output fields under events filters.

[Table 41 on page 106](#) summarizes key output fields under events details.

Table 40: System—Fields on the Events Filter

| Field | Description |
|------------------------|---|
| System Log File | Specifies the name of the system log file that records errors and events. |
| Process | Specifies the system processes that generate the events to display. |
| Include archived files | Specifies to enable the option to include archived files. Select to enable. |
| Date from | Specifies the beginning date range to monitor. Set the date using the calendar pick tool. |
| To | Specifies the end of the date range to monitor. Set the date using the calendar pick tool. |
| Event ID | Specifies the specific ID of the error or event to monitor. |
| Description | Enter a description for the errors or events. |
| Search | Fetches the errors and events specified in the search criteria. |
| Reset | Clears the cache of errors and events that were previously selected. |

Table 41: System—Fields under Event Details

| Field | Description |
|---------|--|
| Process | Displays the system process that generated the error or event. |

Table 41: System—Fields under Event Details (*continued*)

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

RELATED DOCUMENTATION

[Monitor All Events](#) | 65

Users

IN THIS CHAPTER

- [Monitor Users](#) | 108

Monitor Users

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

Use this page to view information related to the bandwidth consumption and session establishment.

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 42 on page 108](#) 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 43 on page 109](#) describes the widgets on the Chart View page.

Table 42: 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. |
| Username | Name of a user. |
| Volume | Bandwidth consumption of the user. |
| Total Sessions | Total number of user sessions. |

Table 42: Users—Fields on the Grid View Page (*continued*)

| Field | Description |
|--------------|---|
| Applications | All the applications used by a user for the time range. |

Table 43: 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 period. |

RELATED DOCUMENTATION

| [Monitor Ports](#) | 47

Device

IN THIS CHAPTER

- [Monitor Chassis Information | 110](#)
- [Monitor Cluster Status | 112](#)
- [Monitor Cluster Statistics | 113](#)
- [Monitor Ethernet Switching | 115](#)
- [Monitor Voice ALGs—Summary | 117](#)
- [Monitor Voice ALGs—H323 | 118](#)
- [Monitor Voice ALGs—MGCP | 120](#)
- [Monitor Voice ALGs—SCCP | 123](#)
- [Monitor Voice ALGs—SIP | 125](#)
- [Monitor DS-Lite | 129](#)

Monitor Chassis Information

You are here: **Monitor** > **Device** > **Chassis Information**.

Use this page to view chassis properties, which includes status of hardware components on the device. This includes routing engine details and power, and fan tray details.

NOTE: J-Web also supports IOC4 and RE3 line cards for SRX5000 line of devices and SCB4 line cards for SRX5600 and SRX5800 devices.

[Table 44 on page 111](#) provides the routing engine details.

Table 44: Routing Engine Details

| Field | Description |
|--------|--|
| Master | <p>Displays information about the routing engine and the CPU load averages for the last 1, 5, and 15 minutes.</p> <p>It also includes the routing engine module, model number, version, part number, serial number, memory utilization, temperature, and start time.</p> |
| Backup | <p>Displays the routing engine module, model number, version, part number, serial number, memory utilization, temperature, and start time.</p> <p>It also displays the CPU load averages for the last 1, 5, and 15 minutes.</p> |

[Table 45 on page 111](#) provides the power and fan tray details.

Table 45: Power and Fan Tray Details

| Field | Description |
|-------|--|
| Power | Displays the names of the device's power supply units and their statuses. |
| Fan | <p>Displays the names of the device's fans and their speeds (normal or high).</p> <p>NOTE: The fan speeds is adjusted automatically according to the current temperature.</p> |

[Table 46 on page 111](#) provides the chassis component details.

Table 46: Chassis Component Details

| Field | Description |
|-------------------------|---|
| General | Displays the version number, part number, serial number, and description of the selected device component. |
| Temperature | Displays the temperature of the selected device component (if applicable). |
| Resource | Displays the state, total CPU DRAM, and start time of the selected device component (if applicable). |
| Sub-Component | Displays information about the device's sub-components (if applicable). Details include the sub-component's version, part number, serial number, and description. |
| Power Budget Statistics | Displays information about the SRX380 device power statistics information. |

RELATED DOCUMENTATION

| [Monitor Cluster Status](#) | 112

Monitor Cluster Status

You are here: **Monitor** > **Device** > **Cluster Status**.

Use this page to view the information of cluster status.

[Table 47 on page 112](#) provides the Cluster Status details.

Table 47: Cluster Status

| Field | Description |
|------------------------|--|
| Refresh Interval (sec) | Displays the time interval set for page refresh. Select the time interval from the list. |
| Refresh | Displays the option to refresh the page. |
| Cluster Status | |
| Redundancy Group | Displays the redundancy group specified for the chassis cluster. |
| Failover | Displays the failover options selected. <ul style="list-style-type: none"> • Counter—Displays the number of times chassis cluster failed. • Action—Displays the active tool for users to fail over chassis cluster. |
| Primary | Displays the node used for the chassis cluster. |
| Switch | Provides an option to switch between the primary and secondary nodes. |
| Status | Displays the state of the redundancy group for node 0 and node 1. The possible states are: <ul style="list-style-type: none"> • Primary—Redundancy group is active and passing traffic. • Secondary—Redundancy group is passive and not passing traffic. • Lost—Node loses contact with the other node through the control link. Most likely to occur when both nodes are in a cluster one node is rebooted, or, because of a control link failure, one node cannot exchange heartbeats with the other node. • Unavailable—Node has not received a single heartbeat over the control link from the other node since the other node booted up. Most likely to occur when one node boots up before the other node or if only one node is present in the cluster. |

Table 47: Cluster Status (*continued*)

| Field | Description |
|-----------------------------|--|
| Preempt | Displays the preempt option selected to initiate a failover for node 0 and 1. The possible preempt options are: <ul style="list-style-type: none"> • Yes—Primary role can be preempted based on priority. • No—Primary role cannot be preempted if the priority changes. |
| Manual Failover | Displays the priority value of node 0 for manual failover. The possible manual failover options are: <ul style="list-style-type: none"> • Yes—If the primary role is set manually, it overrides the Priority and Preempt options. • No—Primary role is not set manually. |
| Interface Monitoring | |
| I/F | Displays the interfaces monitored by the redundancy group and shows their respective weights. |
| Weight | Displays the weight for the interface to be monitored. |
| Status | Displays the status of the interface. |

RELATED DOCUMENTATION

[Monitor Cluster Statistics](#) | 113

Monitor Cluster Statistics

You are here: **Monitor** > **Device** > **Cluster Statistics**.

Use this page to view the information of cluster status.

[Table 48 on page 113](#) provides the Cluster Statistics details.

Table 48: Cluster Statistics

| Field | Description |
|--------------------------------|-------------|
| Control Link Statistics | |

Table 48: Cluster Statistics (*continued*)

| Field | Description |
|-------------------------------|---|
| Control Link Statistics | Displays the Statistics of the control link used by chassis cluster traffic. Statistics for Control link 1 are displayed when you use dual control links (SRX5000 line of devices only). |
| Heartbeat packets sent | Displays the Number of heartbeat messages sent on the control link. |
| Heartbeat packets received | Displays the number of heartbeat messages received on the control link. |
| Heartbeat packet errors | Displays the number of heartbeat packets received with errors on the control link. |
| Fabric Link Statistics | |
| Fabric Link Statistics | Displays the statistics of the fabric link used by chassis cluster traffic. Statistics for Child Link 1 are displayed when you use dual fabric links. |
| Probes sent | Displays the number of probes sent on the fabric link. |
| Probes received | Displays the number of probes received on the fabric link. |
| Services Synchronized | |
| Service name | Displays the name of the service. |
| Rtos sent | Displays the number of runtime objects (RTOs) sent. |
| Rtos received | Displays the number of RTOs received. |
| Translation context | Displays the messages synchronizing Network Address Translation (NAT) translation context. |
| Incoming NAT | Displays the messages synchronizing incoming Network Address Translation (NAT) service. |
| Resource manager | Displays the messages synchronizing resource manager groups and resources. |
| Session create | Displays the messages synchronizing session creation. |
| Session close | Displays the messages synchronizing session close. |
| Session change | Displays the messages synchronizing session change. |

Table 48: Cluster Statistics (*continued*)

| Field | Description |
|--------------------------------|--|
| Gate create | Displays the messages synchronizing creation of pinholes (temporary openings in the firewall). |
| Session ageout refresh request | Displays the messages synchronizing request session after age-out. |
| Session ageout refresh reply | Displays the messages synchronizing reply session after age-out. |
| IPsec VPN | Displays the messages synchronizing VPN session. |
| Firewall user authentication | Displays the messages synchronizing firewall user authentication session. |
| MGCP ALG | Displays the messages synchronizing MGCP ALG sessions. |
| H323 ALG | Displays the messages synchronizing H.323 ALG sessions. |
| SIP ALG | Displays the messages synchronizing SIP ALG sessions. |
| SCCP ALG | Displays the messages synchronizing SCCP ALG sessions. |
| PPTP ALG | Displays the messages synchronizing PPTP ALG sessions. |
| RTSP ALG | Displays the messages synchronizing RTSP ALG sessions. |
| MAC address learning | Displays the messages synchronizing MAC address learning. |

RELATED DOCUMENTATION

[Monitor Ethernet Switching](#) | 115

Monitor Ethernet Switching

You are here: **Monitor** > **Device** > **Ethernet Switching**.

Use this page to view chassis properties, which includes status of hardware components on the device. This includes routing engine details and power, and fan tray details.

NOTE: This option is not available for SRX5000 line of devices, SRX4200, and SRX4600 devices.

Table 49 on page 116 provides the Ethernet Switching details.

Table 49: Ethernet Switching

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

RELATED DOCUMENTATION

Monitor Voice ALGs—Summary | 117

Monitor Voice ALGs—Summary

You are here: **Monitor** > **Device** > **Voice ALGs** > **Summary**.

Use this page to view information related to voice ALG summary.

[Table 50 on page 117](#) describes the fields on the Summary page.

Table 50: Fields on the Summary Page

| Field | Description |
|----------------------------|---|
| Refresh Interval (30 sec) | Displays the time interval set for page refresh. Select the time interval from the list. |
| Refresh | Click the refresh icon at the top right corner to display the option to refresh the page. |
| Protocol Name | Displays the protocols configured. |
| Total Calls | Displays the total number of calls. |
| Number of Active Calls | Displays the number of active calls. |
| Number of Received Packets | Displays the number of packets received. |
| Number of Errors | Displays the number of errors. |
| H.323 Calls Chart | Displays the H.323 calls chart. |
| MGCP Calls Chart | Displays the MGCP calls chart. |
| SCCP Calls Chart | Displays the SCCP calls chart. |
| SIP Calls Chart | Displays the SIP calls chart. |

RELATED DOCUMENTATION

[Monitor Voice ALGs—H323](#) | 118

Monitor Voice ALGs—H323

You are here: **Monitor** > **Device** > **Voice ALGs** > **H323**.

Use this page to view counter summary, error counter, counter summary chart and message counter of H323.

[Table 51 on page 118](#) describes the fields on the H323 page.

Table 51: Fields on the H323 Page

| Field | Description |
|---------------------------|---|
| Refresh Interval (30 sec) | Displays the time interval set for page refresh. Select the time interval from the list. |
| Refresh | Click the refresh icon at the top right corner to display the option to refresh the page. |
| Clear | Provides an option to clear the monitor summary. Click clear to clear the monitor summary. |

H323 Counters Summary

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

H.323 Error Counter

Table 51: Fields on the H323 Page (*continued*)

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

Counter Summary Chart

| | |
|------------------|--|
| Packets Received | Provides the graphical representation of the packets received. |
|------------------|--|

H.323 Message Counter

| | |
|----------|--|
| Category | <p>Displays the following categories:</p> <ul style="list-style-type: none"> • RRQ—Registration Request message counter. • RCF—Registration Confirmation Message. • ARQ—Admission Request message counter. • ACF—Admission Confirmation. • URQ—Unregistration Request. • UCF—Unregistration Confirmation. • DRQ—Disengage Request. • DCF—Disengage Confirmation. • Oth RAS—Other incoming Registration, Admission, and Status messages message counter. • Setup—Timeout value, in seconds, for the response of the outgoing setup message. • Alert—Alert message type. • Connect—Connect setup process. • CallProd—Number of call production messages sent. • Info—Number of info requests sent. • RelCmpl—Number of Rel Cmpl message sent. • Facility—Number of facility messages sent. • Empty—Empty capabilities to the support message counter. • OLC—Open Local Channel message counter. • OLC ACK—Open Local Channel Acknowledge message counter. • Oth H245—Other H.245 message counter |
|----------|--|

Table 51: Fields on the H323 Page (*continued*)

| Field | Description |
|-------|---|
| Count | Provides count of response codes for each H.323 message counter category. |

RELATED DOCUMENTATION

| [Monitor Voice ALGs—MGCP](#) | 120

Monitor Voice ALGs—MGCP

You are here: **Monitor** > **Device** > **Voice ALGs** > **MGCP**.

Use this page to view counters and calls of voice ALG MGCP.

[Table 52 on page 120](#) describes the fields on the MGCP page.

Table 52: Fields on the MGCP Page

| Field | Description |
|---------------------------|---|
| Refresh Interval (30 sec) | Displays the time interval set for page refresh. Select the time interval from the list. |
| Refresh | Click the refresh icon at the top right corner to display the option to refresh the page. |
| Clear | Provides an option to clear the monitor summary. Click Clear to clear the monitor summary. |

Counters—MGCP Counters Summary

Table 52: Fields on the MGCP Page (*continued*)

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

Counters—MGCP Error Counter

| | |
|------------------------|---|
| Category | <p>Displays the following categories:</p> <ul style="list-style-type: none"> • Unknown-method—MGCP ALG unknown method errors. • Decoding error—MGCP ALG decoding errors. • Transaction error—MGCP ALG transaction errors. • Call error—MGCP ALG call counter errors. • Connection error—MGCP ALG connection errors. • Connection flood drop—MGCP ALG connection flood drop errors. • Message flood drop—MGCP ALG message flood drop error. • IP resolve error—MGCP ALG IP address resolution errors. • NAT error—MGCP ALG NAT errors. • Resource manager error—MGCP ALG resource manager errors. • DSCP Marked error—MGCP ALG DSCP marked errors. |
| Count | Provides the count of response codes for each summary error counter category. |
| Counters Summary Chart | Displays the Counter Summary Chart. |

Counters—MGCP Packet Counters

Table 52: Fields on the MGCP Page (*continued*)

| Field | Description |
|---------------|---|
| Category | <p>Displays the following categories:</p> <ul style="list-style-type: none"> • CRCX—Create Connection • MDCX—Modify Connection • DLCX—Delete Connection • AUEP—Audit Endpoint • AUCX—Audit Connection • NTFY—Notify MGCP • RSIP—Restart in Progress • EPCF—Endpoint Configuration • RQNT—Request for Notification • 000-199—Respond code is 0-199 • 200-299—Respond code is 200-299 • 300-399—Respond code is 300-399 |
| Count | Provides count of response codes for each MGCP packet counter category. |
| Calls | |
| Endpoint@GW | Displays the endpoint name. |
| Zone | <p>Displays the following options:</p> <ul style="list-style-type: none"> • trust—Trust zone. • untrust—Untrust zone. |
| Endpoint IP | Displays the endpoint IP address. |
| Call ID | Displays the call identifier for ALG MGCP. |
| RM Group | Displays the resource manager group ID. |
| Call Duration | Displays the duration for which connection is active. |
| Refresh | Click the refresh icon at the top right corner to display the option to refresh the page. |
| Show | Click the icon to display the content. |

RELATED DOCUMENTATION

| [Monitor Voice ALGs—SCCP](#) | 123

Monitor Voice ALGs—SCCP

You are here: **Monitor** > **Device** > **Voice ALGs** > **SCCP**.

Use this page to view counters and calls of voice ALG SCCP.

[Table 53 on page 123](#) describes the fields on the SCCP page.

Table 53: Fields on the SCCP Page

| Field | Description |
|---------------------------|--|
| Refresh Interval (30 sec) | Displays the time interval set for page refresh. Select the time interval from the list. |
| Refresh | Click the refresh icon at the top right corner to display the option to refresh the page. |
| Clear | Provides an option to clear the monitor summary. Click Clear to clear the monitor summary. |

Counters—SCCP Call Statistics

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

Counters—SCCP Error Counters

Table 53: Fields on the SCCP Page (*continued*)

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

RELATED DOCUMENTATION

Monitor Voice ALGs—SIP

You are here: **Monitor** > **Device** > **Voice ALGs** > **SIP**.

Use this page to view counters and calls of voice ALG SIP.

[Table 54 on page 125](#) describes the fields on the SIP page.

Table 54: Fields on the SIP Page

| Field | Description |
|------------------------------|--|
| Refresh Interval (30 sec) | Displays the time interval set for page refresh. Select the time interval from the list. |
| Refresh | Displays the option to refresh the page. |
| Clear | Provides an option to clear the monitor summary. Click Clear to clear the monitor summary. |

Counters—SIP Counters Information

Table 54: Fields on the SIP Page (*continued*)

| Field | Description |
|--------|--|
| Method | <p>Displays the SIP counter information. The available options are:</p> <ul style="list-style-type: none"> • BYE—Number of BYE requests sent. A user sends a BYE request to abandon a session. A BYE request from either user automatically terminates the session. • REGISTER—Number of REGISTER requests sent. A user sends a REGISTER request to a SIP registrar server to inform it of the current location of the user. The SIP registrar server records all the information it receives in REGISTER requests and makes this information available to any SIP server attempting to locate a user. • OPTIONS—Number of OPTIONS requests sent. An OPTION message is used by the User Agent (UA) to obtain information about the capabilities of the SIP proxy. A server responds with information about what methods, session description protocols, and message encoding it supports. • INFO—Number of INFO requests sent. An INFO message is used to communicate mid-session signaling information along the signaling path for the call. • MESSAGE—Number of MESSAGE requests sent. SIP messages consist of requests from a client to the server and responses to the requests from the server to a client for the purpose of establishing a session (or a call). • NOTIFY— Number of NOTIFY requests sent. A NOTIFY message – is sent to inform subscribers about the change in state of the subscription. • PRACK—Number of PRACK requests sent. The PRACK request plays the same role as the ACK request, but for provisional responses. • PUBLISH—Number of PUBLISH requests sent. The PUBLISH request is used for publishing the event state. PUBLISH is similar to REGISTER that allows a user to create, modify, and remove state in another entity which manages this state on behalf of the user. • REFER—Number of REFER requests sent. A REFER request is used to refer the recipient (identified by the Request-URI) to a third party identified by the contact information provided in the request. • SUBSCRIBE—Number of SUBSCRIBE requests sent. A SUBSCRIBE request is used to request current state and state information updates from a remote node. • UPDATE—Number of UPDATE requests sent. An UPDATE request is used to create a temporary opening in the firewall (pinhole) for new or updated Session Description Protocol (SDP) information. The following header fields are modified: Via, From, To, Call-ID, Contact, Route, and Record-Route. • BENOTIFY—Number of BENOTIFY requests sent. A BENOTIFY request is used to reduce the unnecessary SIP signaling traffic on application servers. Applications that do not need a response for a NOTIFY request can enhance performance by enabling BENOTIFY. • SERVICE—Number of SERVICE requests sent. The SERVICE method is used by a SIP client to request a service from a SIP server. It is a standard SIP message and will be forwarded until it reaches the server or end user that is performing the service. • OTHER—Number of OTHER requests sent. |
| T, RT | Displays the transmit and retransmit method. |

Table 54: Fields on the SIP Page (*continued*)

| Field | Description |
|---------------------------|--|
| 1xx, RT | Displays one transmit and retransmit method. |
| 2xx, RT | Displays two transmit and retransmit methods. |
| 3xx, RT | Displays three transmit and retransmit methods. |
| 4xx, RT | Displays four transmit and retransmit methods. |
| 5xx, RT | Displays five transmit and retransmit methods. |
| 6xx, RT | Displays six transmit and retransmit methods. |
| Calls | |
| Call ID | Displays the call ID. |
| Method | Displays the call method used. |
| State | Displays the state of the ALG SIP. |
| Group ID | Displays the group identifier. |
| Show | Enables you to show the hidden content. |
| Refresh | Click the refresh icon at the top right corner to refresh the content. |
| SIP Error Counters | |
| Invite Method Chart | <p>Displays the invite method chart. The available options are:</p> <ul style="list-style-type: none"> • T/RT • 1xx/ RT • 2xx/ RT • 3xx/ RT • 4xx/ RT • 5xx/ RT • 6xx/ RT |

Table 54: Fields on the SIP Page (*continued*)

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

RELATED DOCUMENTATION

[Monitor DS-Lite | 129](#)

Monitor DS-Lite

You are here: **Monitor** > **Device** > **DS-Lite**.

Use this page to view information related to DS-Lite page.

[Table 55 on page 129](#) describes the fields on the DS-Lite page.

Table 55: Fields on the DS-Lite Page

| Field | Description |
|--|---|
| Refresh Interval | Displays the time interval for page refresh. Select the time interval from the list. |
| Refresh | Click the refresh icon at the top right corner to display the fresh content. |
| General Info | |
| Name | Displays the name of the DS-Lite configuration. |
| Address | Displays the IP address of the device. |
| Status | Displays the status of the DS-Lite configuration. <ul style="list-style-type: none"> • Connected—DS-Lite configuration is connected. • Disconnected—DS-Lite configuration is not connected. |
| Num of software initiator | Displays the number of software initiators connected to the device. |
| Software Initiator from Selected Item | |
| Address | Displays the IP address of the software of the selected DS-Lite configuration. |
| Status | Displays the status of the software initiator. <ul style="list-style-type: none"> • Active—The software initiator is active. • Inactive—The software initiator is inactive. <p>The status types displayed are active and inactive.</p> |
| spu-id | Displays the identification number of the Services Processing Unit. |
| Show | Enables you to see the hidden content. |
| Refresh | Click the refresh icon at the top right corner to display the fresh content. |

RELATED DOCUMENTATION

| [Monitor Chassis Information](#) | 110

Routing

IN THIS CHAPTER

- [Monitor Route Information | 131](#)
- [Monitor RIP Information | 134](#)
- [Monitor OSPF Information | 135](#)
- [Monitor BGP Information | 138](#)

Monitor Route Information

You are here: **Monitor > Routing > Route Information.**

Use this page to view information about routes in a routing table, including destination, protocol, state, and parameter information.

[Table 56 on page 131](#) describes the fields on the Route Information page.

Table 56: Fields on the Route Information Page

| Field | Description |
|---------------------|---|
| Route Filter | |
| Destination Address | Specifies the destination address of the route. Enter the destination address. |
| Protocol | Specifies the protocol from which the route was learned. Enter the protocol name. |
| Next hop address | Specifies the network layer address of the directly reachable neighboring system (if applicable) and the interface used to reach it. Enter the next hop address. |

Table 56: Fields on the Route Information Page (*continued*)

| Field | Description |
|------------------------|--|
| Receive protocol | <p>Specifies the dynamic routing protocol using which the routing information was received through a particular neighbor.</p> <p>Enter the routing protocol.</p> |
| Best route | <p>Specifies only the best route available.</p> <p>Select the view details of the best route.</p> |
| Inactive routes | <p>Specifies the inactive routes.</p> <p>Select the view details of inactive routes.</p> |
| Exact route | <p>Specifies the exact route.</p> <p>Select the view details of the exact route.</p> |
| Hidden routes | <p>Specifies the hidden routes.</p> <p>Select the view details of hidden routes.</p> |
| Search | <p>Applies the specified filter and displays the matching messages.</p> <p>To apply the filter and display messages, click Search.</p> |
| Reset | <p>Resets selected options to default</p> <p>To reset the filter, click Reset.</p> |
| Route Table | |
| Static Route Addresses | The list of static route addresses. |
| Generate Report | Creates an HTML report based on the - specified parameters. |
| refresh | Click the refresh icon at the top right corner to display the fresh content. |
| Protocol | Protocol from which the route was learned: Static , Direct , Local , or the name of a particular protocol. |

Table 56: Fields on the Route Information Page (*continued*)

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

RELATED DOCUMENTATION

[Monitor RIP Information](#) | 134

Monitor RIP Information

You are here: **Monitor** > **Routing** > **RIP Information**.

Use this page to view RIP routing information, including a summary of RIP neighbors and statistics.

[Table 57 on page 134](#) describes the fields on the RIP Information page.

Table 57: Fields on the RIP Information Page

| Field | Description |
|--------------------------|---|
| RIP Neighbors | |
| Protocol Name | The RIP protocol name. |
| Port number | The port on which RIP is enabled. |
| Hold down time | The interval during which routes are neither advertised nor updated. |
| Global routes learned | Number of RIP routes learned on the logical interface. |
| Global routes hold down | Number of RIP routes that are not advertised or updated during the hold-down interval. |
| Global request dropped | Number of requests dropped. |
| Global responses dropped | Number of responses dropped. |
| RIP Statistics | |
| Details | Tab used to view the details of the interface on which RIP is enabled. |
| Neighbor | Name of the RIP neighbor. NOTE: This value is the name of the interface on which RIP is enabled. Click the name to see the details for this neighbor. |
| State | State of the RIP connection: Up or Dn (Down). |

Table 57: Fields on the RIP Information Page (*continued*)

| Field | Description |
|---------------------|---|
| Source Address | Local source address. This value is the configured address of the interface on which RIP is enabled. |
| Destination Address | Destination address. This value is the configured address of the immediate RIP adjacency. |
| Send Mode | The mode of sending RIP messages. |
| Receive Mode | The mode in which messages are received. |
| In Metric | Value of the in coming metric configured for the RIP neighbor. |

RELATED DOCUMENTATION

| [Monitor OSPF Information](#) | 135

Monitor OSPF Information

You are here: **Monitor** > **Routing** > **OSPF Information**.

Use this page to view OSPF routing information, including a summary of OSPF neighbors, interfaces, and statistics.

[Table 58 on page 135](#) describes the fields on the OSPF Information page.

Table 58: Fields on the OSPF Information Page

| Field | Description |
|------------------------|--|
| OSPF Interfaces | |
| Details | Tab used to view the details of the selected OSPF. |
| Interface | Name of the interface running OSPF. |

Table 58: Fields on the OSPF Information Page (*continued*)

| Field | Description |
|--------------------------------|--|
| State | <p>Displays one of the following State of the interface:</p> <ul style="list-style-type: none"> • BDR • Down • DR • DRother • Loop • PtToPt • Waiting <p>NOTE: The Down state, indicating that the interface is not functioning. The PtToPt state, indicating that a point-to-point connection has been established, are the most common states.</p> |
| Area | Number of the area that the interface is in. |
| DR ID | ID of the area's designated device. |
| BDR ID | ID of the area's backup designated device. |
| Neighbors | Number of neighbors on this interface. |
| OSPF Statistics—Packets | |
| Sent | Displays the total number of packets sent. |
| Received | Displays the total number of packets received. |
| OSPF Statistics—Details | |
| Flood Queue Depth | Number of entries in the extended queue. |
| Total Retransmits | Number of retransmission entries enqueued. |
| Total Database Summaries | Total number of database description packets. |
| OSPF Neighbors | |
| Address | Address of the neighbor. |
| Interface | Interface through which the neighbor is reachable. |

Table 58: Fields on the OSPF Information Page (*continued*)

| Field | Description |
|---------------|---|
| State | <p>Displays one of the following state of the neighbor:</p> <ul style="list-style-type: none"> • Attempt • Down • Exchange • ExStart • Full • Init • Loading • 2way <p>Generally, only the Down state, indicating a failed OSPF adjacency, and the Full state, indicating a functional adjacency, are maintained for more than a few seconds. The other states are transitional states that a neighbor is in only briefly while an OSPF adjacency is being established.</p> |
| ID | ID of the neighbor. |
| Priority | Priority of the neighbor to become the designated router. |
| Activity Time | The activity time. |
| Area | Area that the neighbor is in. |
| Options | Option bits received in the hello packets from the neighbor. |
| DR Address | Address of the designated router. |
| BDR Address | Address of the backup designated router. |
| Uptime | Length of time since the neighbor came up. |
| Adjacency | Length of time since the adjacency with the neighbor was established. |

RELATED DOCUMENTATION

Monitor BGP Information

You are here: **Monitor** > **Routing** > **BGP Information**.

Use this page to monitor BGP routing information on the routing device, including a summary of BGP routing and neighbor information.

[Table 59 on page 138](#) describes the fields on the BGP Information page.

Table 59: Fields on the BGP Information Page

| Field | Description |
|-------------------------|--|
| BGP Peer Summary | |
| Total Groups | Number of BGP groups. |
| Total Peers | Number of BGP peers. |
| Down Peers | Number of unavailable BGP peers. |
| Unconfigured Peers | Address of each BGP peer. |
| RIB Summary tab | |
| RIB Name | Name of the RIB group. |
| Total Prefixes | Total number of prefixes from the peer, both active and inactive, that are in the routing table. |
| Active Prefixes | Number of prefixes received from the EBGp peers that are active in the routing table. |
| Suppressed Prefixes | Number of routes received from EBGp peers currently inactive because of damping or other reasons. |
| History Prefixes | History of the routes received or suppressed. |
| Dumped Prefixes | Number of routes currently inactive because of damping or other reasons. These routes do not appear in the forwarding table and are not exported by routing protocols. |
| Pending Prefixes | Number of pending routes. |
| State | Status of the graceful restart process for this routing table: BGP restart is complete, BGP restart in progress, VPN restart in progress, or VPN restart is complete. |

Table 59: Fields on the BGP Information Page (*continued*)

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

RELATED DOCUMENTATION

[Monitor Route Information](#) | 131

Class of Service (CoS)

IN THIS CHAPTER

- [Monitor CoS Interfaces | 140](#)
- [Monitor Classifiers | 141](#)
- [Monitor CoS Value Aliases | 142](#)
- [Monitor RED Drop Profiles | 142](#)
- [Monitor Forwarding Classes | 143](#)
- [Monitor Rewrite Rules | 144](#)
- [Monitor Scheduler Maps | 145](#)

Monitor CoS Interfaces

You are here: **Monitor** > **Class of Service** > **Interfaces**.

Use this page to display details about the physical and logical interfaces and the CoS components assigned to them.

[Table 60 on page 140](#) describes the fields on the Interfaces page.

Table 60: Fields on the Interfaces Page

| Field | Description |
|------------------|--|
| Interface | Name of a physical interface to which CoS components are assigned. To display names of logical interfaces configured on this physical interface, click the plus sign (+). |
| Scheduler Map | Name of the scheduler map associated with this interface. |
| Queues Supported | Number of queues you can configure on the interface. |
| Queues in Use | Number of queues currently configured. |

RELATED DOCUMENTATION

| [Monitor Classifiers](#) | 141

Monitor Classifiers

You are here: **Monitor** > **Class of Service** > **Classifiers**.

Use this page to display the mapping of incoming CoS value to forwarding class and loss priority.

[Table 61 on page 141](#) describes the fields on the Classifiers page.

Table 61: Fields on the Classifiers Page

| Field | Description |
|----------------------------|---|
| Classifier Name | Name of a classifier. To display classifier assignments, click the plus sign (+). |
| CoS Value Type | The classifiers are displayed by type: <ul style="list-style-type: none">• dscp—All classifiers of the DSCP type.• dscp ipv6—All classifiers of the DSCP IPv6 type.• exp—All classifiers of the MPLS EXP type.• ieee-802.1—All classifiers of the IEEE 802.1 type.• inet-precedence—All classifiers of the IP precedence type. |
| Index | Internal index of the classifier. |
| Incoming CoS Value | CoS value of the incoming packets, in bits. These values are used for classification. |
| Assign to Forwarding Class | Forwarding class that the classifier assigns to an incoming packet. This class affects the forwarding and scheduling policies that are applied to the packet as it transits the device. |
| Assign to Loss Priority | Loss priority value that the classifier assigns to the incoming packet based on its CoS value. |

RELATED DOCUMENTATION

| [Monitor CoS Interfaces](#) | 140

Monitor CoS Value Aliases

You are here: **Monitor** > **Class of Service** > **CoS Value Aliases**.

Use this page to view information about routes in a routing table, including destination, protocol, state, and parameter information.

[Table 62 on page 142](#) describes the fields on the Value Aliases page.

Table 62: Fields on the CoS Value Aliases Page

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

RELATED DOCUMENTATION

[Monitor Classifiers](#) | [141](#)

Monitor RED Drop Profiles

You are here: **Monitor** > **Class of Service** > **RED Drop Profiles**.

Use this page to view information about routes in a routing table, including destination, protocol, state, and parameter information.

[Table 63 on page 143](#) describes the fields on the RED Drop Profiles page.

Table 63: Fields on the RED Drop Profiles Page

| Field | Description |
|-----------------------|---|
| RED Drop Profile Name | <p>Name of the RED drop profile.</p> <p>A drop profile consists of pairs of values between 0 and 100, one for queue buffer fill level and one for drop probability, that determine the relationship between a buffer's fullness and the likelihood it will drop packets.</p> <p>To display profile values, click the plus sign (+).</p> |
| Type | <p>Type of a specific drop profile:</p> <ul style="list-style-type: none"> • interpolated—The two coordinates (x and y) of the graph are interpolated to produce a smooth profile. • segmented—The two coordinates (x and y) of the graph are represented by line fragments to produce a segmented profile. |
| Index | Internal index of this drop profile. |
| Fill Level | Percentage fullness of a buffer queue. This value is the x coordinate of the RED drop profile graph. |
| Drop Probability | Drop probability of a packet corresponding to a specific queue buffer fill level. This value is the y coordinate of the RED drop profile graph. |

RELATED DOCUMENTATION

[Monitor Classifiers](#) | 141

Monitor Forwarding Classes

You are here: **Monitor** > **Class of Service** > **Forwarding Classes**.

Use this page to view the current assignment of CoS forwarding classes to queue numbers on the system.

[Table 64 on page 144](#) describes the fields on the Forwarding Classes page.

Table 64: Fields on the Forwarding Classes Page

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

RELATED DOCUMENTATION

[Monitor RED Drop Profiles](#) | 142

Monitor Rewrite Rules

You are here: **Monitor** > **Class of Service** > **Rewrite Rules**.

Use this page to view information about routes in a routing table, including destination, protocol, state, and parameter information.

[Table 65 on page 144](#) describes the fields on the Rewrite Rules page.

Table 65: Fields on the Rewrite Rules Page

| Field | Description |
|-------------------|-------------------------|
| Rewrite Rule Name | Names of rewrite rules. |

Table 65: Fields on the Rewrite Rules Page (*continued*)

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

RELATED DOCUMENTATION

[Monitor Forwarding Classes](#) | 143

Monitor Scheduler Maps

You are here: **Monitor** > **Class of Service** > **Scheduler Maps**.

Use this page to view information on assignments of CoS forwarding classes to schedulers.

[Table 66 on page 146](#) describes the fields on the Scheduler Maps page.

Table 66: Fields on the Scheduler Maps Page

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

Table 66: Fields on the Scheduler Maps Page *(continued)*

| Field | Description |
|-------------------|---|
| Protocol | Transport protocol corresponding to a drop profile. |
| Drop Profile Name | Name of the drop profile. |
| index | Internal index for this particular rewrite rule. |

RELATED DOCUMENTATION

| [Monitor Rewrite Rules](#) | 144

MPLS

IN THIS CHAPTER

- [Monitor MPLS Interfaces | 148](#)
- [Monitor LSP Information | 149](#)
- [Monitor LSP Statistics | 150](#)
- [Monitor RSVP Sessions | 151](#)
- [Monitor RSVP Interfaces | 153](#)

Monitor MPLS Interfaces

NOTE: This option is not available for SRX5000 and SRX4000 line of devices.

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

Use this page to view interfaces on which MPLS is configured, including operational state and any administrative groups applied to an interface.

[Table 67 on page 148](#) describes the fields on the Interfaces page.

Table 67: Fields on the MPLS Interfaces Page

| Field | Description |
|-----------------------|--|
| Interface | Name of the interface on which MPLS is configured. |
| State | State of the specified interface: Up or Dn (down). |
| Administrative groups | Administratively assigned colors of the MPLS link configured on the interface. |

RELATED DOCUMENTATION

Monitor LSP Information

You are here: **Monitor > MPLS > LSP Information.**

Use this page to view all label-switched paths configured on the services router, including all inbound, outbound, and transit LSP information.

Table 68 on page 149 describes the fields on the LSP Information page.

Table 68: Fields on the LSP Information Page

| Field | Description |
|-------------|--|
| Ingress LSP | Information about LSPs on the inbound device. Each session has one line of output. |
| Egress LSP | Information about the LSPs on the outbound device. Each session has one line of output. MPLS learns this information by querying RSVP, which holds all the transit and outbound session information. |
| Transit LSP | Number of LSPs on the transit routers and the state of these paths. MPLS learns this information by querying RSVP, which holds all the transit and outbound session information. |
| To | Destination (outbound device) of the session. |
| From | Source (inbound device) of the session. |
| State | State of the path. It can be Up, Down, or AdminDn. AdminDn indicates that the LSP is being taken down gracefully. |
| Rt | Number of active routes (prefixes) installed in the routing table. For inbound RSVP sessions, the routing table is the primary IPv4 table (inet.0). For transit and outbound RSVP sessions, the routing table is the primary MPLS table (mpls.0). |
| Active Path | Name of the active path: Primary or Secondary. This field is used for inbound LSPs only. |

Table 68: Fields on the LSP Information Page *(continued)*

| Field | Description |
|----------|---|
| P | An asterisk (*) in this column indicates that the This field is used for inbound LSPs only. This field is used for inbound LSPs only. |
| LSPname | Configured name of the LSP. |
| Style | RSVP reservation style. This field consists of two parts. The first is the number of active reservations. The second is the reservation style, which can be FF (fixed filter), SE (shared explicit), or WF (wildcard filter). This field is used for outbound and transit LSPs only. |
| Labelin | Incoming label for this LSP. |
| Labelout | Outgoing label for this LSP. |
| Total | Total number of LSPs displayed for the particular type—ingress (inbound), egress (outbound), or transit. |

RELATED DOCUMENTATION

| [Monitor MPLS Interfaces](#) | 148

Monitor LSP Statistics

You are here: **Monitor** > **MPLS** > **LSP Statistics**.

Use this page to view statistics for LSP sessions currently active on the device.

[Table 69 on page 150](#) describes the fields on the LSP Statistics page.

Table 69: Fields on the LSP Statistics Page

| Field | Description |
|-------------|--|
| Ingress LSP | Information about LSPs on the inbound device. Each session has one line of output. |

Table 69: Fields on the LSP Statistics Page (*continued*)

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

RELATED DOCUMENTATION

| [Monitor LSP Information](#) | 149

Monitor RSVP Sessions

You are here: **Monitor** > **MPLS** > **RSVP Sessions**.

Use this page to view information about RSVP-signaled LSP sessions currently active on the device, ingress and outbound egress addresses, LSP state, and LSP name.

[Table 70 on page 152](#) describes the fields on the RSVP Sessions page.

Table 70: Fields on the RSVP Sessions Page

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

RELATED DOCUMENTATION

Monitor RSVP Interfaces

You are here: **Monitor > MPLS > RSVP Interfaces.**

Use this page to view information about interfaces on which RSVP is enabled, including the interface name, total bandwidth through the interface.

[Table 71 on page 153](#) describes the fields on the RSVP Interfaces page.

Table 71: Fields on the RSVP Interfaces Page

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

RELATED DOCUMENTATION

DHCP

IN THIS CHAPTER

- [Monitor DHCP Server | 154](#)
- [Monitor DHCP Relay | 156](#)

Monitor DHCP Server

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

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

[Table 72 on page 154](#) describes the fields on the DHCP Server page.

Table 72: Fields on the DHCP Server Page

| Field | Description |
|---------------------|--|
| Routing Instance | Select the routing instance name. |
| Interface Details | Displays the interface on which the DHCP server is configured. |
| Clear All Bindings | Clears all the binding information. |
| Binding Information | |
| IP address | Displays the IP address of the DHCP server. |
| Session id | Displays the Session ID of the subscriber session. |
| Hardware address | Displays the Hardware address of the DHCP server. |
| Expires | Displays the number of seconds in which the lease expires. |

Table 72: Fields on the DHCP Server Page (*continued*)

| Field | Description |
|---|---|
| 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. |
| Interface | Displays the interface on which the request was received. |
| Statistics Information | |
| Message Counters - Sent | <p>Number of BOOTREPLY, DHCPPOFFER, DHCPACK, DHCPNAK, DHCPFORCERENEW, DHCPLEASEDUNASSIGNED, DHCPLEASEUNKNOWN, AND DHCPLEASEACTIVE messages sent from the DHCP server to DHCP clients.</p> <p>Displays these information in a bar chart.</p> |
| Message Counters - Received | <p>Number of BOOTREQUEST, DHCPDECLINE, DHCPDISCOVER, DHCPINFORM, DHCPRELEASE, DHCPREQUEST, DHCPLEASEQUERY, and DHCPBULKLEASE messages sent from DHCP clients and received by the DHCP server.</p> <p>Displays these information in a bar chart.</p> |
| Dropped Packet Counters - Total Dropped Packets | Displays the number of dropped packet counters in a pie chart. |
| Clear All Statistics | Clears all the collected statistical information. |

RELATED DOCUMENTATION

[Monitor DHCP Relay](#) | 156

Monitor DHCP Relay

You are here: **Monitor** > **DHCP** > **DHCP Relay**.

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

[Table 73 on page 156](#) describes the fields on the DHCP Relay page.

Table 73: Fields on the DHCP Relay Page

| Field | Description |
|----------------------------|--|
| Interface Details | Displays the interface on which the DHCP relay is configured. |
| Clear All Bindings | Clears all the binding information. |
| Routing Instance | Select the routing instance name. |
| Binding Information | |
| IP address | Displays the IP address of the DHCP relay. |
| Session id | Displays the Session ID of the subscriber session. |
| Hardware address | Displays the Hardware address of the DHCP relay. |
| Expires | Displays the number of seconds in which the lease expires. |
| 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. • FORCERENEW—Client has received the FORCERENEW message from the server. • INIT— Initial state. • RELEASE—Client is releasing the IP address lease. • RENEWING—Client is sending a request to renew the IP address lease. • REQUESTING—Client is requesting a DHCP server. • SELECTING—Client is receiving offers from DHCP servers. |
| Interface | Displays the interface on which the request was received. |

Table 73: Fields on the DHCP Relay Page (*continued*)

| Field | Description |
|-------------------------------|---|
| Statistics Information | |
| Message Counters - Sent | <p>Number of BOOTREPLY, DHCPPOFFER, DHCPACK, DHCPNAK, DHCPFORCERENEW, DHCPLEASEDUNASSIGNED, DHCPLEASEUNKNOWN, AND DHCPLEASEACTIVE messages sent from the DHCP server to DHCP clients.</p> <p>Displays these information in a bar chart.</p> |
| Message Counters - Received | <p>Number of BOOTREQUEST, DHCPDECLINE, DHCPDISCOVER, DHCPINFORM, DHCPRELEASE, DHCPREQUEST, DHCPLEASEQUERY, and DHCPBULKLEASE messages sent from DHCP clients and received by the DHCP server.</p> <p>Displays these information in a bar chart.</p> |
| Packet Counters - Dropped | Displays the number of dropped packet counters in a pie chart. |
| Packet Counters - Forwarded | Displays the number of forwarded packet counters in a pie chart. |
| Clear All Statistics | Clears all the collected statistical information. |

RELATED DOCUMENTATION

| [Monitor DHCP Server](#) | 154

NAT

IN THIS CHAPTER

- [Monitor Source NAT | 158](#)
- [Monitor Destination NAT | 164](#)
- [Monitor Static NAT | 166](#)
- [Monitor Interface NAT Ports | 168](#)

Monitor Source NAT

You are here: **Monitor > NAT > Source NAT.**

Use this page to view configured information about source Network Address Translation (NAT) rules, pools, persistent NAT, paired addresses, and resource usage.

[Table 74 on page 158](#) describes the fields on the Source NAT page.

Table 74: Fields on the Source NAT Page

| Field | Description |
|------------------|--|
| Rules | |
| Refresh Interval | Indicates the duration of time after which you want the data on the page to be refreshed. |
| Refresh | Click the refresh icon at the top right corner to display the fresh content. |
| Rule-set Name | Name of the rule set. Select all rule sets or a specific rule set to display from the list. |
| Total rules | Number of rules configured. |
| ID | Rule ID number. |

Table 74: Fields on the Source NAT Page (*continued*)

| Field | Description |
|--------------------------------|--|
| Name | Name of the rule. |
| From | Name of the routing instance/zone/interface from which the packet flows. |
| To | Name of the routing instance/zone/interface to which the packet flows. |
| Source address range | Source IP address range in the source pool. |
| Destination address range | Destination IP address range in the source pool. |
| Source ports | Source port numbers. |
| Ip protocol | IP protocol. |
| Action | Action taken for a packet that matches a rule. |
| Persistent NAT type | Persistent NAT type. |
| Inactivity timeout | Inactivity timeout interval for the persistent NAT binding. |
| Alarm threshold | Utilization alarm threshold. |
| Max session number | The maximum number of sessions. |
| Sessions (Succ/Failed/Current) | <p>Successful, failed, and current sessions.</p> <ul style="list-style-type: none"> • Succ—Number of successful session installations after the NAT rule is matched. • Failed—Number of unsuccessful session installations after the NAT rule is matched. • Current—Number of sessions that reference the specified rule. |
| Translation Hits | Number of times a translation in the translation table is used for a source NAT rule. |
| Refresh | Click the refresh icon at the top right corner to display the fresh content. |
| Top 10 Translation Hits | |
| Graph | Displays the graph of top 10 translation hits. |

Table 74: Fields on the Source NAT Page (*continued*)

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

Table 74: Fields on the Source NAT Page (continued)

| Field | Description |
|---|--|
| FPC PIC ID | Displays the FPC PIC ID. |
| NOTE: This option is available for SRX4000 and SRX5000 lines of devices. | |
| binding total | Displays the total number of persistent NAT bindings for the FPC. |
| binding in use | Number of persistent NAT bindings that are in use for the FPC. |
| enode total | Total number of persistent NAT enodes for the FPC. |
| enode in use | Number of persistent NAT enodes that are in use for the FPC. |
| Persistent NAT table | |
| Source NAT pool | Name of the pool. Select all pools or a specific pool to display from the list. |
| Internal IP | Internal IP address. Select all IP addresses or a specific IP address to display from the list. |
| Internal port | Displays the internal ports configured in the system. Select the port to display from the list. |
| Internal protocol | Internal protocols. Select all protocols or a specific protocol to display from the list. |
| Internal IP | Internal transport IP address of the outgoing session from internal to external. |
| Internal port | Internal transport port number of the outgoing session from internal to external. |
| Internal protocol | Internal protocol of the outgoing session from internal to external. |
| Reflective IP | Translated IP address of the source IP address. |
| Reflective port | Displays the translated number of the port. |
| Reflective protocol | Translated protocol. |

Table 74: Fields on the Source NAT Page (*continued*)

| Field | Description |
|-------------------------------------|---|
| Source NAT pool | Name of the source NAT pool where persistent NAT is used. |
| Type | Persistent NAT type. |
| Left time/Conf time | Inactivity timeout period that remains and the configured timeout value. |
| Current session num/Max session num | Number of current sessions associated with the persistent NAT binding and the maximum number of sessions. |
| Source NAT rule | Name of the source NAT rule to which this persistent NAT binding applies. |
| Search | Applies the specified filter and displays the matching messages. |
| Reset | Resets selected options to default |
| Clear | Removes the selected option. |
| Clear All | Removes all the options available. |
| Refresh | Click the refresh icon at the top right corner to display the fresh content. |
| External node table | |
| Internal IP | Internal transport IP address of the outgoing session from internal to external. |
| Internal port | Internal port number of the outgoing session from internal to external. |
| External IP | External IP address of the outgoing session from internal – to external. |
| External port | External port of the outgoing session from internal to external. |
| Zone | External zone of the outgoing session from internal to external. |
| Refresh | Click the refresh icon at the top right corner to display the fresh content. |
| Paired Address | |
| Pool name | Name of the pool. Select all pools or a specific pool to display from the list. |

Table 74: Fields on the Source NAT Page (continued)

| Field | Description |
|-------------------|---|
| Specified Address | IP address. Select all addresses, or select the internal or external IP address to display, and enter the IP address |
| Pool name | Displays the selected pool or pools. |
| Internal address | Displays the internal IP address. |
| External address | Displays the external IP address. |
| Refresh | Click the refresh icon at the top right corner to display the fresh content. |
| Search | Applies the specified filter and displays the matching messages. |
| Reset | Enables you to get back to the default configuration. |

Resource Usage

Utilization for All source pools

| | |
|-------------------------|---|
| Pool name | Name of the pool. NOTE: To view additional usage information for Port Address Translation (PAT) pools, select a pool name. The information displays under Detail Port Utilization for Specified Pool. |
| Pool type | Pool type: PAT or Non-PAT. |
| Port overloading factor | Port overloading capacity for PAT pools. |
| Address | Addresses in the pool. |
| Used | Number of used resources in the pool. For Non-PAT pools, the number of used IP addresses is displayed. For PAT pools, the number of used ports is displayed. |
| Available | Number of available resources in the pool. For Non-PAT pools, the number of available IP addresses is displayed. For PAT pools, the number of available ports is displayed. |

Table 74: Fields on the Source NAT Page (*continued*)

| Field | Description |
|------------|---|
| Total | <p>Number of used and available resources in the pool.</p> <p>For Non-PAT pools, the total number of used and available IP addresses is displayed.</p> <p>For PAT pools, the total number of used and available ports is displayed.</p> |
| Usage | <p>Percent of resources used.</p> <p>For Non-PAT pools, the percent of IP addresses used is displayed.</p> <p>For PAT pools, the percent of ports, including single and twin ports, is displayed.</p> |
| Peak usage | Percent of resources used during the peak date and time. |

RELATED DOCUMENTATION

| [Monitor Destination NAT](#) | 164

Monitor Destination NAT

You are here: **Monitor** > **NAT** > **Destination NAT**.

Use this page to view destination Network Address Translation (NAT) summary table and details of the specified NAT destination address pool.

[Table 75 on page 164](#) describes the fields on the Destination NAT page.

Table 75: Fields on the Destination NAT Page

| Field | Description |
|---------------|---|
| Rules | |
| Rule-set name | <p>Name of the rule set.</p> <p>Select all rule sets or a specific rule set to display from the list.</p> |
| Total rules | Number of rules configured. |

Table 75: Fields on the Destination NAT Page (*continued*)

| Field | Description |
|----------------------------------|--|
| ID | Rule ID number. |
| Name | Name of the rule. |
| Ruleset Name | Name of the rule set. |
| From | Name of the routing instance/zone/interface from which the packet flows. |
| Source address range | Source IP address range in the source pool. |
| Destination address range | Destination IP address range in the source pool. |
| Destination port | Destination port in the destination pool. |
| IP protocol | IP protocol. |
| Action | Action taken for a packet that matches a rule. |
| Alarm threshold | Utilization alarm threshold. |
| Sessions (Succ/ Failed/ Current) | <p>Successful, failed, and current sessions.</p> <ul style="list-style-type: none"> • Succ—Number of successful session installations after the NAT rule is matched. • Failed—Number of unsuccessful session installations after the NAT rule is matched. • Current—Number of sessions that reference the specified rule. |
| Translation hits | Number of times a translation in the translation table is used for a destination NAT rule. |
| Refresh Interval | Indicates the duration of time after which you want the data on the page to be refreshed. |
| Refresh | Click the refresh icon at the top right corner to display the fresh content. |
| Pools | |
| Pool Name | <p>The names of the pools.</p> <p>Select all pools or a specific pool to display from the list.</p> |

Table 75: Fields on the Destination NAT Page (*continued*)

| Field | Description |
|--------------------------------|---|
| Total Pools | Total pools added. |
| ID | ID of the pool. |
| Name | Name of the destination pool. |
| Address range | IP address range in the destination pool. |
| Port | Destination port number in the pool. |
| Routing instance | Name of the routing instance. |
| Total addresses | Total IP address, IP address set, or address book entry. |
| Translation hits | Number of times a translation in the translation table is used for destination NAT. |
| Top 10 Translation Hits | |
| Graph | Displays the graph of top 10 translation hits. |
| Refresh | Click the refresh icon at the top right corner to display the fresh content. |

RELATED DOCUMENTATION

| [Monitor Source NAT](#) | 158

Monitor Static NAT

You are here: **Monitor** > **NAT** > **Static NAT**.

Use this page to view information related to NAT rules.

[Table 76 on page 167](#) describes the fields on the Static NAT page.

Table 76: Fields on the Static NAT Page

| Field | Description |
|-----------------------|--|
| Rule-set Name | Name of the rule set. Select all rule sets or a specific rule set to display from the list. |
| Total rules | Number of rules configured. |
| Refresh | Indicates the duration of time after which you want the data on the page to be refreshed. |
| Refresh Interval | Click the refresh icon at the top right corner to display the fresh content. |
| ID | Rule ID number. |
| Position | Position of the rule that indicates the order in which it applies to traffic. |
| Name | Name of the rule. |
| Ruleset Name | Name of the rule set. |
| From | Name of the routing instance/interface/zone from which the packet comes. |
| Source addresses. | Source IP addresses. |
| Source ports | Source port numbers. |
| Destination addresses | Destination IP address and subnet mask. |
| Destination ports | Destination port numbers. |
| Host addresses | Name of the host addresses. |
| Host ports | Host port numbers. |
| Netmask | Subnet IP address. |
| Host routing instance | Name of the routing instance from which the packet comes. |
| Alarm threshold | Utilization alarm threshold. |

Table 76: Fields on the Static NAT Page (*continued*)

| Field | Description |
|----------------------------------|---|
| Sessions (Succ/ Failed/ Current) | Successful, failed, and current sessions. <ul style="list-style-type: none"> • Succ—Number of successful session installations after the NAT rule is matched. • Failed—Number of unsuccessful session installations after the NAT rule is matched. • Current—Number of sessions that reference the specified rule. |
| Translation hits | Number of times a translation in the translation table is used for a static NAT rule. |
| Top 10 Translation Hits Graph | Displays the graph of top 10 translation hits. |

RELATED DOCUMENTATION

| [Monitor Destination NAT](#) | 164

Monitor Interface NAT Ports

You are here: **Monitor** > **NAT** > **Interface NAT Ports**.

Use this page to view ports usage for an interface source pool.

[Table 77 on page 168](#) describes the fields on the Interface NAT Ports page.

Table 77: Fields on the Interface NAT Ports Page

| Field | Description |
|------------------------------------|--|
| Interface NAT Summary Table | |
| Pool Index | Port pool index. |
| Total Ports | Total number of ports in a port pool. |
| Single Ports Allocated | Number of ports allocated one at a time that are in use. |
| Single Ports Available | Number of ports allocated one at a time that are free for use. |

Table 77: Fields on the Interface NAT Ports Page (*continued*)

| Field | Description |
|----------------------|---|
| Twin Ports Allocated | Number of ports allocated two at a time that are in use. |
| Twin Ports Available | Number of ports allocated two at a time that are free for use. |
| Refresh Interval | Indicates the duration of time after which you want the data on the page to be refreshed. |
| Refresh | Click the refresh icon at the top right corner to display the fresh content. |

RELATED DOCUMENTATION

[Monitor Source NAT](#) | 158

Authentication

IN THIS CHAPTER

- [Monitor Firewall Authentication | 170](#)
- [Monitor Local Authentication | 171](#)
- [Monitor UAC Authentication | 172](#)

Monitor Firewall Authentication

You are here: **Monitor** > **Authentication** > **Firewall Auth.**

Use this page to view user table and history table of firewall authentication.

[Table 78 on page 170](#) describes the fields on the Firewall Authentication page.

Table 78: Fields on the Firewall Authentication Page

| Field | Description |
|---------------------------|--|
| Virtual Chassis Member | Displays the list of virtual chassis member. Select one of the virtual chassis members listed. |
| Authentication Type | Displays the authentication type used by the firewall. |
| Refresh Interval (30 sec) | Displays the time interval set for page refresh. Select the time interval from the list. |
| Refresh | Displays the option to refresh the page. |
| Clear | Provides an option to clear the summary. Select one of the options available: <ul style="list-style-type: none">● Clear User Table—Enables you to clear user summary.● Clear History Table—Enables you to clear history summary. |

Table 78: Fields on the Firewall Authentication Page (*continued*)

| Field | Description |
|----------------------|---|
| User Table | |
| ID | Displays the authentication identification number. |
| Source IP | Displays the IP address of the authentication source. |
| Age | Displays the idle timeout for the user. |
| Status | Displays the status of authentication (success or failure). |
| User | Displays the name of the user. |
| History Table | |
| ID | Displays the identification number. |
| Source IP | Displays the IP address of the authentication source. |
| Duration | Displays the authentication duration. |
| Status | Displays the status of authentication (success or failure). |
| User | Displays the name of the user. |

RELATED DOCUMENTATION

[Monitor Local Authentication](#) | 171

Monitor Local Authentication

You are here: **Monitor** > **Authentication** > **Local Authentication**.

Use this page to view information about local authenticated user.

[Table 79 on page 172](#) describes the fields on the Local Authentication page.

Table 79: Fields on the Local Authentication Page

| Field | Description |
|------------------------|--|
| Virtual Chassis Member | Displays the list of virtual chassis members. Select one of the virtual chassis members listed. |
| Filter by | Displays the local authentication information based on the selected filter. |
| IP | Displays the IP address. |
| User Name | Displays the name of the user. |
| Role List | Displays the list of roles assigned to the username. |
| Search | Click to search a particular data. |
| Clear All | Click to clear all the content. |
| Refresh | Click the refresh icon at the top right corner to display the fresh content. |

RELATED DOCUMENTATION

| [Monitor UAC Authentication](#) | 172

Monitor UAC Authentication

You are here: **Monitor** > **Authentication** > **UAC Authentication**.

Use this page to view information about UAC authenticated user.

[Table 80 on page 172](#) describes the fields on the UAC Authentication page.

Table 80: Fields on the UAC Authentication Page

| Field | Description |
|-----------|---|
| Filter by | Displays the UAC authentication value based on the selected filter. |
| Search | Click to search any particular data. |

Table 80: Fields on the UAC Authentication Page (*continued*)

| Field | Description |
|-----------|--|
| Refresh | Click the refresh icon at the top right corner to display the fresh content. |
| ID | Displays the authentication identification number. |
| Source IP | Displays the IP address of the authentication source. |
| User Name | Displays the name of the user. |
| Age | Displays the idle timeout for the user |
| Role List | Displays the list of roles assigned to the username. |

RELATED DOCUMENTATION

[Monitor Firewall Authentication](#) | 170

Security Services

IN THIS CHAPTER

- [Monitor Policy Activities | 174](#)
- [Monitor Shadow Policies | 177](#)
- [Monitor Screen Counters | 180](#)
- [Monitor UTM—Antivirus | 181](#)
- [Monitor UTM—Web Filtering | 183](#)
- [Monitor UTM—Antispam | 184](#)
- [Monitor UTM—Content Filtering Profiles | 185](#)
- [Monitor ICAP Redirect | 186](#)
- [Monitor IPS Attacks | 187](#)
- [Monitor IPS Status | 189](#)
- [Monitor Application Firewalls | 190](#)
- [Monitor Applications | 192](#)
- [Monitor Application Tracking | 193](#)
- [Monitor AppQoS | 196](#)
- [Monitor Advanced Threat Prevention—Statistics | 198](#)

Monitor Policy Activities

You are here: **Monitor > Security Services > Policy > Activities.**

Use this page to display, sort, and review policy activity for every activated policy on the device.

[Table 81 on page 175](#) describes the fields on the Activities page.

Table 81: Fields on the Activities Page

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

Table 81: Fields on the Activities Page (*continued*)

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

Table 81: Fields on the Activities Page (*continued*)

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

RELATED DOCUMENTATION

| [Monitor Shadow Policies](#) | 177

Monitor Shadow Policies

You are here: **Monitor** > **Security Services** > **Policy** > **Shadow Policies**.

Use this page to check the policy list. You can enter a criteria and conduct a policy search. The search results include all policies that match the traffic criteria in the sequence in which they will be encountered.

[Table 82 on page 177](#) describes the fields on the Shadow Policies page.

Table 82: Fields on the Shadow Policies Page

| Field | Description |
|------------------------------|-------------|
| Check Policies Search | |

Table 82: Fields on the Shadow Policies Page (*continued*)

| Field | Description |
|-----------------------|--|
| Policy Context | |
| Zone Policy | <p>Specifies the source zone policy.</p> <p>Options available are:</p> <ul style="list-style-type: none"> • From Zone—Name or ID of the source zone. If a From Zone is specified by name, the name is translated to its ID internally. • To Zone—Name or ID of the destination zone. If a To Zone is specified by name, the name is translated to its ID internally. |
| Global Policy | Specifies that the policy defined is a global policy and zones are not required. |
| Packet Info | |
| Source Address | Address of the source in IP notation. |
| Source Port | Port number of the source. |
| Destination Address | Address of the destination in IP notation. |
| Destination Port | Port number of the destination. |
| Source Identity | Name of the source identity. |

Table 82: Fields on the Shadow Policies Page (*continued*)

| Field | Description |
|----------------------------|---|
| Protocol | <p>Name or equivalent value of the protocol to be matched.</p> <ul style="list-style-type: none"> • ah—51 • egp—8 • esp—50 • gre—47 • icmp—1 • igmp—2 • igp—9 • ipip—94 • ipv6—41 • ospf—89 • pgm—113 • pim—103 • rdp—27 • rsvp—46 • sctp—132 • tcp—6 • udp—17 • vrrp—112 |
| Search | Enable you to search for a particular data in the page. |
| Reset | Enable you to get back to the default configuration. |
| Check Policies List | |
| From Zone | Name of the source zone. |
| To Zone | Name of the destination zone. |
| Move | <p>Select according to the requirement:</p> <ul style="list-style-type: none"> • Move Up—Enables you to move up the list. • Move Down—Enables you to move down the list. • Move to Top—Enables you to move to the top of the list. • Move to Bottom—Enables you to move to the bottom of the list. • Move to—Enables you to move to a particular point on the list. |

Table 82: Fields on the Shadow Policies Page (*continued*)

| Field | Description |
|-----------------------|---|
| Total Policies | Number of policies retrieved. |
| Default Policy action | The action to be taken if no match occurs. |
| Name | Policy name |
| Source Address | Name of the source address (not the IP address) of a policy. Address sets are resolved to their individual names. |
| Destination Address | Displays the destination address. |
| Source Identity | Name of the source identity for the policy. |
| Application | Name of a pre configured or custom application of the policy match. |
| Action | Action taken when a match occurs as specified in the policy. |
| Hit Counts | Number of matches for this policy. This value is the same as the Policy Lookups in a policy statistics report. |
| Active Sessions | Number of active sessions matching this policy. |

RELATED DOCUMENTATION

[Monitor Screen Counters](#) | 180

Monitor Screen Counters

You are here: **Monitor** > **Security Services** > **Screen Counters**.

Use this page to view screen statistics for a specified security zone.

[Table 83 on page 181](#) describes the fields on the Screen Counters page.

Table 83: Fields on the Screen Counters Page

| Field | Description |
|---------------------|--|
| Type | Select a type of screen counter: <ul style="list-style-type: none"> • I/F—Displays the interfaces monitored by the IDS attack type and counter value. • Zone—Displays the zone name for IDS attack type. |
| Select a value | Select a value for the Type of screen counter from the list. |
| Disable Log | Enables you to disable the log. |
| Refresh Interval | Indicates the duration of time after which you want the data on the page to be refreshed. |
| Refresh | Click the refresh icon at the top right corner to display the fresh content. |
| Clear | Clears all the data from the display page. |
| IDS attack type | Displays the type of IDS attacks. |
| Counter | Displays the number of times the attacks took place. |
| Log | Displays the log for the IDS attacks. |
| Screen Counter Hits | Displays the details of the screen counter hits. |

RELATED DOCUMENTATION

| [Monitor UTM—Antivirus](#) | 181.

Monitor UTM—Antivirus

You are here: **Monitor** > **Security Services** > **UTM** > **Antivirus**.

Use this page to view information and statistics of UTM antivirus.

[Table 84 on page 182](#) describes the fields on the Antivirus page.

Table 84: Fields on the Antivirus Page

| Field | Description |
|--|---|
| UTM Antivirus | |
| AV Key Expire Date | Displays antivirus licence key expiration date. |
| Update Server | Displays antivirus pattern update server settings. |
| Interval | Displays antivirus pattern interval. |
| Auto Update Status | Displays antivirus pattern auto update status. |
| Last Result | Displays last result of database loading. |
| AV Signature Version | Displays database version timestamp virus record number. |
| Scan Engine Type | Displays the information of the scan engine. |
| Pattern Type | Displays the pattern type. |
| Onbox AV Load Flavor Running | On-box AV is enabled. |
| Onbox AV Load Flavor Configured NOTE: This option is available for SRX5000 and SRX4000 lines of devices. | On-box Antivirus (AV) is configured either in the heavy or light mode. |
| Antivirus statistics | <p>Displays the antivirus statistics:</p> <ul style="list-style-type: none"> Statistics type: <ul style="list-style-type: none"> Intelligent-prescreening Passed Forwarded to scan engine Scan Request: <ul style="list-style-type: none"> Total Clean Threat-found Fall Back |
| Clear Anti-Virus Statistics | <p>Clear all current viewable statistics and begin collecting new statistics.</p> <p>Click Clear Anti-Virus Statistics.</p> |

RELATED DOCUMENTATION

Monitor UTM—Web Filtering | 183

Monitor UTM—Web Filtering

You are here: **Monitor** > **Security Services** > **UTM** > **Web Filtering**.

Use this page to view information and statistics of UTM web filtering.

[Table 85 on page 183](#) describes the fields on the Web Filtering page.

Table 85: Fields on the Web Filtering Page

| Field | Description |
|------------------------------|--|
| UTM Web Filtering Statistics | |
| Statistics type | <div>Displays the available information:</div> <ul style="list-style-type: none">Statistics type:<ul style="list-style-type: none">Total RequestsAllowlist HitBlocklist HitQueries To ServerServer Reply PermitServer Reply BlockCustom Category PermitCustom Category BlockSite Reputation PermitSite Reputation BlockCache Hit PermitCache Hit BlockSafe Search RedirectWeb Filtering Session totalWeb Filtering Session In useFall back<ul style="list-style-type: none">DefaultTimeoutServer-ConnectivityToo-Many-Requests |

Table 85: Fields on the Web Filtering Page (*continued*)

| Field | Description |
|--------------------------------|---|
| Clear Web Filtering Statistics | Click Clear Web Filtering Statistics to clear all current viewable statistics and begin collecting new statistics. |

RELATED DOCUMENTATION

| [Monitor UTM—Antispam](#) | 184

Monitor UTM—Antispam

You are here: **Monitor** > **Security Services** > **UTM** > **Antispam**.

Use this page to view status and statistics of UTM antispam.

[Table 86 on page 184](#) describes the fields on the Antispam page.

Table 86: Fields on the Antispam Page

| Field | Description |
|---------------------|---|
| UTM Antispam Status | Displays the DNS server setting IP and interface details for the following servers: <ul style="list-style-type: none"> • Primary • Secondary • Ternary |

Table 86: Fields on the Antispam Page (*continued*)

| Field | Description |
|----------------------------|---|
| UTM Anti-spam Statistics | <p>Displays the antispam statistics type and counter information:</p> <ul style="list-style-type: none"> • Total Connections • Denied Connections • Total Greetings • Denied Greetings • Total Email Scanned • Spam Total • Spam Tagged • Spam Dropped • DNS Errors • Timeout Errors • Return Errors • Invalid Parameter Errors • Statistics Start Time • Statistics for the last 10 days |
| Clear Anti-Spam Statistics | <p>Clear all current viewable statistics and begin collecting new statistics.</p> <p>Click Clear Anti-Spam Statistics.</p> |

RELATED DOCUMENTATION

[Monitor UTM—Content Filtering Profiles](#) | 185

Monitor UTM—Content Filtering Profiles

You are here: **Monitor** > **Security Services** > **UTM** > **Content Filtering Profiles**.

Use this page to view UTM content filtering statistics.

[Table 87 on page 186](#) describes the fields on the Content Filtering page.

Table 87: Fields on the Content Filtering Page

| Field | Description |
|------------------------------------|--|
| UTM Content Filtering Statistics | <p>Displays the statistics type, counter passed, and counter blocked details:</p> <ul style="list-style-type: none"> • Base on command list • Base on mime list • Base on extension list • ActiveX plug-in • Java applet • EXE files • ZIP files • HTTP cookie |
| Clear Content Filtering statistics | <p>Clear all current viewable statistics.</p> <p>Click Clear Content Filtering statistics.</p> |

RELATED DOCUMENTATION

| [Monitor ICAP Redirect](#) | 186

Monitor ICAP Redirect

You are here: **Monitor** > **Security Services** > **ICAP Redirect**.

Use this page to monitor ICAP Redirect details.

[Table 88 on page 186](#) describes the fields on the ICAP Redirect page.

Table 88: Fields on the ICAP Redirect Page

| Field | Description |
|-----------------------|---|
| Refresh Interval(sec) | Select the refresh rate. |
| Refresh | Refresh at any given point, irrespective of the refresh rate set. |
| Clear Statistics | Clears all the collated data. |
| Server Status | Displays the status of the ICAP server. |

Table 88: Fields on the ICAP Redirect Page (*continued*)

| Field | Description |
|--------------------|--|
| Message Redirected | Displays the number of HTTP requests that have passed through the ICAP channel. |
| Message Received | Displays the number of HTTP requests that have passed through the ICAP channel. <ul style="list-style-type: none"> • Message REQMOD Redirected—Displays the number of messages that went through the redirect request on HTTP request. • Message RESPMOD Redirected—Displays the number of messages that went through the redirect response on HTTP request. |
| Fallback Details | Displays the Timeout, Connectivity, and Default values for Permitted, Rejected, and Log permitted parameters if the ICAP server is unavailable. |

RELATED DOCUMENTATION

| [Monitor IPS Attacks](#) | 187

Monitor IPS Attacks

You are here: **Monitor** > **Security Services** > **IPS** > **Attacks**.

Use this page to view attack table data and top N attack hits.

[Table 89 on page 187](#) describes the fields on the Attacks page.

Table 89: Fields on the Attacks Page

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

Table 89: Fields on the Attacks Page (*continued*)

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

Table 89: Fields on the Attacks Page (*continued*)

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

RELATED DOCUMENTATION

| [Monitor IPS Status](#) | 189

Monitor IPS Status

You are here: **Monitor** > **Security Services** > **IPS** > **Status**.

Use this page to view IDP Status, memory, counters, policy rulebase statistics, and attack table statistics.

[Table 90 on page 189](#) describes the fields on the Status page.

Table 90: Fields on the Status Page

| Field | Description |
|-------------------|---|
| IDP Status | |
| Status of IDP | Displays the status of the current IDP policy. |
| Up Since | Displays the time from when the IDP policy first began running on the system. |

Table 90: Fields on the Status Page (*continued*)

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

RELATED DOCUMENTATION

| [Monitor Application Firewalls](#) | 190

Monitor Application Firewalls

You are here: **Monitor** > **Security Services** > **Application FW**.

Use this page to view rule set, rules in selected rule set, and counters for selected rule-set.

[Table 91 on page 191](#) describes the fields on the Application FW page.

Table 91: Fields on the Application FW Page

| Field | Description |
|---------------------------------------|---|
| Rule Set | |
| Name | <p>Displays the rule sets configured for the device.</p> <p>Select a rule set to display its associated rules and counters in the lower panes.</p> |
| Default Rule | <p>Displays the action taken when traffic does not match any of the associated rules.</p> <ul style="list-style-type: none"> • permit—Permits all traffic that does not match any rule in the rule set. • deny—Denies all traffic that does not match any rule in the rule set. |
| Rules | Displays the rule names associated with the rule set. |
| Refresh | Click the refresh icon at the top right corner to display the fresh content. |
| Rules in Selected Rule Set | |
| Rule Name | Lists the names of the rules included in the rule set. |
| Match Dynamic Applications | Displays the dynamic applications used as match criteria for the associated rule. |
| Action | <p>Displays the action to be taken if the traffic matches the associated rule's match criteria.</p> <ul style="list-style-type: none"> • permit—Permits traffic that matches the rule. • deny—Denies traffic that matches the rule. |
| Counters for Selected Rule-Set | |
| Refresh interval (sec) | Specifies the interval in seconds when counter values are refreshed. |
| Counter | Displays the counter for rule in the rule set |
| Value | Displays the value for rule in the rule set |
| Clear Statistics | Clears the statistics in the associated pane. |

RELATED DOCUMENTATION

Monitor Applications

You are here: **Monitor** > **Security Services** > **Applications**.

Use this page to view information about bandwidth consumption, session establishment, and risks associated with your applications.

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.

Table 92 on page 192 describes the fields on the Applications page.

Table 92: Fields on the Applications 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. |
| 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. |

Table 92: Fields on the Applications Page (*continued*)

| Field | Description |
|-----------------|--|
| Users | Total number of users accessing the application. |
| Volume | Bandwidth used by the application. |
| Total Sessions | Total number of application sessions. |
| Category | Category of the application, such as web, infrastructure, and so on. |
| Sub-Category | <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> |

RELATED DOCUMENTATION

| [Monitor Application Tracking](#) | 193

Monitor Application Tracking

You are here: **Monitor** > **Security Services** > **Application Tracking**.

Use this page to monitor sessions and bytes of a particular application or group of applications.

[Table 93 on page 194](#) describes the fields on the Application Tracking page.

Table 93: Fields on the Application Tracking Page

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

Table 93: Fields on the Application Tracking Page (*continued*)

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

Table 93: Fields on the Application Tracking Page (*continued*)

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

RELATED DOCUMENTATION

| [Monitor AppQoS](#) | 196.

Monitor AppQoS

You are here: **Monitor** > **Security Services** > **Application QoS**.

Use this page to diagnose and verify the connectivity of Application QoS.

NOTE: This option is available only for SRX4000 and SRX5000 lines of devices.

[Table 94 on page 196](#) describes the fields on the Application QoS page.

Table 94: Fields on the Application QoS Page

| Field | Description |
|------------------|---|
| Refresh Interval | Indicates the duration of time after which you want the data on the page to be refreshed. |

Table 94: Fields on the Application QoS Page (*continued*)

| Field | Description |
|---------------------------------------|--|
| Refresh | Updates the display with current information. The refresh limit updates the display automatically at the interval specified. To change the refresh rate, select the number of seconds in the Refresh interval (sec) field. |
| Rate limiters statistics | |
| Clear statistics | Clears the statistics in the associated pane. |
| PIC | Select the PIC to display the AppQoS settings of the most recent sessions |
| Rule-set Name | Name of the rule set applied to each session. |
| Application | Applications associated with the applied rule set. |
| Client2server rate limiter | Name of the rate limiter applied in the client-to-server direction. |
| C2s Rate (bps) | Maximum transfer rate specified for the client-to-server rate limiter. |
| Server2client rate limiter(bps) | Name of the rate limiter applied in the server-to-client direction. |
| S2C Rate(bps) | Maximum transfer rate specified for the server-to-client rate limiter. |
| Rules statistics Pane | |
| Clear statistics | Clears the statistics in the associated pane. |
| PIC | PIC for which the rule statistics are displayed. Select the PIC to display the number of times each AppQoS rule set and rule are applied on this PIC. |
| Rule- set name | Name of the rule set applied to each session. |
| Rule name | Name of the rule in the rule set. |
| Hits | Number of occurrences when this rule has been matched and applied. |
| Counters for Selected Rule-Set | |
| Clear counter | Resets the counters to 0 in the associated pane. |
| PIC | PIC number for which the AppQoS counts apply. |

Table 94: Fields on the Application QoS Page (*continued*)

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

RELATED DOCUMENTATION

| [About the Diagnostics Page](#) | 370

Monitor Advanced Threat Prevention—Statistics

You are here: **Monitor** > **Security Services** > **Advanced Threat Prevention** > **Statistics**.

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

[Table 95 on page 198](#) describes the fields on the Statistics page.

Table 95: Fields on the Statistics Page

| Field | Description |
|---|---|
| Advanced Anti Malware Session Statistics | |
| Sessions | <p>Below are the options under session:</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. |

Table 95: Fields on the Statistics Page (*continued*)

| Field | Description |
|---|--|
| Clear Statistics | Clear the statistics. |
| Graph | Shows the anti-malware session statistics. |
| Security Intelligence Session Statistics | |
| Profiles | Displays the IP address of the software of the selected DS-Lite configuration. |
| Sessions | <p>Below are the options under session:</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 Policy Activities | 174

VPN

IN THIS CHAPTER

- [Monitor VPN—Phase I | 200](#)
- [Monitor VPN—Phase II | 201](#)

Monitor VPN—Phase I

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

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

[Table 96 on page 200](#) describes the fields on the Phase I page.

Table 96: Fields on the Phase I Page

| Field | Description |
|---------------------------|---|
| IKE Security Associations | |
| Refresh Interval | Indicates the duration of time after which you want the data on the page to be refreshed. |
| Refresh | Click the refresh icon at the top 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. |

Table 96: Fields on the Phase I Page (*continued*)

| Field | Description |
|------------------|---|
| Responder Cookie | <p>Random number generated by the remote node and sent back to the initiator as a verification that the packets were received.</p> <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> |
| 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](#) | 201

Monitor VPN—Phase II

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

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

[Table 97 on page 201](#) describes the fields on the Phase II page.

Table 97: Fields on the Phase II Page

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

Table 97: Fields on the Phase II Page (*continued*)

| Field | Description |
|------------|---|
| Clear All | Clears all the data on the display page. |
| By bytes | Provides total number of bytes encrypted and decrypted by the local system across the IPsec tunnel. |
| By packets | Provides total number of packets encrypted and decrypted by the local system across the IPsec tunnel. |

IPsec Statistics

—Provides details of the IPsec statistics.

| | |
|----------------------------|---|
| Counter | Displays the number of chassis cluster node. |
| Value | Displays the values for the respective chassis cluster nodes. |
| Input/Output bytes/Packets | Displays the chart for phase II statistics input or output bytes. |

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 97: Fields on the Phase II Page *(continued)*

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

RELATED DOCUMENTATION

| [Monitor VPN—Phase I](#) | 200

Flow Session

IN THIS CHAPTER

- [Monitor Flow Session](#) | 204

Monitor Flow Session

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

Use this page to view flow session information of the respective session.

[Table 98 on page 204](#) describes the fields on the Flow Session page.

Table 98: Fields on the Flow Session Page

| Field | Description |
|--|---|
| Flow Session Search | |
| —Provides the option to search sessions. | |
| Application | Displays the application name for the session summary. |
| Protocol | Provides the option to enter protocol details. |
| Source IP/Prefix | Enter the IP address of the authentication source. |
| Dest IP/Prefix | Enter the IP address of the authentication destination. |
| Search | Enables you to search for the flow session after all details are entered. |
| Reset | Enables you to go back to the default configuration. |

Table 98: Fields on the Flow Session Page (*continued*)

| Field | Description |
|---|--|
| Advanced | <p>Provides you advanced options to search for Flow sessions.</p> <p>Enter the below details:</p> <ul style="list-style-type: none"> • Application—Displays the application name for the session summary. • Source IP/ Prefix—Enter the IP address of the authentication source. • Source Port—Enter the specified source port. • Protocol—Provides the options to enter protocol details. • AppFW Rule Set—Displays the number of application firewall rule set configurations. • Application Group—Enables you to collect application group statistics. • Interface—Select an interface from the list. • Dest IP/ Prefix—Enter the IP address of the authentication destination. • Dest Port—Enter the specified destination port • Family—Select an option from the list. • Application Firewall—Check the box to permit, reject, or deny traffic based on the application of the traffic. • Application QoS—displays traffic based on application type and limits the amount of bandwidth an application can consume. <p>NOTE: This option is available only with SRX4000 and SRX5000 line of devices.</p> |
| Flow Session Summary | |
| —Provides a summary of the all the options selected in the Flow Gate. | |
| Clear | <p>Provides the option to clear the session details statistics.</p> <p>Click Clear to clear the details session statistics.</p> |
| Flow Session Information | |
| Session ID | Displays the number that identifies the session. Use this ID to get more information about the session. |
| Policy | Displays the policy that permitted the traffic. |
| TimeOut | Displays the idle timeout after which the session expires. |
| Status | Displays the status of the session. |
| Source IP/Port | Enter the IP address of the authentication source. |

Table 98: Fields on the Flow Session Page (continued)

| Field | Description |
|------------------|--|
| Protocol | Provides the option to enter protocol details. Enter the protocol details. |
| InComing IF | Displays the incoming flow (source and destination IP addresses, application protocol, and interface). |
| Outgoing IF | Displays the reverse flow (source and destination IP addresses, application protocol, and interface). |
| AppSecure Detail | Displays list of all enabled and disabled application signatures and existing application rule sets on the device. |
| Refresh | Click the refresh icon at the top right corner to display the fresh content. |

RELATED DOCUMENTATION

| [Monitor Flow Gate](#) | 207.

Flow Gate

IN THIS CHAPTER

- [Monitor Flow Gate | 207](#)

Monitor Flow Gate

You are here: **Monitor** > **Flow Gate**.

Use this page to view information about gates in the security firewall.

[Table 99 on page 207](#) describes the fields on the Flow Gate page.

Table 99: Fields on the Flow Gate Page

| Field | Description |
|---|---|
| Flow Gate Search | |
| Source Prefix | Enter the source prefix which you have already defined, to be included in the match condition. |
| Source Port | Enter the source port type to be included in, or excluded from, the match condition. |
| Destination Prefix | Enter the destination prefix which you have already defined, to be included in the match condition. |
| Destination Port | Enter the port types to be included in, or excluded from, the match condition. |
| Protocol | Provides the option to enter protocol details. |
| Flow Gate Summary | |
| —Provides a summary of the all the options selected in the Flow Gate. | |
| Flow Gate Information | |

Table 99: Fields on the Flow Gate Page (*continued*)

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

RELATED DOCUMENTATION

[Monitor VLAN](#) | 209

VLAN

IN THIS CHAPTER

- [Monitor VLAN | 209](#)

Monitor VLAN

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

Use this page to view information VLAN.

[Table 100 on page 209](#) describes the fields on the VLAN page.

Table 100: Fields on the VLAN Page

| Field | Description |
|-------------------|--|
| VLAN | |
| Routing Instance | Displays the routing instance name. |
| VLAN Name | Displays the name of the VLAN. |
| VLAN ID | Displays the VLAN ID number. |
| MAC Table | |
| Select a VLAN | Displays the configured VLANs. Select a VLAN from the list. |
| MAC Address | Displays the MAC address associated with the VLAN. |
| MAC Flags | Displays the flags associated with the MAC address. |
| Logical Interface | Displays the name of a logical interface associated with the VLAN. |

RELATED DOCUMENTATION

| [Monitor Threats Map \(Live\)](#) | 215

Wireless LAN

IN THIS CHAPTER

- [Monitor Wireless LAN | 211](#)

Monitor Wireless LAN

You are here: **Monitor** > **Wireless LAN**.

Use this page to view wireless access points details.

NOTE: Starting in Junos OS Release 20.1R1, J-Web supports SRX380 devices. You can monitor the SRX380 device supported Wi-Fi Mini-Physical Interface Modules (Mini-PIMs).

[Table 101 on page 211](#) describes the fields on the Wireless LAN page.

Table 101: Fields on the Wireless LAN Page

| Field | Description |
|----------------------|-------------|
| Access Point Details | |

Table 101: Fields on the Wireless LAN Page (*continued*)

| Field | Description |
|----------------------------|---|
| Name | <p>Displays the following names:</p> <ul style="list-style-type: none"> • Access Point—Name of the access point. • Type—Type of access point (internal or external). • Location—Location of the access point. • Serial Number—Serial number of the access point. • Firmware Version—Firmware version for the access point. • Alternate Version—Backup firmware for the access point. • Regulatory Domain—Regulatory domain of the access point, such as FCC (Federal Communications Commission), ETSI (European Union Telecommunications Institute), TELEC, or WORLD. • Country—Country name. • Access Interface—Port where the access point is connected. • Packet Capture—ON or OFF. The default is OFF. • MAC Address—MAC address of the external access point. • IPv4 Address—IPv4 address of the access point. • Status—ON or OFF. • MAC Address—MAC address of radio 1. • Mode—Mode of radio 1. The mode can be ac, a, an, or 5GHz 802.11n. The default is 802.11 a/n. • Channel—Frequency at which radio 1 operates. • Status—ON or OFF. • MAC Address—MAC address of radio 2. • Mode—Mode of radio 2. The mode can be bg, bgn, or 2.4GHz 802.11n. The default is 802.11 b/g/n. • Channel—Frequency at which radio 2 operates. |
| Value | Displays the values for the respective names. |
| Client Associations | |
| VAP | <p>Displays the virtual access point with which the client is associated. For example, wlan0vap2 means the client is associated with VAP 2 on radio 1.</p> <p>wlan0 means the client is associated with VAP 0 on radio 1.</p> <p>wlan1 means the client is associated with VAP 0 on radio 2.</p> |
| Client MAC Address | Displays the MAC address of the associated wireless client. |

Table 101: Fields on the Wireless LAN Page (*continued*)

| Field | Description |
|-------------------|--|
| Authentication | <p>Displays the underlying IEEE 802.11 authentication status, if the virtual access point security mode is set to none or static WEP.</p> <p>This status does not show IEEE 802.1x authentication or association status. If the virtual access point security mode is set to 802.1x or WPA, it is possible for a client association to be shown as being authenticated when it has actually not been authenticated through the second layer of security.</p> |
| Channel/Rate/RSSI | <p>Displays the following information:</p> <ul style="list-style-type: none"> • Channel—Channel on which the client associations are currently broadcasting. • Rate—IEEE 802.11 mode being used on the client associations. • RSSI—Received Signal Strength Indicator for the current channel. |
| Packets Rx/Tx | Displays the number of packets received from the wireless clients and transmitted from the access point to the wireless client. |
| Bytes Rx/Tx | Displays the number of bytes received from the wireless clients and transmitted from the access point to the wireless client. |

Neighboring Access Points

| | |
|-------------|--|
| MAC Address | Displays the MAC address of the neighbor access point. |
| Privacy | <p>Displays the security status on the neighbor access point:</p> <ul style="list-style-type: none"> • Off—Security mode is set to none (no security). • On—There is some security in place. |
| WPA | Displays if Wi-Fi Protected Access (WPA) security is on or off on the neighbor access point. |
| Band | <p>Displays the IEEE 802.11 mode being used on the neighbor access point:</p> <ul style="list-style-type: none"> • 2.4—IEEE 802.11b, 802.11g, or 802.11n mode, or a combination of these modes. • 5—IEEE 802.11ac, 802.11a or 802.11n mode, or both modes. |
| Channel | Displays the channel on which the neighbor access point is currently broadcasting. |
| SSID | Displays if the service set identifier that identifies the WLAN that the neighbor access point is broadcasting. |

Virtual Access Points Details

| | |
|------|---|
| Name | Displays the name of the virtual access points. |
|------|---|

Table 101: Fields on the Wireless LAN Page (*continued*)

| Field | Description |
|-------|--|
| Value | Displays the details of the virtual access points. For example, SSID, VLAN ID, upload limit and so on. |

Release History Table

| Release | Description |
|------------------------|--|
| 20.1R1 | Starting in Junos OS Release 20.1R1, J-Web supports SRX380 devices. You can monitor the SRX380 device supported Wi-Fi Mini-Physical Interface Modules (Mini-PIMs). |

RELATED DOCUMENTATION

| [Monitor Threats Map \(Live\)](#) | **215**

Threats Map (Live)

IN THIS CHAPTER

- [Monitor Threats Map \(Live\)](#) | 215

Monitor Threats Map (Live)

You are here: **Monitor** > **Threats Map (Live)**.

NOTE: Threats Map (Live) page is available on all the SRX Series devices 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 Sky ATP, and screen options. You can also click a specific geographical location to view the event count and the top five inbound and outbound IP addresses.

NOTE: To view the data on the Threats Map (Live) page, ensure that:

- Security logging is enabled. If not, go to **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 Sky ATP server.

The threat data is displayed starting from 12:00 AM (midnight) up to the current time (in your time zone) on that day and is updated every 30 seconds. The current date and time are displayed at the top right and a legend is displayed at the bottom left of the page.

If a threat occurs when you are viewing the page, an animation shows the country from which the threat originated (source) and the country in which the threat occurred (destination).

NOTE: Threats with unknown geographical IP addresses and private IP addresses are displayed as UNKNOWN_COUNTRY.

Field Descriptions

Table 102 on page 216 displays the fields of the Threats Map (Live) page.

Table 102: Fields on the Threats Map (Live) Page

| Field | Description |
|---------------------------------|--|
| Total Threats Blocked & Allowed | Displays the total number of threats blocked and allowed. Click the hyperlinked number to go to the All Events (Monitor > Events > All Events) page (filtered view of the Grid View tab), where you can view more information about the IPS, virus, spam, Juniper Sky ATP, and screen events. |
| Threats Blocked & Allowed | <p>Displays the total number of threats blocked and allowed by the following categories:</p> <ul style="list-style-type: none"> • IPS Threats • Virus • Spam • Screen • Juniper Sky ATP <p>Click the hyperlinked number for a category to go to the page for that category, where you can view more information about that category. For example, clicking the hyperlinked number for IPS threats takes you to the IPS (Monitor > Events > IPS) page (filtered view of the Grid View tab).</p> |
| Top Destination Countries | Displays the top five destination countries and the number of threats per country. Click the hyperlink for a country to go to the All Events (Monitor > Events > All Events) page (filtered view of the Grid View tab), where you can view more information about the IPS, virus, spam, Juniper Sky ATP, and screen events for that country. |
| Top Source Countries | Displays the top five source countries and the number of threats per country. Click the hyperlink for a country to go to the All Events (Monitor > Events > All Events) page (filtered view of the Grid View tab), where you can view more information about the IPS, virus, spam, Juniper Sky ATP, and screen events for that country. |

Threat Types

The Threats Map (Live) page displays blocked and allowed threat events based on feeds from IPS, antivirus, antispam engines, Juniper Sky ATP, and screen options. [Table 103 on page 217](#) describes different types of threats blocked and allowed.

Table 103: Types of Threats

| Attack | Description |
|-------------------|--|
| IPS threat events | <p>Intrusion detection and prevention (IDP) attacks detected by the IDP module.</p> <p>The information reported about the attack (displayed on the IPS (Monitor > Events > IPS) page) includes information about:</p> <ul style="list-style-type: none"> • Specific events names • Specific event names with either source or destination country |
| Virus | <p>Virus attacks detected by the antivirus engine.</p> <p>The information reported about the attack (displayed on the Antivirus (Monitor > Events > Antivirus) page) includes information about:</p> <ul style="list-style-type: none"> • Specific events names • Specific event names with either source or destination country |
| Spam | <p>E-mail spam that is detected based on the blocklist spam e-mails.</p> <p>The information reported about the attack (displayed on the Antispam (Monitor > Events > Antispam) page) includes information about:</p> <ul style="list-style-type: none"> • Specific events names • Specific event names with source country |
| Juniper Sky ATP | <p>Events that are detected based on Juniper Sky ATP policies.</p> <p>The information reported about the attack (displayed on the Screen (Monitor > Events > ATP) page) includes information about:</p> <ul style="list-style-type: none"> • Specific events names • Specific event names with either source or destination country |
| Screen | <p>Events that are detected based on screen options.</p> <p>The information reported about the attack (displayed on the Screen (Monitor > Events > Screen) page) includes information about:</p> <ul style="list-style-type: none"> • Specific events names • Specific event names with either source or destination country |

Tasks You Can Perform

You can perform the following tasks from this page:

- Toggle between updating the data and allowing live updates—Click the **Pause** icon to stop the page from updating the threat map data and to stop animations. Click the **Play** icon to update the page data and resume animations.
- Zoom in and out of the page—Click the zoom in (+) and zoom out (–) icons to zoom in and out of the page.
- Pan the page—Click and drag the mouse to pan the page.
- View country-specific details:
 - Click a country on the threat map to view threat information specific to that country. A *Country-Name* pop-up appears displaying country-specific information.
 - Click **View Details** in the *Country-Name* pop-up to view additional details. The *Country-Name (Details)* panel appears.

[Table 104 on page 218](#) provides more details on the country-specific threat information.

Table 104: Country-Specific Threat Information

| Field | Description |
|--|---|
| Displayed in Country-Name pop-up | |
| <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. Click the hyperlinked number to go to the All Events (Monitor > Events > All Events) page, where you can view more information about the events. |
| 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 | |

Table 104: Country-Specific Threat Information (*continued*)

| Field | Description |
|--|---|
| <i>Number of threat events</i> Threat Events since 12:00 am | <p>Displays the total number of threat events (inbound and outbound) since midnight for that country.</p> <p>Click the hyperlinked number to go to the All Events (Monitor > Events > All Events) page, where you can view more information about the events.</p> |
| Number of Inbound Events | <p>Displays the total number of inbound threats for the country and the number of inbound threat events for each of the following categories:</p> <ul style="list-style-type: none"> • IPS Threats • Virus • Spam • Screen • Juniper Sky ATP <p>Click the hyperlinked number for a category to go to the page for that category, where you can view more information about that category. For example, clicking the hyperlinked number for IPS threats takes you to the IPS (Monitor > Events > IPS) page.</p> <p>Click Top 5 IP Addresses (Inbound) to view the IP address and the number of events for that IP address for the top five inbound events.</p> <p>Click View All IP Addresses to view all the destination IP addresses and number of events for that IP address.</p> <p>NOTE: You can view or select View All IP Addresses only after you click Top 5 IP Addresses (Inbound).</p> |

Table 104: Country-Specific Threat Information (*continued*)

| Field | Description |
|---------------------------|---|
| Number of Outbound Events | <p>Displays the total number of outbound threats for the country and the number of outbound threat events for each of the following categories:</p> <ul style="list-style-type: none"> • IPS Threats • Virus • Spam • Screen • Juniper Sky ATP <p>Click the hyperlinked number for a category to go to the page for that category, where you can view more information about that category. For example, clicking the hyperlinked number for screens takes you to the Screen (Monitor > Events > Screen) page.</p> <p>Click Top 5 IP Addresses (Outbound) to view the IP address and the number of events for that IP address for the top five outbound events.</p> <p>Click View All IP Addresses to view all the source IP addresses and number of events for that IP address.</p> <p>NOTE: You can view or select View All IP Addresses only after you click Top 5 IP Addresses (Outbound).</p> |

RELATED DOCUMENTATION

| [Monitor VLAN](#) | 209

4

PART

Device Administration

Basic Settings | **223**

Setup | **238**

Cluster Management | **275**

User Management | **284**

Certificate Management—Device Certificates | **290**

Certificate Management—Trusted Certificate Authority | **302**

Certificate Management—Certificate Authority Group | **313**

Multi Tenancy—Resource Profiles | **319**

Multi Tenancy—Interconnecting Ports | **327**

Multi Tenancy—Logical Systems | **337**

Multi Tenancy—Tenants | **351**

License Management | **362**

ATP Management | **367**

Operations | **372**

Software Management | **379**

Configuration Management | **382**

Alarm Management | **386**

RPM | **395**

Tools | **407**

Basic Settings

IN THIS CHAPTER

- [Configure Basic Settings](#) | 223

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.

- **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 105 on page 224](#) describes the fields on the Basic Settings page.

Table 105: Fields on the Basic Settings Page

| Field | Action |
|--------------------------------|---|
| System Identity Details | |
| Host Name | 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 | <p>Enter a password for the root user.</p> <p>NOTE: After you have defined a root password, that password is required when you log in to the J-Web or the CLI.</p> |
| Confirm Password | Re-enter the password to confirm. |
| 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 top right side 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 top right side 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 top right side of the DNS Servers table or right-click on the hostname and delete it. |

Table 105: 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"> Click + at the top right side of the Domain Search table. Enter a domain name. The string must contain an alphanumeric character and can include underscores, hyphen, slash and dot. No spaces allowed. 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"> Select a domain name that you want to edit. Click the pencil icon at the top right side of the Domain Search table or right-click on the domain name and edit the name. 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 top right side of the Domain Search table or right-click on the name and delete it. |
| Date and Time Details | |
| Time Zone | Select the time zone from the list in which the router resides. |
| Current date/time | Displays the current date and time. |

Table 105: Fields on the Basic Settings Page (continued)

| Field | Action |
|--|--|
| Time Source | <p>Select an option from the list to set the system time:</p> <hr/> <p>Sync with NTP Server—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>Sync with Computer Time—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 Configure Time—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> |
| Management Access Configuration | |
| Loopback Address | <p>Enter IP address and subnet for the loopback address.</p> <p>NOTE: If the SRX device does not have a dedicated management port (fxp0), then Loopback Address and Subnet are the only options available for the management access configuration.</p> |

Table 105: Fields on the Basic Settings Page (continued)

| Field | Action |
|------------------------|--|
| Subnet | <p>Enter the address, for example, 255.255.255.0. You can also specify the address prefix.</p> <p>Specifies the range of logical addresses within the address space that is assigned to an organization.</p> |
| IPv4 | <p>Select this option to enable IPv4.</p> <p>NOTE: IPv4 configuration is supported only on the SRX devices with fxp0 port.</p> |
| Management Access Port | Enter an IPv4 address for the device. |
| Subnet | <p>Enter the address, for example, 255.255.255.0. You can also specify the address prefix.</p> <p>Specifies the range of logical addresses within the address space that is assigned to an organization.</p> |
| Default Gateway | Enter the default gateway address for IPv4. |
| 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. |
| RFC Complaint | <p>Select this option to enable RFC complaint.</p> <p>Provides NETCONF sessions complaint with RFC 4741.</p> |
| Netconf -> SSH | Select this option to enable NETCONF connections over SSH connections. |
| Trace Options | Select this option to enable NETCONF trace options. |
| On Demand | Select this option to enable on-demand tracing. |
| No Remote Trace | Select this option to enable no remote tracing. |

Table 105: Fields on the Basic Settings Page (*continued*)

| Field | Action |
|----------------------------|---|
| Junoscript Over Clear Text | Select this option to enable Junoscript connections over clear text. |
| Junoscript Over SSL | Select this option to enable Junoscript connections over SSL. |
| Junoscript Certificate | Select the local certificate for SSL from the list. |
| HTTP | Select this option to enable HTTP connection settings. |
| 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 | <p>Specifies the certificate that you want to use to secure the connection from the HTTPS certificates list when you enable HTTPS.</p> <p>Select the HTTPS certificate from the list.</p> |
| PKI Certificate | <p>Select the PKI certificate for HTTPS from the list.</p> <p>NOTE: This option is available only if you select pki-local-certificate in the HTTPS Certificate options.</p> |
| Local Certificate | <p>Select the local certificate for HTTPS from the list.</p> <p>NOTE: This option is available only if you select local-certificate in the HTTPS Certificate options.</p> |
| HTTPS Port | Select the TCP port by clicking top or bottom arrows for incoming HTTPS connections. |
| WEB API | |
| Web API | Select to enable Web API configuration. |
| Client | Select to enable client for the Web API. |

Table 105: Fields on the Basic Settings Page (*continued*)

| Field | Action |
|------------------|---|
| Host Name | <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. |
| 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. |

Table 105: Fields on the Basic Settings Page (*continued*)

| Field | Action |
|------------------|--|
| User | Select this option to enable user credentials. |
| Name | Enter a username. |
| Password | Enter the user password. |
| REST API | |
| REST API | Enable this option to allow RPC execution over HTTP(S) connection. |
| 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 105: 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 | Select the Cipher suites in order of your preference and click on the left arrow or right arrow to add. |
| 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> |
| Certificate Authority 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. |
| Certificate | |

Table 105: Fields on the Basic Settings Page (*continued*)

| Field | Action |
|-------------------------|--|
| Certificate | <p>Specifies the certificate name to secure HTTPS connections.</p> <p>Select an option:</p> <ul style="list-style-type: none"> • To add a new certificate, click +. Then, enter the certificate name and certificate content and then click OK. • To edit an existing certificate, select it and click the pencil icon or right-click on it and click Edit Row. Then, edit the certificate content and click OK. • To delete an existing certificate, select it and click the delete icon or right-click on it and click Delete Row. |
| Security Logging | |
| Stream mode Logging | <p>Select this option to enable logging.</p> <p>NOTE: Starting in Junos OS Release 19.1R1, the Enable Traffic Logs option is available for user logical system and tenants.</p> |
| 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> |
| UTC Timestamp | <p>Select this option to enable UTC Timestamp for security log timestamps.</p> |
| 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> |

Table 105: Fields on the Basic Settings Page (*continued*)

| Field | Action |
|--------------------|---|
| Interface | <p>Select a source interface from the list.</p> <p>NOTE: This option is available if you select the log on type as Source Interface.</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> |
| 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 105: 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. |
| SNMP | |
| 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> |

Table 105: Fields on the Basic Settings Page *(continued)*

| Field | Action |
|----------------------|---|
| System Location | Enter any location information for the system (lab name or rack name, for example). |
| System Name Override | Specifies the option to override the system hostname. Enter the name of the system. |
| Community | Specifies the name and authorization for the SNMP community. <ul style="list-style-type: none"> • Click +. • Enter the name of the community being added. • Select the desired authorization (either read-only or read-write) from the list. Click tick mark. |
| Trap Groups | |
| Name | Click + to add a trap group. Enter the SNMP trap group being configured. |
| Categories | Select trap categories to add to the trap group being configured. The options available are: <ul style="list-style-type: none"> • Authentication • Chassis • Configuration • Link • Remote operations • RMON alarm • Routing • Startup • CRRP events |
| Targets | Specifies one or more IP addresses that specify the systems to receive SNMP traps that are generated by the trap group being configured. Click +, enter the target IP address for SNMP trap group, and click tick mark. |

Table 105: 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> |
| 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: Starting in Junos OS Release 20.1R1, J-Web supports SRX380 devices which support power supply redundancy for power management.

Table 105: Fields on the Basic Settings Page *(continued)*

| Field | Action |
|----------------|---|
| 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 | Enable this option to manage power on the SRX380 device. NOTE: This option is available only when the device is in the standalone mode. |

Release History Table

| Release | Description |
|------------------------|--|
| 20.1R1 | Starting in Junos OS Release 20.1R1, J-Web supports SRX380 devices which support power supply redundancy for power management. |
| 19.1R1 | Starting in Junos OS Release 19.1R1, the Enable Traffic Logs option is available for user logical system and tenants. |

RELATED DOCUMENTATION

| [Configure Setup Wizard](#) | 238

Setup

IN THIS CHAPTER

- Configure Setup Wizard | 238
- Configure Cluster (HA) Mode | 262

Configure Setup Wizard

You are here: **Device Administration** > **Setup**.

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

NOTE: Starting in Junos OS Release 20.1R1, you can configure SRX380 device using Setup Wizard.

NOTE: You can also configure the setup modes in the factory default settings. Connect your management device (laptop or PC) to the SRX device in factory default settings, the J-Web Setup wizard will appear. For more information on the Setup wizard in the factory default settings, see [“Start J-Web” on page 3](#).

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

NOTE: Click **Cancel** to exit the mode selection window.

- **Standard mode**—Configure your SRX Series device to operate in a standard mode. In this mode, you can configure basic settings such as device and users, time and DNS Servers, also management interface, zones and interfaces, and security policies.

- Cluster (HA) mode—Configure your SRX Series device 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. See [“Configure Cluster \(HA\) Mode” on page 262](#).

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

- Passive mode—Configure your SRX Series device to operate in a TAP mode. TAP mode allows you to passively monitor traffic flows across a network. If IDP 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 devices does not support the passive mode configuration.

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 Devices using the J-Web Setup wizard:

1. Click on the mode you want to setup.

NOTE: For the standard and the passive modes, the Reset Configuration message window appears. Click **Proceed to Launch** to launch the Setup Wizard. Launching the Setup wizard resets the device to the factory default configuration after saving a backup of the current committed configuration to the local file system. If you click **Cancel** any time in the wizard before completing the configuration, the current rolls back the configuration to the current committed state.

2. For standard mode and passive mode, complete the configuration according to the guidelines provided in [Table 106 on page 240](#).

NOTE:

- If you select Cluster (HA) Mode, for the configuration information see [“Configure Cluster \(HA\) Mode” on page 262](#).
- In the Setup wizard, root password is mandatory and all the other options are optional. In the passive mode, management interface, TAP interface, and services are mandatory.

3. Click **Finish**.

A successful message appears and the device configuration mode of your choice is set up.

NOTE:

- Once the configuration is complete, the entire configuration is committed to the device and a successful message appears. If the commit fails, the CLI displays an error message and you remain at the wizard's last page. If required, you can change the configuration until the commit is successful.
- If the connectivity is lost during commit or if commit takes more than a minute, a message will be displayed with configured IP address to access J-Web again.
- For SRX300 line of devices and SRX550M devices, an additional message will be displayed about the device reboot if you have enabled Juniper Sky ATP or Security Intelligence services. For other SRX devices, the device will not reboot.

Table 106: Setup Wizard Configuration

| Field | Action |
|---------------------------|--|
| Device & Users | |
| System Identity | |
| Hostname | <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> |
| Allow root user SSH login | <p>Enable this option to allow the root login (to the device) using SSH.</p> |
| Device Password | |

Table 106: Setup Wizard Configuration (continued)

| Field | Action |
|-------------------------------|--|
| 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> |
| Confirm Password | Reenter the password. |
| User Management | <p>You can create additional user accounts in addition to root user account.</p> <p>NOTE: We recommend that you do not use root user account as a best practice to manage your devices.</p> <p>To add additional user accounts and to assign them a role:</p> <ol style="list-style-type: none"> 1. Click +. 2. Enter the details in the following fields: <ul style="list-style-type: none"> • Username—Enter a username. Do not use space or symbols. • Password—Enter a password. You can use alphanumeric characters and special characters; the minimum length is six characters. • Confirm Password—Reenter the password. • Role—Select a role from the list. Available options are: Super User, Operator, Read-Only, and Unauthorized. 3. Click the tick mark. <p>You can edit the user details using the pencil icon or select the existing user and delete it using the delete icon.</p> |
| Time & DNS Servers | |
| Set Date & Time | |
| Set system time | Select either NTP server or Manual to configure the system time. |

Table 106: Setup Wizard Configuration (continued)

| Field | Action |
|---|--|
| Date and Time | Select the date and time (in DD-MM-YYYY and HH:MM:SS 24-hour or AM/PM formats) to configure the system time manually. |
| NTP Server | <p>Enter a hostname or IP address of the NTP server.</p> <p>Once the system is connected to the network, the system time is synced with the NTP server time.</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> |
| Time zone | Select an option from the list. By default, device current time (UTC) is selected. |
| DNS Servers | |
| DNS Server 1 | <p>By default, 8.8.8.8 is displayed.</p> <p>NOTE: Entering a new IP address for the DNS server will remove the default IP address.</p> |
| DNS Server 2 | <p>Enter an IP address for the DNS server. By default, 8.8.4.4 is displayed.</p> <p>NOTE: Entering a new IP address for the DNS server will remove the default IP address.</p> |
| Management Interface | |
| Management Interface | |
| <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 106: Setup Wizard Configuration (*continued*)

| Field | Action |
|---|---|
| Management Port | <p>Select an option 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 TAP mode, it is mandatory to configure a management port. J-Web needs a management port for viewing generated report. |
| IPv4 | |
| <p>NOTE: Click Email it to self to get the newly configured IPv4 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 | Enter a subnet mask for the IPv4 address. |
| Static Route | Enter an IPv4 address for the static route to route to the other network devices. |
| Static Route Subnet Mask | Enter a subnet mask for the static route IPv4 address. |
| 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 to route to the other network devices. |

Table 106: Setup Wizard Configuration (*continued*)

| Field | Action |
|----------------------------|---|
| 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 not available if the management port is fxp0. If the management port is not fxp0, a new dedicated functional management zone is created and the configures access protocols are added to the zone.
- In the Setup wizard, you cannot add any additional protocols.

| | |
|---------|---|
| HTTPS | Select this option for the web management using HTTP secured by SSL. NOTE: By default, this option is selected. |
| SSH | Select this option for the SSH service. NOTE: By default, this option is selected. |
| Ping | Select this option for the internet control message protocol. NOTE: By default, this option is selected. |
| DHCP | Select this option for the Dynamic Host Configuration Protocol. |
| Netconf | Select this option for the NETCONF Service. |

Zones & Interfaces—For Standard Mode

Zones & Interfaces

| | |
|-------------|--|
| Zone Name | View the zone name populated from your device factory default settings. NOTE: For Standard mode, trust and untrust zones are created by default even if these zones are not available in the factory default settings. |
| Interfaces | View the interfaces name populated from your device factory default settings. |
| Description | Enter the description for zone and interfaces. |

Table 106: Setup Wizard Configuration (*continued*)

| Field | Action |
|--|---|
| Edit | <p>Select a zone and click the pencil icon at the right corner of the table to modify the configuration.</p> <p>For more information on editing zones, see Table 4 on page 17 and Table 5 on page 22.</p> |
| Search | Click the search icon at the right corner of the table to quickly locate a zone or an interface. |
| Detailed View | <p>Hover over the zone name and click the Detailed View icon to view the zone and interface details.</p> <p>You can also click More and select Detailed View for the selected zone.</p> |
| Zones & Interfaces—For Passive Mode | |
| TAP Interface | |
| Physical Interface | <p>Select an interface from the list.</p> <p>You can select up to a maximum of eight interfaces.</p> <p>For Passive mode, untrust zone will be displayed.</p> |
| Internet Connectivity | |
| <p>NOTE: Your device must have internet connectivity to use IPS, AppSec, Web filtering, Juniper Sky ATP, and Security threat intelligence services.</p> | |
| Name | <p>View the zone name populated from your device factory default settings.</p> <p>NOTE: For Passive mode, untrust zone is created by default.</p> |
| Interfaces | View the interfaces name populated from your device factory default settings. |
| Description | Enter the description for zone and interfaces. |

Table 106: Setup Wizard Configuration (*continued*)

| Field | Action |
|--------------------------|---|
| Edit | <p>Select a zone and click the pencil icon at the right corner of the table to modify the configuration.</p> <p>For more information on editing zones, see Table 4 on page 17 and Table 5 on page 22.</p> |
| Search | Click the search icon at the right corner of the table to quickly locate a zone or an interface. |
| Detailed View | <p>Hover over the zone name and click the Detailed View icon to view the zone and interface details.</p> <p>You can also click More and select Detailed View for the selected zone.</p> |
| Default Gateway | |
| Default Gateway (IPv4) | Enter the IPv4 address of the default gateway. |
| Default Gateway (IPv6) | Enter the IPv6 address of the default gateway. |
| Security Policies | |
| Reporting | |
| On-Box Reporting | <p>Enable this option to deploy logging and reporting.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • We recommend you use Stream mode logging to syslog server. • This option is supported only for the TAP mode. |
| Services | |
| UTM | Enable this option for configuring UTM services. |
| License | <p>Enter UTM 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 UTM services, your device must have internet connectivity from a revenue interface. |

Table 106: Setup Wizard Configuration (continued)

| Field | Action |
|-----------------------|---|
| UTM Type | <p>Select an option to configure UTM 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 | <p>Enable this option to install the IPS signatures.</p> <ul style="list-style-type: none"> • IPS Policy—Displays the IPS policy wizard name. • License—Enter the license key and click Install License to add a new license. <p>NOTE: The installation process may take few minutes.</p> <ul style="list-style-type: none"> • IPS Signature—Click Browse to navigate to the IPS signature package folder and select it. Click Install to install the selected IPS signature package. <p>NOTE: You can download the IPS signature offline package at https://support.juniper.net/support/downloads/.</p> |
| Sky ATP | <p>Enable this option to use Juniper Sky ATP services.</p> <p>NOTE: After the Juniper Sky ATP configuration is pushed, only the SRX300 line of devices and SRX550M devices are rebooted. Your device must have internet connectivity to enable Juniper Sky ATP enrollment process through J-Web.</p> |
| 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 Sky ATP enrollment process through J-Web.</p> |

Table 106: Setup Wizard Configuration (*continued*)

| Field | Action |
|---------------|---|
| User Firewall | <p>Enable this option to use user firewall services.</p> <ul style="list-style-type: none"> • 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. |

Inspect Pass-through Tunnel

NOTE: This option is supported only for the TAP mode.

| | |
|-------|--|
| IP-IP | Enable this option for the SRX Series device to inspect pass through traffic over an IP-IP tunnel. |
| GRE | Enable this option for the SRX Series device to inspect pass through traffic over a GRE tunnel. |

Security Policy

NOTE: The table lists the security policy along with the selected advanced security settings.

| | |
|-------------|--|
| Policy Name | <p>Name of the policy.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • If you are in Standard mode, trust-to-untrust policy is created by default. • If you are in TAP mode, tap-policy is created by default. |
| From Zone | <p>Name of the source zone.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • If you are in Standard mode, permits all traffic from the trust zone. • If you are in TAP mode, permits all traffic from the tap zone. |
| To Zone | <p>Name of the destination zone.</p> <ul style="list-style-type: none"> • If you are in Standard mode, permits all traffic from the trust zone to the untrust zone. • If you are in 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. |

Table 106: Setup Wizard Configuration (*continued*)

| Field | Action |
|-------------|--|
| 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. |
| Services | Name of the configured advanced security settings. |

Table 107: Edit Trust Zone

| Field | Action |
|----------------------------|--|
| General Information | |
| Name | Displays the zone name. |
| Description | Enter the description for the zone. |
| Application Tracking | Enables this option to provide application tracking support to the zone. |
| Source Identity Log | Enables this option to trigger user identity logging when that zone is used as the source zone in a security policy. |
| Services | By default, this option is enabled. You can disable if required. all—Specifies all system services. |
| Protocols | By default, this option is enabled. You can disable if required. all—Specifies all protocol. |
| Interfaces | |
| Name | Displays the name of the interface |
| Description | Displays the description of the interface. |
| IP Address | Displays the IP address of the interface. |
| VLAN | Displays the VLAN name. |

Table 107: Edit Trust Zone (continued)

| Field | Action |
|-----------|--|
| Services | Displays the system service option selected. |
| Protocols | Displays the protocol option selected. |

Table 107: Edit Trust Zone (continued)

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

Table 107: Edit Trust Zone (continued)

| Field | Action |
|-------|--|
| | <p>To add a switching or a routing interface:</p> <ol style="list-style-type: none"> Click +. <p>The Add Interface page appears.</p> <ol style="list-style-type: none"> Enter the following details: <ul style="list-style-type: none"> General (fields for switching interface): <ul style="list-style-type: none"> Type (family)—Select Switching. <p>NOTE: This option will be available for only SRX300 line of devices, SRX550M, and SRX1500 devices. For SRX5000 line of devices, SRX4100, SRX4200, SRX4600, and vSRX devices, the Type (family) field is not available.</p> <ul style="list-style-type: none"> Routing Interface (IRB) Unit—Enter the IRB unit. Description—Enter the description for the interface. General (fields for routing interface): <ul style="list-style-type: none"> Type (family)—Select Routing. <p>For SRX5000 line of devices, SRX4100, SRX4200, SRX4600, and vSRX devices, the Type (family) field is not available.</p> <ul style="list-style-type: none"> Interface Name—Select an option from list. Interface Unit—Enter the Inet unit. <p>NOTE: VLAN tagging is enabled automatically if the interface unit is higher than zero.</p> <ul style="list-style-type: none"> Description—Enter the description for the interface. VLAN ID—Enter the VLAN ID. <p>NOTE: VLAN ID is mandatory if the interface unit is higher than zero.</p> Interfaces—Select an interface from the Available column and move it to the Selected column. <p>NOTE: This option is available only for the Switching family type.</p> <ul style="list-style-type: none"> IPv4: <ul style="list-style-type: none"> IPv4 Address—Enter a valid IPv4 address for the switching or the routing interface. Subnet Mask—Enter a subnet mask for the IPv4 address. |

Table 107: Edit Trust Zone (continued)

| Field | Action |
|-------|--|
| | <ul style="list-style-type: none">● IPv6:<ul style="list-style-type: none">● IPv6 Address—Enter a valid IPv6 address for the switching or the routing interface.● Subnet Prefix—Enter a subnet prefix for the IPv6 address.● VLAN Details:<p>NOTE: This option is available only for the Switching family type.</p><ul style="list-style-type: none">● VLAN Name—Enter a unique name for the VLAN.● VLAN ID—Enter the VLAN ID. |

Table 107: Edit Trust Zone (continued)

| Field | Action |
|-------|--|
| | <ul style="list-style-type: none">● DHCP Local Server:<ul style="list-style-type: none">● DHCP Local Server—Enable this option to configure the switch to function as an extended DHCP local server.● DHCP Pool Name—Enter the DHCP pool name.● DHCP Pool Range (Low)—Enter an IP address that is the lowest address in the IP address pool range.● DHCP Pool Range (High)—Enter an IP address that is the highest address in the IP address pool range.<p>NOTE: This address must be greater than the address specified in DHCP Pool Range (Low).</p>● Propagate Settings from—Select an interface on the router through which the resolved DHCP queries are propagated to the DHCP pool. |

Table 107: Edit Trust Zone (continued)

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

Table 107: Edit Trust Zone (continued)

| Field | Action |
|-------|--|
| | <ul style="list-style-type: none"> • 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. <p>• Protocols—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 107: Edit Trust Zone (continued)

| Field | Action |
|--------|--|
| Edit | <p>Select an interface and click the edit icon at the top right corner of the table.</p> <p>The Edit Interface page appears with editable fields.</p> <p>NOTE: As interface name is prepopulated, you cannot edit it.</p> |
| Delete | <p>Select an interface and click the delete icon at the top 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 | <p>Click the search icon at the top right corner of the table and enter partial text or full text of the keyword in the search bar.</p> <p>The search results are displayed.</p> |

Table 108: Edit Untrust Zone

| Field | Action |
|----------------------------|--|
| General Information | |
| Name | Displays the zone name as untrust. |
| Description | Enter the description for the zone. |
| Application Tracking | Enables this option to provide application tracking support to the zone. |
| Source Identity Log | Enables this option for system services. |
| Interfaces | |
| Name | Displays the name of the physical interface |
| Description | Displays the description of the interface. |
| Address Mode | Displays the type of address mode. |
| IP Address | Displays the IP address of the interface. |

Table 108: Edit Untrust Zone (*continued*)

| Field | Action |
|-----------|--|
| Services | Displays the system service option selected. |
| Protocols | Displays the protocol option selected. |

Table 108: Edit Untrust Zone (continued)

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

Table 108: Edit Untrust Zone (continued)

| Field | Action |
|-------|--|
| | <p>To add an interface to the untrust zone:</p> <ol style="list-style-type: none"> Click +. <p>The Add Interface page appears.</p> <ol style="list-style-type: none"> Enter the following details: <ul style="list-style-type: none"> General: <ul style="list-style-type: none"> Interface Name—Select an interface from the list. Interface Unit—By default 0 will be populated. You can change the unit value if required. 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. <p>NOTE: PPPoE (PAP) and PPPoE (CHAP) are not supported for SRX5000 line of devices and if any of the devices are in passive mode.</p> <ul style="list-style-type: none"> Username—Enter a username for PPPoE (PAP) or PPPoE (CHAP) authentication. Password—Enter a password for PPPoE (PAP) or PPPoE (CHAP) authentication. IPv4: <p>NOTE: This option is available only for the Static IP address mode.</p> <ul style="list-style-type: none"> IPv4 Address—Enter a valid IPv4 address for the interface. Subnet Mask—Enter a subnet mask for the IPv4 address. IPv6: <p>NOTE: This option is available only for the Static IP address mode.</p> <ul style="list-style-type: none"> IPv6 Address—Enter a valid IPv6 address for the interface. Subnet Prefix—Enter a subnet prefix for the IPv6 address. |

Table 108: Edit Untrust Zone (*continued*)

| Field | Action |
|--------|--|
| | <ul style="list-style-type: none"> • 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. |
| Edit | <p>Select an interface and click the edit icon at the top right corner of the table.</p> <p>The Edit Interface page appears with editable fields.</p> <p>NOTE: As interface name is prepopulated, you cannot edit it.</p> |
| Delete | <p>Select an interface and click the delete icon at the top 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 | <p>Click the search icon at the top right corner of the table and enter partial text or full text of the keyword in the search bar.</p> <p>The search results are displayed.</p> |

Release History Table

| Release | Description |
|------------------------|--|
| 20.1R1 | Starting in Junos OS Release 20.1R1, you can configure SRX380 device using Setup Wizard. |

RELATED DOCUMENTATION

| [Start J-Web](#) | 3

Configure Cluster (HA) Mode

You are here: **Device Administration** > **Setup**.

The Junos OS provides high availability on SRX Series device by using chassis clustering. SRX Series Services Gateways can be configured to operate in cluster mode, where a pair of devices can be connected together and configured to operate like a single node, providing device, interface, and service level redundancy.

NOTE: Starting in Junos OS Release 20.1R1, you can configure SRX380 device using Cluster (HA) Setup.

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 devices are in factory default. You can also create HA using the same wizard from Device Administration > Setup when the devices are already in the network.

NOTE: In the factory default settings, a warning message is displayed in SRX300, SRX320, SRX320-POE, SRX340, SRX345, and SRX380 devices to disconnect the ports between the two nodes. This is to avoid displaying the details of the other nodes.

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 > Setup.**

To set up cluster (HA):

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

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 device. It shows a graphical representation for primary unit (Node 0) and secondary unit (Node 1) and guides you to first configure the primary unit (node 0).

2. Select **Yes, this is the primary unit (Node 0)**, to select the unit.

NOTE: If you have already configured the primary node settings, then select **No, this is the secondary unit (Node 1)** and follow the instructions from Step 8.

3. Click **Next**.
4. To configure the primary unit, complete the configuration according to the guidelines provided in [Table 109 on page 263](#).

Table 109: 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. |

Table 109: Primary Unit Configuration (*continued*)

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

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)

Table 109: Primary Unit Configuration (*continued*)

| Field | Description | Action |
|----------------------------|--|---|
| Node 0 Management IPv6 | Specifies the management IPv6 address of node 0. | Enter a valid IPv6 address for the management interface. |
| Node 0 Subnet Prefix | Specifies subnet prefix for IPv6 address. | Enter a subnet prefix for the IPv6 address. |
| Node 1 Management IPv6 | Specifies the management IPv6 address of node 1. | Enter a valid IPv6 address for the management interface. |
| Node 1 Subnet Prefix | Specifies subnet prefix for IPv6 address. | Enter a subnet prefix for the IPv6 address. |
| 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 109: 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. |
| Node 1 Port | Optional. Specifies port number on which to configure the control port. | Select an option from the list. |
| Save Backup (Optional) | | |

Table 109: Primary Unit Configuration (*continued*)

| Field | Description | Action |
|-------------------------|---|---|
| Save Backup (to client) | <p>Saves backup of the current configuration to the client local machine.</p> <p>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.</p> | Enable the option to save the backup file of your settings. |

- Click **Reboot and Continue** to restart the primary unit to configure chassis cluster.
- After rebooting the primary unit (node 0), connect to the management port of the secondary unit to switch to the secondary unit.
- 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.
- To configure the secondary unit, complete the configuration according to the guidelines provided in [Table 110 on page 267](#).

Table 110: Secondary Unit Configuration

| Field | Description | Action |
|-----------------------------------|---|---|
| Secondary Unit Information | | |
| Cluster ID | <p>Specifies the number by which a cluster is identified.</p> <p>NOTE: Cluster ID must be same for both primary and secondary units.</p> | 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. |

Table 110: Secondary Unit Configuration (*continued*)

| Field | Description | Action |
|---|---|---|
| Control Ports | | |
| NOTE: This option is available only for SRX5600 and SRX5800 devices. | | |
| Dual Link | Provides redundant link for failover. | <p>By default, this option is disabled.</p> <p>Once you enable dual link option, the following fields appear:</p> <ul style="list-style-type: none"> • Link 1 <ul style="list-style-type: none"> • Node 0 FPC—Select an option from the list. • Node 0 Port—Select an option from the list. • Node 1 FPC. • Node 1 Port. • Link 2 (Optional) <ul style="list-style-type: none"> • Node 0 FPC—Select an option from the list. • Node 0 Port—Select an option from the list. • Node 1 FPC. • Node 1 Port. |
| Node 0 FPC | Specifies FPC slot number on which to configure the control port. | Select an option from the list. |
| Node 0 Port | Specifies port number on which to configure the control port. | Select an option from the list. |
| Node 1 FPC | Optional. Specifies FPC slot number on which to configure the control port. | Select an option from the list. |
| Node 1 Port | Optional. Specifies port number on which to configure the control port. | Select an option from the list. |
| Save Backup (Optional) | | |

Table 110: Secondary Unit Configuration (*continued*)

| Field | Description | Action |
|-------------------------|---|---|
| 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 the Cluster Status step in the wizard.

NOTE:

- J-Web uses **show chassis cluster status** to verify control link status. Number on the link signifies if it is single (1) or dual links (2).

The control and fabric link status colors are as follows:

- Green—Indicates that the links are up.
- Red—Indicates that the links are down.
- Orange—Indicates that one of the dual links is up.
- Grey—Indicates that the fabric link is not configured.
- If chassis cluster is not connected, then the connection is failed and the all possible failure reasons will be displayed. For information on troubleshooting tips, see [Juniper Knowledge Search](#).
- You can configure fabric link only after the chassis cluster is formed. For the first time configuration, the chassis status displays as **The fabric ports links is not yet configured**.

12. To configure fabric link, complete the configuration according to the guidelines provided in [Table 111 on page 270](#).

Table 111: 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 112 on page 270](#).

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

Table 112: Add Reth Interface

| Field | Description | Action |
|-----------|------------------------------------|----------------------------------|
| RETH Name | Specifies the reth interface name. | Enter a name for reth interface. |

Table 112: Add Reth Interface (*continued*)

| Field | Description | Action |
|-------------------------|--|---|
| Node 0 Interfaces | Specifies the list of Node 0 interfaces. | Select an interface from the Available column and move it to the Selected column. |
| Node 1 | Specifies the Node 1 interfaces based on the node 0 interfaces. | - |
| Advance Settings | | |
| LACP Configuration | Optional. Configure Link Aggregation Control Protocol (LACP). | - |
| LACP Mode | Optional. Specifies the LACP mode. Available options are: <ul style="list-style-type: none"> • active—Initiate transmission of LACP packets. • passive—Respond to LACP packets. • periodic—Interval for periodic transmission of LACP packets. | Select an option from the list. |
| Periodicity | Optional. Specifies the interval at which the interfaces on the remote side of the link transmit link aggregation control protocol data units (PDUs). Available options are: <ul style="list-style-type: none"> • fast—Transmit link aggregation control PDUs every second. • slow—Transmit link aggregation control PDUs every 30 seconds. | Select an option from the list. |
| Description | Optional. Specifies the description for LACP. | Enter a description. |
| VLAN Tagging | Optional. Specifies whether or not to enable VLAN tagging. | Enable this option. |
| 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 113 on page 272](#).

Table 113: Add Reth Logical Interface

| Field | Description | Action |
|--------------------------------|--|---------------------------------------|
| General | | |
| Reth Interface Name | Specifies the name of the reth interface. | Enter a name for the reth interface. |
| Logical Interface Unit | Specifies the logical interface unit. | Enter the logical interface unit. |
| Description | Specifies the description of the reth interface. | Enter the description. |
| VLAN ID | Optional. Specifies the VLAN ID. | Enter the VLAN ID. |
| IPv4 Address | | |
| IPv4 Address | Specifies the IPv4 address. | Click + and enter a valid IP address. |
| Subnet Mask | Specifies the subnet mask for IPv4 address. | Enter a valid subnet mask. |
| IPv6 Address (Optional) | | |
| IPv6 Address | Specifies the IPv6 address. | Enter a valid IP address. |
| Prefix Length | Specifies the number of bits set in the subnet mask. | Enter the prefix length. |

18. Click **OK**.

19. To configure zones, complete the configuration according to the guidelines provided in [Table 114 on page 273](#).

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 114: 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. |
| 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 | | |

Table 114: Create Zones (*continued*)

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

Release History Table

| Release | Description |
|------------------------|--|
| 20.1R1 | Starting in Junos OS Release 20.1R1, you can configure SRX380 device using Cluster (HA) Setup. |

RELATED DOCUMENTATION

[Configure PPPoE](#) | 459

Cluster Management

IN THIS CHAPTER

- [About the Cluster Configuration Page | 275](#)
- [Edit Node Settings | 277](#)
- [Add an HA Cluster Interface | 278](#)
- [Edit an HA Cluster Interface | 280](#)
- [Delete HA Cluster Interface | 280](#)
- [Add a Redundancy Group | 281](#)
- [Edit a Redundancy Group | 283](#)
- [Delete Redundancy Group | 283](#)

About the Cluster Configuration Page

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 277](#).
- Add an HA cluster interface. See [“Add an HA Cluster Interface” on page 278](#).
- Edit an HA cluster interface. See [“Edit an HA Cluster Interface” on page 280](#).
- Delete HA cluster interface. See [“Delete HA Cluster Interface” on page 280](#).
- Add a redundancy group. See [“Add a Redundancy Group” on page 281](#).
- Edit a redundancy group. See [“Edit a Redundancy Group” on page 283](#).
- Delete redundancy group. See [“Delete Redundancy Group” on page 283](#).

Field Descriptions

Table 115 on page 276 and Table 116 on page 276 describes the fields on the Cluster Configuration page.

Table 115: 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. |
| 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 | Displays the state of the redundancy group. <ul style="list-style-type: none"> • Primary—Redundancy group is active. • Secondary—Redundancy group is passive. |

Table 116: Fields on the HA Cluster Settings Page

| Field | Action |
|------------------------------|---|
| Interfaces | |
| Global Settings | To configure the global settings: <ol style="list-style-type: none"> 1. Click Global Settings at the upper right side 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. |

Table 116: Fields on the HA Cluster Settings Page (*continued*)

| Field | Action |
|-------------------------|--|
| Redundancy Group | Displays the redundancy group. |
| 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 side of the page.

The Edit Node Settings page appears with editable fields.

Table 117: Fields on the Edit Node Settings Page

| Field | Description |
|----------------------|---|
| Node Settings | |
| Host Name | Enter the name of the host. |
| Backup Router | Enter the backup router address to be used during failover. |
| Destination | |

Table 117: Fields on the Edit Node Settings Page (*continued*)

| Field | Description |
|------------------|--|
| IP | <p>Enter the destination IP address.</p> <p>Click + to add the destination IP address or select an existing IP address and click X to delete it.</p> |
| Interface | |
| Interface | <p>Select an interface available for the router from the list.</p> <p>NOTE: You can add and edit two interfaces for each fabric link.</p> |
| 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](#) | 275

Add an HA Cluster Interface

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

To add an HA cluster interface:

1. Click + on the upper right side of the Cluster Configuration page.
The Add HA Cluster Interface page appears.
2. Complete the configuration according to the guidelines provided in [Table 118 on page 279](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 118: Fields on the Add HA Cluster Interface Page

| Field | Action |
|-----------------------------|--|
| Fabric Link | |
| Fabric Link 0 (fab0) | |
| Interface | <p>Enter the interface IP address for fabric link 0 and click + to add it.</p> <p>Select an existing interface and click X to delete the interface.</p> |
| Fabric Link 1 (fab1) | |
| Interface | <p>Enter the interface IP address for fabric link 1 and click + to add it.</p> <p>Select an existing interface and click X to delete the interface.</p> |
| 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 | <p>Select an option from list:</p> <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. |
| X | Select one or more existing redundant Ethernet configurations and click X to delete it. |

RELATED DOCUMENTATION

[Edit an HA Cluster Interface | 280](#)
[Delete HA Cluster Interface | 280](#)
[Add a Redundancy Group | 281](#)

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 side 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 278](#).

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

RELATED DOCUMENTATION

[About the Cluster Configuration Page | 275](#)

[Delete HA Cluster Interface | 280](#)

Delete HA Cluster Interface

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

To delete HA cluster interface:

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 side of the page.
3. Click **Yes** to delete or click **No** to retain the HA cluster interface.

RELATED DOCUMENTATION

[Add an HA Cluster Interface | 278](#)

[Edit an HA Cluster Interface | 280](#)

Add a Redundancy Group

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

To add a redundancy group:

1. Click **+** on the upper right side of the Cluster Configuration page.
The Add Redundancy Group page appears.
2. Complete the configuration according to the guidelines provided in [Table 119 on page 281](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 119: 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). |
| Gratuitous ARP Count | Enter a value. The range is 1 through 16. The default is 4. 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. |
| node0 priority | Enter the node priority number as 0 for a redundancy group. |
| 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. |

Table 119: Fields on the Add Redundancy Group Page (*continued*)

| Field | Action |
|---------------------------------------|---|
| 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. |
| 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 | 283](#)
[Delete Redundancy Group | 283](#)
[About the Cluster Configuration Page | 275](#)

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 side 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 281](#).

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

RELATED DOCUMENTATION

[Delete Redundancy Group | 283](#)

[About the Cluster Configuration Page | 275](#)

Delete Redundancy Group

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

To delete redundancy groups:

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 side of the page.
3. Click **Yes** to delete or click **No** to retain the redundancy group.

RELATED DOCUMENTATION

[Add a Redundancy Group | 281](#)

[Edit a Redundancy Group | 283](#)

User Management

IN THIS CHAPTER

- [About the User Management Page | 284](#)
- [Add a User | 287](#)
- [Edit a User | 289](#)
- [Delete User | 289](#)

About the User Management Page

You are here: **Device Administration** > **User Management**.

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:

- Add a user. See [“Add a User” on page 287](#).
- Edit a user. See [“Edit a User” on page 289](#).
- Delete a user. See [“Delete User” on page 289](#).

Field Descriptions

[Table 120 on page 284](#) describes the fields on the User Management page.

Table 120: Fields on the User Management Page

| Field | Description |
|--------------|-------------|
| User Details | |

Table 120: Fields on the User Management Page (*continued*)

| Field | Description |
|---------------------------------|--|
| User Details | <p>Provides the users details to the device's local database. The options available are:</p> <ul style="list-style-type: none"> • Add • Edit • Delete • Search • Filter |
| 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>Specifies the details of RADIUS servers.</p> <p>Click Configure.</p> <p>To add a new RADIUS server, click +. Then enter the details specified below and click OK.</p> <ul style="list-style-type: none"> • IP Address—Enter the server's 32-bit IP address. • Password—Enter the secret password for the server. • Confirm Password—Re-enter the secret password for the server. • Server Port—Enter an appropriate port. • Source Address—Enter the source IP address of the server. • Time out—Specify the amount of time (in seconds) the device should wait for a response from the server. • Retry Attempts—Specify the number of times that the server should try to verify the user's credentials. <p>To delete an existing RADIUS server, select it and click Delete.</p> |

Table 120: Fields on the User Management Page (*continued*)

| Field | Description |
|---|--|
| TACACS | |
| TACACS Servers | <p>Specifies the details of TACACS servers.</p> <p>Click Configure.</p> <p>To add a new TACACS server, click +. Then enter the details specified below and click OK.</p> <ul style="list-style-type: none"> • IP Address—Enter the server's 32-bit IP address. • Password—Enter the secret password for the server. • Confirm Password—Re-enter the secret password for the server. • Server Port—Enter an appropriate port. • Source IP Address—Enter the source IP address of the server. • Time out—Specify the amount of time (in seconds) the device should wait for a response from the server. <p>To delete an existing TACACS server, select it and click Delete.</p> |
| Password Settings | |
| <p>NOTE:</p> <ul style="list-style-type: none"> • Starting in Junos OS Release 19.1R1, the User Management configuration supports the password settings range. • J-Web interface does not support configuring the number of characters by which the new password should be different from the existing password. | |
| Minimum Reuse | <p>Starting in Junos OS Release 19.1R1, the Minimum Reuse option is supported.</p> <p>Click top or bottom arrow to specify the minimum number of old passwords that you want to use. Range: 1-20.</p> |
| Maximum Lifetime | <p>Starting in Junos OS Release 19.1R1, the Maximum Lifetime option is supported.</p> <p>Click top or bottom arrow to specify the maximum lifetime of your password in days. Range: 30-365.</p> |

Table 120: Fields on the User Management Page (continued)

| Field | Description |
|------------------|--|
| Minimum Lifetime | <p>Starting in Junos OS Release 19.1R1, the Minimum Lifetime option is supported.</p> <p>Click top or bottom arrow to specify the minimum lifetime of your password in days. Range: 1-30.</p> |

Release History Table

| Release | Description |
|------------------------|--|
| 19.1R1 | Starting in Junos OS Release 19.1R1, the User Management configuration supports the password settings range. |
| 19.1R1 | Starting in Junos OS Release 19.1R1, the Minimum Reuse option is supported. |
| 19.1R1 | Starting in Junos OS Release 19.1R1, the Maximum Lifetime option is supported. |
| 19.1R1 | Starting in Junos OS Release 19.1R1, the Minimum Lifetime option is supported. |

RELATED DOCUMENTATION

| |
|-----------------------------------|
| Add a User 287 |
| Edit a User 289 |
| Delete User 289 |

Add a User

You are here: **Device Administration > User Management.**

To add a user:

1. Click the add icon (+) on the upper right side of the User Details page.
The Create User page appears.
2. Complete the configuration according to the guidelines provided in [Table 121 on page 288](#).

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

Table 121: Fields on the Add 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 login password for the user. |
| Role | Select the user's access privilege from the following options: <ul style="list-style-type: none"> • super-user • operator • read-only • unauthorized • lsys • tenant |

RELATED DOCUMENTATION

[About the User Management Page | 284](#)

[Edit a User | 289](#)

[Delete User | 289](#)

Edit a User

You are here: **Device Administration** > **User Management**.

To edit a user:

1. Select an existing user profile that you want to edit on the User Profiles page.
2. Click the pencil icon available on the upper right side of the page.

The Edit User page appears with editable fields. For more information on the options, see [“Add a User” on page 287](#).

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

RELATED DOCUMENTATION

[About the User Management Page | 284](#)

[Add a User | 287](#)

[Edit a User | 289](#)

Delete User

You are here: **Device Administration** > **User Management**.

To delete users:

1. Select one or more users that you want to delete from the User Profile page.
2. Click the delete icon available on the upper right side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the User Management Page | 284](#)

[Add a User | 287](#)

[Edit a User | 289](#)

Certificate Management—Device Certificates

IN THIS CHAPTER

- [About the Device Certificates Page | 290](#)
- [Import a Device Certificate | 291](#)
- [Export a Device Certificate | 293](#)
- [Add a Device Certificate | 294](#)
- [Delete Device Certificate | 296](#)
- [View Details of a Device Certificate | 297](#)
- [Search Text in the Device Certificates Table | 300](#)

About the Device Certificates Page

You are here: **Device Administration** > **Certificate Management** > **Device Certificates**.

Manage the device certificates to authenticate Secure Socket Layer (SSL). SSL uses public-private key technology that requires a paired private key and an authentication certificate for providing the SSL service. SSL encrypts communication between your device and the Web browser with a session key negotiated by the SSL server certificate.

You can perform the following tasks:

- Import a certificate to manually load externally generated certificates or CSR. See [“Import a Device Certificate” on page 291](#).

NOTE: You must obtain the private key, passphrase, and the signed certificate from certificate authority (CA) server.

- Export a local certificate or CSR from the default location to a specific location within the device. See [“Export a Device Certificate” on page 293](#).
- View the details of a certificate. See [“View Details of a Device Certificate” on page 297](#).
- Generate a certificate. See [“Add a Device Certificate” on page 294](#).

- Delete a certificate. See [“Delete Device Certificate” on page 296](#).
- Search for text in a device certificate table. See [“Search Text in the Device Certificates Table” on page 300](#).
- Filter the device certificates information based on select criteria. To do this, select the filter icon at the top right-hand corner of the table. The columns in the grid change to accept filter options. Type the filter options; the table displays only the data that fits the filtering criteria.
- Show or hide columns in the Device Certificates table. To do this, use the Show Hide Columns icon in the top right corner of the page and select the options you want to show or deselect to hide options on the page

[Table 122 on page 291](#) provides the details of the fields of the Device Certificates page.

Table 122: Fields on Device Certificates Page

| Field | Description |
|------------------|--|
| Certificate ID | Displays the certificate ID. Certificate ID is a unique value across the device. This will be used to create a key pair along with the algorithm to associate with the key. |
| Issuer Org | Displays the details of the authority that issued the certificate. |
| Status | Displays whether the status of the certificate is valid, expired, and so on. |
| Expiration Date | Displays certificate expiration date. |
| Encryption Type | Displays whether the algorithm of the certificate is RSA, DSA, or ECDSA encryption. |
| Signature Status | Displays whether the status of the certificate is signed or in certificate signing request (CSR) stage. |

Import a Device Certificate

To import a device certificate:

1. Select **Device Administration > Certificate Management > Device Certificates**.
2. Click **Import**.
The Import Certificate page appears.
3. Complete the configuration according to the guidelines provided in [Table 123 on page 292](#).

4. Click **OK** to import the certificate.

You are taken to the Device Certificates page. If the certificate content that you imported is validated successfully, a confirmation message is displayed; if not, an error message is displayed.

After importing a certificate, you can use it when you create an SSL proxy profile and for IPsec VPN peers authentication.

5. Click **Cancel** to cancel your entries and returns to the Device Certificates page.

Table 123: Fields on the Import Certificate Page

| Field | Action |
|---------------------------|---|
| Type | Select an option to specify whether the certificate that you are importing is an Externally Generated Certificate or a CSR. |
| Certificate ID | Enter a unique value for the certificate ID for an externally generated certificate. Select an option from the list to specify the certificate ID for a CSR. |
| File path for Certificate | Click Browse to navigate to the path from where you want to import the certificate. |
| File path for Private Key | Click Browse to navigate to the path from where you want to import the private key. |
| Passphrase | Enter the passphrase used to protect the private key or key pair of the certificate file. |

RELATED DOCUMENTATION

| | |
|--|-----|
| About the Device Certificates Page | 290 |
| Export a Device Certificate | 293 |
| Add a Device Certificate | 294 |
| Delete Device Certificate | 296 |
| View Details of a Device Certificate | 297 |
| Search Text in the Device Certificates Table | 300 |

Export a Device Certificate

To export a device certificate:

1. Select **Device Administration > Certificate Management > Device Certificates**.
2. Click **Export**.

The Export Certificate page appears.

3. Complete the configuration according to the guidelines provided in [Table 124 on page 293](#).
4. Click **OK** to export the certificate.

Once you save or download the exported file(s), a confirmation message is displayed; if not, an error message is displayed.

Table 124: Fields on the Export Certificate Page

| Field | Action |
|--------------------|--|
| Type | Select an option from the list to specify whether the certificate that you are exporting is a Local Certificate or a CSR. |
| Certification Name | Select an option from the list for the local certificate name. |
| Certificate ID | This option is available only for CSR. Select an option from the list for the CSR certificate ID. |
| Format | Select an option from the list to specify whether the exporting certificate format is Privacy-Enhanced Mail (PEM) or Distinguished Encoding Rules (DER). |
| Key Pair | Enable or disable exporting key pair of a certificate. |
| Passphrase | Enter the passphrase to protect the private key or key pair of the certificate file. |

RELATED DOCUMENTATION

[About the Device Certificates Page | 290](#)

[Import a Device Certificate | 291](#)

[Add a Device Certificate | 294](#)

[Delete Device Certificate | 296](#)

[View Details of a Device Certificate | 297](#)

[Search Text in the Device Certificates Table | 300](#)

Add a Device Certificate

To add a device certificate:

1. Select **Device Administration > Certificate Management > Device Certificates**.

2. Click the add icon (+).

The Generate Certificate page appears.

3. Complete the configuration according to the guidelines provided in [Table 125 on page 294](#).

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

If you click **OK**, a new certificate with the provided configuration is created.

Table 125: Fields on the Generate Certificate Page

| Field | Action |
|----------------------------|--|
| Certificate Details | |
| Certificate Type | Select one of the certificate types from the list that you want to generate: <ul style="list-style-type: none">Local Self-Signed—Allows for use of SSL-based (Secure Sockets Layer) services without requiring that the user or administrator to undertake the considerable task of obtaining an identity certificate signed by a CA. Self-signed certificates are usually used for internal purpose.Local Certificate—Validates the identity of the security device. A local certificate imports or references an SSL certificate. |
| CA Profile Name | This option is available for a local certificate. Select one of the CA profile name from the list or click Create to add a CA Profile. For details on adding a CA profile, see the table in the <i>Adding a Certificate Authority Profile</i> section. |
| Certificate ID | Enter a unique value for the certificate ID. |

Table 125: Fields on the Generate Certificate Page (*continued*)

| Field | Action |
|-----------------|--|
| Encryption Type | <p>Select one of the types of encryption from the list:</p> <ul style="list-style-type: none"> • RSA Encryption • DSA Encryption <p>NOTE: The certificate cannot be used in SSL Proxy profile if it is generated using type DSA.</p> <ul style="list-style-type: none"> • ECDSA Encryption |
| Key Size | <p>Select one of the key sizes from the list:</p> <ul style="list-style-type: none"> • RSA encryption supports 1024 bits, 2048 bits, or 4096 bits. • DSA encryption supports 1024 bits, 2048 bits, or 4096 bits. • ECDSA encryption supports 256 bits, 384 bits, or 521 bits. |

Subject (Minimum of one field required)

| | |
|--------------------------|---|
| Domain Component | Enter the domain component that you want to be associated with the certificate. |
| Common Name | Enter a common name with the certificate. |
| Organizational Unit Name | Enter the organizational unit that you want to be associated with the certificate. |
| Organizational Name | Enter the organizational name that you want to be associated with this certificate. |
| Serial Number | Enter a serial number of the device. |
| Locality | Enter the locality name. |
| State | Enter the state name. |
| Country | Enter the country name. |

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 a user email address. |
| IPv4 Address | Enter the IPv4 address of the device. |

Table 125: Fields on the Generate Certificate Page (continued)

| Field | Action |
|---------------------|---|
| IPv6 Address | This option is available for a local certificate. Enter the IPv6 address of the device. |
| Advanced | |
| Digest | Select the digest from the list: <ul style="list-style-type: none">• For local Self-signed certificate (RSA/DSA/ECDSA) options are: None, SHA-1 digests, or SHA-256 digests.• For local certificate options are:<ul style="list-style-type: none">• RSA/DSA: None, SHA-1 digests, or SHA-256 digests• ECDSA: None, SHA-256 digests, or SHA-384 digests. |
| Signing Certificate | Enable or disable specifies that the certificate is used to sign other certificates. |

RELATED DOCUMENTATION

| |
|--|
| About the Device Certificates Page 290 |
| Import a Device Certificate 291 |
| Export a Device Certificate 293 |
| Delete Device Certificate 296 |
| View Details of a Device Certificate 297 |
| Search Text in the Device Certificates Table 300 |

Delete Device Certificate

To delete a device certificate:

1. Select **Device Administration > Certificate Management > Device Certificates**.
2. Select the certificate you want to delete.
3. On the upper right side of the Device Certificates page, click the delete icon to delete.

A confirmation window appears.

- 4. Click **Yes** to delete.

RELATED DOCUMENTATION


| |
|--|
| About the Device Certificates Page 290 |
| Import a Device Certificate 291 |
| Export a Device Certificate 293 |
| Add a Device Certificate 294 |
| View Details of a Device Certificate 297 |
| Search Text in the Device Certificates Table 300 |

View Details of a Device Certificate

To view the details of a device certificate:

- 1. Select **Device Administration > Certificate Management > Device Certificates**.
- 2. Select an existing certificate.
- 3. Select **More > Detailed View**.

The View Certificate page appears with the details of the certificate.

**NOTE:** When you hover over the certificate ID, a Detailed View icon appears before the certificate ID. You can also use this icon to view the certificate details.

- 4. Click **OK** after viewing the certificate details.

Table 126 on page 297 provides the field details of the certificate on the View Certificate page.

Table 126: Fields on the View Certificate Page

| Field | Action |
|---------------------|--------|
| Certificate Details | |

Table 126: Fields on the View Certificate Page (*continued*)

| Field | Action |
|---------------------------|--|
| Certificate ID | Displays the certificate ID. |
| Certificate Version | Displays the certificate revision number. |
| Certificate Type | Displays the certificate type. For example, Signed. |
| Encryption Type | Displays the encryption type. For example, RSA. |
| Key Size | Displays the key size of the encryption type. |
| Serial Number | Displays the unique serial number of the certificate. |
| Subject | |
| Domain Component | Displays the domain component associated with the certificate. |
| Common Name | Displays the common name associated with the certificate. |
| Organizational Unit Name | Displays the organizational unit associated with the certificate. |
| Organizational Name | Displays the organizational name associated with this certificate. |
| Serial Number | Displays the serial number of the device. |
| Locality | Displays the locality name. |
| State | Displays the state name. |
| Country | Displays the country name. |
| Subject Alt Name | |
| Domain Name | Displays the Fully Qualified Domain Name (FQDN). |
| Email | Displays the email ID of the certificate holder. |
| IPv4 Address | Displays the IPv4 address. |
| IPv6 Address | Displays the IPv6 address. |
| Issuer Information | |

Table 126: Fields on the View Certificate Page (*continued*)

| Field | Action |
|----------------------------|---|
| Common Name | Displays the issuer common name associated with the certificate. |
| Domain Component | Displays the issuer domain component associated with the certificate. |
| Organization Name | Displays the issuer organizational name. |
| Organization Unit Name | Displays the issuer organizational unit. |
| Locality Name | Displays the issuer locality name. |
| State or Province Name | Displays the issuer state or region name. |
| Validity | |
| Not Before | Displays the start time when the certificate becomes valid. |
| Not After | Displays the end time when the certificate becomes invalid. |
| Auto Re Enrollment | |
| Status | Displays whether the auto re enrollment is enabled or disabled. |
| Next Trigger Time | Displays the how long auto-reenrollment should be initiated before expiration. |
| Fingerprint | |
| MD5 | Displays the MD5 fingerprints to identify the certificate. |
| SHA1 | Displays the SHA-1 fingerprints to identify the certificate. |
| Signature Algorithm | |
| Algorithm | Displays whether the signature algorithm is SHA-1, SHA-256, or SHA-384 digest. |
| Distribution CRL | |
| URL | Displays the URL of the certificate revocation list (CRL) server. |
| LDAP | Displays the name of the location from which the CRL is retrieved through Lightweight Directory Access Protocol (LDAP). |

Table 126: Fields on the View Certificate Page (continued)

| Field | Action |
|--|---|
| Authority Information Access OCSP | |
| URL | Displays the URL of the Online Certificate Status Protocol (OCSP) server. |

RELATED DOCUMENTATION

| |
|--|
| About the Device Certificates Page 290 |
| Import a Device Certificate 291 |
| Export a Device Certificate 293 |
| Add a Device Certificate 294 |
| Delete Device Certificate 296 |
| Search Text in the Device Certificates Table 300 |

Search Text in the Device Certificates Table

You are here: **Device Administration > Certificate Management > Device Certificates.**

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

To search for text:

1. Enter partial text or full text of the keyword in the search bar and click the search icon.

The search results are displayed.

2. Click **X** next to a search keyword or click **Clear All** to clear the search results.

RELATED DOCUMENTATION

| |
|--|
| About the Device Certificates Page 290 |
| Import a Device Certificate 291 |
| Export a Device Certificate 293 |
| Add a Device Certificate 294 |

[Delete Device Certificate | 296](#)

[View Details of a Device Certificate | 297](#)

Certificate Management—Trusted Certificate Authority

IN THIS CHAPTER

- [About the Trusted Certificate Authority Page | 302](#)
- [Generate Default Trusted Certificate Authorities | 303](#)
- [Enroll a CA Certificate | 304](#)
- [Import a CA Certificate | 305](#)
- [Add a Certificate Authority Profile | 306](#)
- [Edit a Certificate Authority Profile | 310](#)
- [Delete Certificate Authority Profile | 310](#)
- [Search Text in the Trusted Certificate Authority Table | 311](#)

About the Trusted Certificate Authority Page

You are here: **Device Administration** > **Certificate Management** > **Trusted Certificate Authority**.

SSL forward proxy ensures secure transmission of data between a client and a server. Before establishing a secure connection, SSL forward proxy checks certificate authority (CA) certificates to verify signatures on server certificates. For this reason, a reasonable list of trusted CA certificates is required to effectively authenticate servers.

You can perform the following tasks:

- Generate a default trusted CAs. See [“Generate Default Trusted Certificate Authorities” on page 303](#).
- Enroll a CA certificate using the Simple Certificate Enrollment Process (SCEP) or Certificate Management Protocol (CMPv2). With SCEP or CMPv2, you can configure Juniper Network device to obtain a local certificate online and start the online enrollment for the specified certificate ID. See [“Enroll a CA Certificate” on page 304](#).
- Import a CA certificate to manually load CA certificates and CRL. See [“Import a CA Certificate” on page 305](#).
- Add a CA profile. See [“Add a Certificate Authority Profile” on page 306](#).
- Edit a CA profile. See [“Edit a Certificate Authority Profile” on page 310](#).

- Delete a CA profile. See [“Delete Certificate Authority Profile” on page 310.](#)
- Search for text in a Trusted Certificate Authority table. See [“Search Text in the Trusted Certificate Authority Table” on page 311.](#)
- Filter the trusted CA information based on select criteria. To do this, select the filter icon at the top right-hand corner of the table. The columns in the grid change to accept filter options. Type the filter options; the table displays only the data that fits the filtering criteria.
- Show or hide columns in the trusted CA table. To do this, use the Show Hide Columns icon in the top right corner of the page and select the options you want to show or deselect to hide options on the page.

[Table 127 on page 303](#) provides the details of the fields of the Trusted Certificate Authority Page.

Table 127: Fields on Trusted Certificate Authority Page

| Field | Description |
|-----------------|---|
| CA Profile | Displays the name of the CA profile. |
| Certificate ID | Displays the CA certificate ID. |
| Issuer Org | Displays the issuer organizational name. |
| Status | <p>Displays the status of the CA certificate.</p> <p>For example:</p> <ul style="list-style-type: none"> • Valid. • Expires in number of day(s). • Expired. • Download Required. This status is for a CA profile with manual enrollment. • Enrollment Required. This status is for a CA profile with automatic enrollment. |
| Expiration Date | Displays CA certificate expiration date. |
| Encryption Type | Displays whether the algorithm of the certificate is RSA, DSA, or ECDSA encryption. |

Generate Default Trusted Certificate Authorities

You are here: **Device Administration > Certificate Management > Trusted Certificate Authority.**

For SSL forward proxy, you need to load trusted CA certificates on your system. By default, Junos OS provides a list of trusted CA certificates that include default certificates used by common browsers. To generate default Trusted CA profiles with default name as Local, click **Generate Default Trusted CAs** and then click **Continue**. This process may take several minutes.

RELATED DOCUMENTATION

| |
|--|
| About the Trusted Certificate Authority Page 302 |
| Enroll a CA Certificate 304 |
| Import a CA Certificate 305 |
| Add a Certificate Authority Profile 306 |
| Edit a Certificate Authority Profile 310 |
| Delete Certificate Authority Profile 310 |
| Search Text in the Trusted Certificate Authority Table 311 |

Enroll a CA Certificate

You are here: **Device Administration > Certificate Management > Trusted Certificate Authority.**

To enroll a trusted CA certificate:

1. Click **Enroll**.
The Enroll CA Certificate page appears.
2. Complete the configuration according to the guidelines provided in [Table 128 on page 304](#).
3. Click **OK** to enroll the CA certificate.

Table 128: Fields on the Enroll CA Certificate Page

| Field | Action |
|-----------------|--|
| CA Profile Name | Select a CA profile name from the list that you want to enroll. |
| Protocol | Select a protocol from the list for the CA certificate that you want to enroll. <ul style="list-style-type: none">• SCEP—Simple Certificate Enrollment Protocol (SCEP)• CMPV2—Certificate Management Protocol version 2 (CMPv2) |

Table 128: Fields on the Enroll CA Certificate Page (*continued*)

| Field | Action |
|---|--|
| NOTE: The following fields are available only if you select CMPv2 protocol. All the fields are mandatory. | |
| CA Secret | Enter the out-of-band secret value received from the CA server. |
| CA Reference | Enter the out-of-band reference value received from the CA server. |
| CA Dn | Enter the distinguished name (DN) of the CA enrolling the EE certificate. NOTE: This optional parameter is mandatory if the CA certificate is not already enrolled. If the CA certificate is already enrolled, the subject DN is extracted from the CA certificate. |
| Certificate Details | Click Add to generate a new certificate inline. |

RELATED DOCUMENTATION

[About the Trusted Certificate Authority Page | 302](#)
[Generate Default Trusted Certificate Authorities | 303](#)
[Enroll a CA Certificate | 304](#)
[Add a Certificate Authority Profile | 306](#)
[Edit a Certificate Authority Profile | 310](#)
[Delete Certificate Authority Profile | 310](#)
[Search Text in the Trusted Certificate Authority Table | 311](#)

Import a CA Certificate

You are here: **Device Administration** > **Certificate Management** > **Trusted Certificate Authority**.

To import a CA certificate:

1. Click **Import**.

The Import CA Certificate page appears.

2. Complete the configuration according to the guidelines provided in [Table 129 on page 306](#).

3. Click **OK** to import the CA certificate.

You are taken to the Trusted Certificate Authority page. If the CA certificate content that you imported is validated successfully, a confirmation message is displayed; if not, an error message is displayed.

Table 129: Fields on the Import CA Certificate Page

| Field | Action |
|------------------------------|--|
| CA Profile Name | Select a CA profile name from the list that you want to import. |
| File path for CA Certificate | Click Browse to navigate to the path from where you want to import the CA certificate. |
| File path for CRL | Click Browse to navigate to the path from where you want to import the Certificate Revocation List (CRL). |

RELATED DOCUMENTATION

Add a Certificate Authority Profile

You are here: **Device Administration > Certificate Management > Trusted Certificate Authority.**

To add a Certificate Authority (CA) profile:

1. Click the add icon (+).
The Add CA Profile page appears.
2. Complete the configuration according to the guidelines provided in [Table 130 on page 306](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.
If you click **OK**, a new CA profile with the provided configuration is created.

Table 130: Fields on the Add CA Profile Page

| Field | Action |
|------------------------|---------------------------------|
| Profile Details | |
| CA Profile Name | Enter a unique CA profile name. |

Table 130: Fields on the Add CA Profile Page (*continued*)

| Field | Action |
|------------------------------------|--|
| CA Identity | Enter a CA identity name. |
| 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> |
| Nonce Payload | <p>Disable the option—Explicitly disable the sending of a nonce payload.</p> <p>Enable the option—Enable the sending of a nonce payload. This is the default.</p> <p>NOTE: This option is applicable only for OCSP.</p> |
| CRL Refresh Interval | <p>Enter the time interval (in hours) between CRL updates.</p> <p>Range: 0 through 8784 hours.</p> <p>NOTE: This option is applicable only for CRL.</p> |
| Password | Enter the password for authentication with the server. |

Table 130: Fields on the Add CA Profile Page (continued)

| Field | Action |
|-----------------------------|--|
| Disable on Download Failure | <p>Enable this option to override the default behavior and permit certificate verification even if the CRL fails to download.</p> <p>NOTE: This option is applicable only for CRL.</p> |
| Enrollment | |
| CA Certificate | Select an option whether you want to enroll the CA certificate manually or automatically. |
| File path for Certificate | Click Browse to navigate to the path from where you want to enroll the CA certificate. |
| URL | Enter the URL from where you want to enroll the CA certificate automatically. |
| Retry | Number of enrollment retry attempts before terminating. Range: 0 - 1080. |
| Retry-interval | Interval in seconds between the enrollment retries. Range: 0 - 3600. |
| Advanced | |
| Administrator | Enter an administrator e-mail address to which the certificate request is sent. |
| Source Address | Enter a source IPv4 or IPv6 address to be used instead of the IP address of the egress interface for communications with external servers. |
| Auto Re Enrollment | Enable this option to request that the issuing CA replace a certificate before its specified expiration date. |
| Re Generate Key Pair | Enable this option to automatically generate a new key pair when auto-reenrolling a device certificate. |
| Protocol | Select an option from the list: Simple Certificate Enrollment Protocol (SCEP) or Certificate Management Protocol version 2 (CMPv2). |
| Challenge Password | Enter the challenge password used by the certificate authority (CA) for certificate enrollment and revocation. This challenge password must be the same used when the certificate was originally configured. |
| Trigger Time | <p>Enter the percentage for the reenroll trigger time before expiration.</p> <p>Range: 1 through 99 percent</p> |

Table 130: Fields on the Add CA Profile Page (*continued*)

| Field | Action |
|------------------|--|
| Digest | <p>Select an option from the list: None, SHA-1 digest (default), or MD5-digest.</p> <p>NOTE: This option is applicable only when you select SCEP protocol.</p> |
| Encryption | <p>Select an option from the list: None, DES, DES 3.</p> <p>NOTE: This option is applicable only when you select SCEP protocol.</p> |
| Routing Instance | Select an option from the list of configured routing instances. |
| Proxy Profile | <p>Select an option from the list. Or</p> <p>To create a new proxy profile inline:</p> <ol style="list-style-type: none"> Click Create. <p>Create Proxy Profile page appears.</p> <ol style="list-style-type: none"> Enter the following details: <ul style="list-style-type: none"> Profile Name—Enter a unique proxy profile name. Connection Type: <ul style="list-style-type: none"> Server IP—Enter the IP address of the server. Host Name—Enter the host name. Port Number—Select the port number by using top/down arrows. <p>Range: 0 through 65535</p> Click OK. |

RELATED DOCUMENTATION

[About the Trusted Certificate Authority Page | 302](#)
[Generate Default Trusted Certificate Authorities | 303](#)
[Enroll a CA Certificate | 304](#)
[Import a CA Certificate | 305](#)
[Edit a Certificate Authority Profile | 310](#)
[Delete Certificate Authority Profile | 310](#)
[Search Text in the Trusted Certificate Authority Table | 311](#)

Edit a Certificate Authority Profile

You are here: **Device Administration** > **Certificate Management** > **Trusted Certificate Authority**.

To edit a Certificate Authority (CA) profile:

1. Select a CA profile.
2. On the upper right side of the Trusted Certificate Authority page, click the pencil icon.

See [“Add a Certificate Authority Profile” on page 306](#) for the options available for editing on the Edit CA Profile page.

NOTE: When you select a CA profile to edit, you cannot edit the following fields:

- CA Profile Name
- Revocation Check
- Enrollment > CA Certificate
- Advanced > Auto Re Enrollment
- Advanced > Protocol

3. Click **OK**

RELATED DOCUMENTATION

| |
|--|
| About the Trusted Certificate Authority Page 302 |
| Generate Default Trusted Certificate Authorities 303 |
| Enroll a CA Certificate 304 |
| Import a CA Certificate 305 |
| Delete Certificate Authority Profile 310 |
| Search Text in the Trusted Certificate Authority Table 311 |

Delete Certificate Authority Profile

You are here: **Device Administration** > **Certificate Management** > **Trusted Certificate Authority**.

To delete a Certificate Authority (CA) profile:

1. Select a CA profile.
2. On the upper right side of the Trusted Certificate Authority page, click the delete icon to delete.
A confirmation window appears.
3. Click **Yes** to delete.

RELATED DOCUMENTATION

| |
|--|
| About the Trusted Certificate Authority Page 302 |
| Generate Default Trusted Certificate Authorities 303 |
| Enroll a CA Certificate 304 |
| Import a CA Certificate 305 |
| Add a Certificate Authority Profile 306 |
| Edit a Certificate Authority Profile 310 |
| Search Text in the Trusted Certificate Authority Table 311 |

Search Text in the Trusted Certificate Authority Table

You are here: **Device Administration** > **Certificate Management** > **Trusted Certificate Authority**.

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

To search for text:

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

RELATED DOCUMENTATION

| |
|--|
| About the Trusted Certificate Authority Page 302 |
|--|

[Generate Default Trusted Certificate Authorities | 303](#)

[Enroll a CA Certificate | 304](#)

[Import a CA Certificate | 305](#)

[Add a Certificate Authority Profile | 306](#)

[Edit a Certificate Authority Profile | 310](#)

[Delete Certificate Authority Profile | 310](#)

Certificate Management—Certificate Authority Group

IN THIS CHAPTER

- [About the Certificate Authority Group Page | 313](#)
- [Import a Trusted CA Group | 314](#)
- [Add a CA Group | 315](#)
- [Edit a CA Group | 316](#)
- [Delete CA Group | 317](#)
- [Search Text in the Certificate Authority Group Table | 317](#)

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 314](#).
- Add a CA group. See [“Add a CA Group” on page 315](#).

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 316](#).
- Delete a CA group. See [“Delete CA Group” on page 317](#).

- Search for text in a CA group table. See [“Search Text in the Certificate Authority Group Table” on page 317](#).
- Filter the CA group information based on select criteria. To do this, select the filter icon at the top right-hand corner of the table. The columns in the grid change to accept filter options. Type the filter options; the table displays only the data that fits the filtering criteria.
- Show or hide columns in the CA group table. To do this, use the Show Hide Columns icon in the top right corner of the page and select the options you want to show or deselect to hide options on the page.

[Table 131 on page 314](#) provides the details of the fields of the Certificate Authority Group Page.

Table 131: 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 132 on page 314](#).

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 132: Fields on the Import Trusted CA Group Page

| Field | Action |
|---------------|-------------------------------|
| CA Group Name | Enter the name of a CA group. |

Table 132: Fields on the Import Trusted CA Group Page (continued)

| Field | Action |
|------------------------|--|
| 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 | 313](#)
- [Add a CA Group | 315](#)
- [Edit a CA Group | 316](#)
- [Delete CA Group | 317](#)
- [Search Text in the Certificate Authority Group Table | 317](#)

Add a CA Group

You are here: **Device Administration** > **Certificate Management** > **Trusted Certificate Authority**.

To add a CA group:

1. Click the add icon (+).
The Add CA Group page appears.
2. Complete the configuration according to the guidelines provided in [Table 133 on page 315](#).
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 133: Fields on the Add CA Group Page

| Field | Action |
|---------------|-------------------------------|
| CA Group Name | Enter a unique CA group name. |

Table 133: Fields on the Add CA Group Page (*continued*)

| Field | Action |
|-------------|---|
| CA Profiles | <p>Select a CA profile name from the list in the Available column and then click the right arrow to move it to the Selected column.</p> <p>NOTE: You can add up to maximum of 20 CA profiles per trusted CA group.</p> |

RELATED DOCUMENTATION

[About the Certificate Authority Group Page | 313](#)
[Import a Trusted CA Group | 314](#)
[Edit a CA Group | 316](#)
[Delete CA Group | 317](#)
[Search Text in the Certificate Authority Group Table | 317](#)

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. On the upper right side of the Certificate Authority Group page, click the pencil icon.
See [“Add a CA Group” on page 315](#) for the options available for editing on the Edit CA Group page.
3. Click **OK**

RELATED DOCUMENTATION

[About the Certificate Authority Group Page | 313](#)
[Import a Trusted CA Group | 314](#)
[Delete CA Group | 317](#)
[Search Text in the Certificate Authority Group Table | 317](#)

Delete CA Group

You are here: **Device Administration** > **Certificate Management** > **Trusted Certificate Authority**.

To delete a CA group:

1. Select a CA group.
2. On the upper right side of the Certificate Authority Group page, click the delete icon to delete.
A confirmation window appears.
3. Click **Yes** to delete.

RELATED DOCUMENTATION

| |
|--|
| About the Certificate Authority Group Page 313 |
| Import a Trusted CA Group 314 |
| Add a CA Group 315 |
| Edit a CA Group 316 |
| Search Text in the Certificate Authority Group Table 317 |

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 top right corner of a page to search for text containing letters and special characters on that page.

To search for text:

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

RELATED DOCUMENTATION

[About the Certificate Authority Group Page | 313](#)

[Import a Trusted CA Group | 314](#)

[Add a CA Group | 315](#)

[Edit a CA Group | 316](#)

[Delete CA Group | 317](#)

Multi Tenancy—Resource Profiles

IN THIS CHAPTER

- [About the Resource Profiles Page | 319](#)
- [Global Settings | 321](#)
- [Add a Resource Profile | 322](#)
- [Edit a Resource Profile | 325](#)
- [Delete Resource Profile | 325](#)

About the Resource Profiles Page

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

NOTE: This menu is supported for only SRX4000 line of devices, SRX5000 line of devices and SRX1500 devices.

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 321](#).
- Create a resource profile. See [“Add a Resource Profile” on page 322](#).
- Edit a resource profile. See [“Edit a Resource Profile” on page 325](#).
- Delete a resource profile. See [“Delete Resource Profile” on page 325](#).
- 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 top right-hand 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 top 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 134 on page 320 describes the fields on the Resource Profiles page.

Table 134: Fields on the Resource Profiles Page

| Field | Description |
|--------------|---|
| Profile Name | Displays the resource (security) profile names. |

Table 134: Fields on the Resource Profiles Page *(continued)*

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

RELATED DOCUMENTATION

| |
|---|
| Global Settings 321 |
| Add a Resource Profile 322 |
| Edit a Resource Profile 325 |
| Delete Resource Profile 325 |

Global Settings

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

To add global settings:

1. Click the **Global Settings** on the upper right side of the Resource Profiles page.
The Global Settings page appears.
2. Complete the configuration according to the guidelines provided in [Table 135 on page 321](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 135: 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 u set 50 %, 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 319 |
| Add a Resource Profile 322 |
| Edit a Resource Profile 325 |
| Delete Resource Profile 325 |

Add a Resource Profile

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

To add a resource profile:

1. Click the add icon (+) on the upper right side of the Resource Profile page.
The Add Resource Profile page appears.
2. Complete the configuration according to the guidelines provided in [Table 136 on page 322](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 136: Fields on the Add Resource Profile Page

| Field | Description |
|----------------------------|--|
| General | |
| 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-software-initiator | Specify the number of IPv6 dual-stack lite (DS-Lite) software initiators that can connect to the software concentrator configured in either a user logical system or the primary logical system. |

Table 136: Fields on the Add Resource Profile Page (*continued*)

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

Table 136: Fields on the Add Resource Profile Page (*continued*)

| Field | Description |
|----------------------------|--|
| 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. |
| 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 | 319](#)

[Global Settings | 321](#)

[Edit a Resource Profile | 325](#)

[Delete Resource Profile | 325](#)

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 side 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 322](#).

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

RELATED DOCUMENTATION

[About the Resource Profiles Page | 319](#)

[Global Settings | 321](#)

[Add a Resource Profile | 322](#)

[Delete Resource Profile | 325](#)

Delete Resource Profile

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

To delete Resource Profiles:

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 side of the page.

3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

| | |
|----------------------------------|-----|
| About the Resource Profiles Page | 319 |
| Global Settings | 321 |
| Add a Resource Profile | 322 |
| Edit a Resource Profile | 325 |

Multi Tenancy—Interconnecting Ports

IN THIS CHAPTER

- [About the Interconnecting Ports Page | 327](#)
- [Add a LT Logical Interface | 329](#)
- [Edit a LT Logical Interface | 335](#)
- [Delete Logical Interface | 335](#)
- [Search for Text in an Interconnect Ports Table | 336](#)

About the Interconnecting Ports Page

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

On SRX Series Services Gateways, the logical tunnel interface is used to interconnect logical systems. Use this page to interconnect logical system that serves as an internal virtual private LAN service (VPLS) switch connecting one logical system on the device to another.

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 329](#).
- Edit a LT Logical Interface. See [“Edit a LT Logical Interface” on page 335](#).
- Delete an Interconnect Interface. See [“Delete Logical Interface” on page 335](#).
- Search for Text in an Interconnect Ports table. See [“Search for Text in an Interconnect Ports Table” on page 336](#).

Field Descriptions

[Table 137 on page 328](#) describes the fields on the Interconnect ports page.

Table 137: 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. |
| 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](#) | 329

Add a LT Logical Interface

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

To add a LT logical interface:

1. Click the add icon (+) available on the upper right side of the Interconnect Ports page.
The Create LT Logical Interface page appears.
2. Complete the configuration according to the guidelines provided in [Table 138 on page 329](#).
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 138 on page 329](#) provides guidelines on using the fields on the Create LT Logical Interface page.

Table 138: Fields on the Create LT Logical Interface Page

| Field | Description |
|----------------------|--|
| Local Details | |
| 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 138: 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 138: 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 |
| 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> |

Table 138: Fields on the Create LT Logical Interface Page *(continued)*

| Field | Description |
|-------------|--|
| 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 138: 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 138: 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](#) | 335

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 side 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 329](#).

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

RELATED DOCUMENTATION

| [Delete Logical Interface](#) | 335

Delete Logical Interface

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

To delete a logical interface:

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 side 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](#) | 336

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 top 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 Interconnecting Ports Page | 327](#)

Multi Tenancy—Logical Systems

IN THIS CHAPTER

- [About the Logical Systems Page | 337](#)
- [Add a Logical System | 339](#)
- [Edit a Logical System | 349](#)
- [Delete Logical System | 349](#)
- [Search Text in Logical Systems Table | 350](#)

About the Logical Systems Page

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

NOTE: This menu is supported for only SRX4000 line of devices, SRX5000 line of devices and SRX1500 devices.

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 339](#).
- Edit a logical system. See [“Edit a Logical System” on page 349](#).
- Delete a logical system. See [“Delete Logical System” on page 349](#).
- Search for Text in a logical system table. See [“Search Text in Logical Systems Table” on page 350](#).
- 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 top right-hand 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 top 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 140 on page 339](#).

Field Descriptions

[Table 139 on page 338](#) describes the fields on the Logical Systems page.

Table 139: 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. |
| Zone | Displays the zone of the resource profile. |

[Table 140 on page 339](#) describes the options on the LSYS page.

Table 140: 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 | 339](#)
[Edit a Logical System | 349](#)
[Delete Logical System | 349](#)
[Search Text in Logical Systems Table | 350](#)

Add a Logical System

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

To add a logical system:

1. Click the add icon (+) on the upper right side of the Logical Systems page.
The Create Logical Systems page appears.
2. Complete the configuration according to the guidelines provided in [Table 141 on page 340](#).
3. Click **Finish** to save the changes. If you want to discard your changes, click **Cancel**.

Table 141: 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 141: Fields on the Add Logical Systems Page *(continued)*

| Field | Description |
|---------------|-------------|
| Resource Name | |

Table 141: Fields on the Add Logical Systems Page (*continued*)

| Field | Description |
|-------|--|
| | <p>Displays the resource name.</p> <ul style="list-style-type: none"> • nat-pat-portnum—Specify the maximum quantity and the reserved quantity of ports for the logical system as part of its security profile. • dslite-software-initiator—Specify the number of IPv6 dual-stack lite (DS-Lite) software initiators that can connect to the software concentrator configured in either a user logical system or the 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. • 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 |

Table 141: Fields on the Add Logical Systems Page (*continued*)

| Field | Description |
|----------|--|
| | <p>the logical systems.</p> <ul style="list-style-type: none"> • 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. • 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. |

Table 141: Fields on the Add Logical Systems Page (*continued*)

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

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 |
| Description | Enter the description. |

Table 141: Fields on the Add Logical Systems Page (*continued*)

| Field | 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 | |
| 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 141: Fields on the Add Logical Systems Page *(continued)*

| Field | Description |
|-----------------|-------------|
| System Services | |

Table 141: Fields on the Add Logical Systems Page (*continued*)

| Field | Description |
|-------|--|
| | <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. • 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. |

Table 141: Fields on the Add Logical Systems Page (*continued*)

| Field | Description |
|-------------------------|--|
| | <ul style="list-style-type: none"> • xnm-clear-text—Specify the JUNOScript API for unencrypted traffic over TCP. • xnm-ssl—Specify the JUNOScript API Service over SSL. |
| 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 | 337](#)
[Add a Logical System | 339](#)
[Edit a Logical System | 349](#)
[Delete Logical System | 349](#)
[Search Text in Logical Systems Table | 350](#)

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 side 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 339](#).

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

RELATED DOCUMENTATION

- [About the Logical Systems Page | 337](#)
- [Add a Logical System | 339](#)
- [Delete Logical System | 349](#)
- [Search Text in Logical Systems Table | 350](#)

Delete Logical System

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

To delete 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 side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

- [About the Logical Systems Page | 337](#)
- [Add a Logical System | 339](#)

| |
|--|
| Edit a Logical System 349 |
| Search Text in Logical Systems Table 350 |

Search Text in Logical Systems Table

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

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

To search for text:

1. 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 337 |
| Add a Logical System 339 |
| Edit a Logical System 349 |
| Delete Logical System 349 |

Multi Tenancy—Tenants

IN THIS CHAPTER

- [About the Tenants Page | 351](#)
- [Add a Tenant | 353](#)
- [Edit a Tenant | 360](#)
- [Delete Tenant | 360](#)
- [Search Text in Tenants Table | 361](#)

About the Tenants Page

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 line of devices, SRX5000 line of devices and SRX1500 devices.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a tenant. See [“Add a Tenant” on page 353](#).
- Edit a tenant. See [“Edit a Tenant” on page 360](#).
- Delete a tenant. See [“Delete Tenant” on page 360](#).
- Search for Text in a tenants table. See [“Search Text in Tenants Table” on page 361](#).
- 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 top right-hand 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 top 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 142 on page 352](#) describes the fields on the Tenants page.

Table 142: 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 | 353](#)

[Edit a Tenant | 360](#)

[Delete Tenant | 360](#)

[Search Text in Tenants Table | 361](#)

Add a Tenant

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

To add a tenant:

1. Click the add icon (+) on the upper right side of the Tenants page.
The Create Tenant page appears.
2. Complete the configuration according to the guidelines provided in [Table 143 on page 353](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 143: 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. |
| 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 322](#) for details on creating and editing resource profile.

Table 143: Fields on the Create Tenant Page (*continued*)

| Field | Description |
|--|---|
| User Details | |
| You can define tenant administrators and users. | |
| Click one: | |
| <ul style="list-style-type: none"> • 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. |
| Role | Select an option from the list to specify the role of the user: <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: | |
| <ul style="list-style-type: none"> • Enable/Disable —Enable or disable the physical interface. • Add icon (+)—Add logical interfaces. • Edit icon (/)—Edit the selected users. • Delete icon—Delete the selected users. | |
| Create-Edit logical interfaces | |
| General | |
| Physical Interface Name | Displays the name of the Physical Interface. |

Table 143: Fields on the Create Tenant Page (*continued*)

| Field | Description |
|---|--|
| Logical Interface Unit | Enter the logical interface unit. |
| 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. |
| 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. |
| Application Tracking | Enables the application tracking support. |
| Source Identity Log | Enable source identity log for this zone. |

Table 143: Fields on the Create Tenant Page (*continued*)

| Field | Description |
|---------------------|---|
| Interfaces | Select an interface from the Available column and move it to Selected column. |
| Selected interfaces | Displays the selected interfaces. |

Table 143: Fields on the Create Tenant Page *(continued)*

| Field | Description |
|-------------------------|-------------|
| System Services Options | |

Table 143: Fields on the Create Tenant Page (*continued*)

| Field | Description |
|-------|--|
| | <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. • 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. |

Table 143: Fields on the Create Tenant Page (*continued*)

| Field | Description |
|-------------------------|---|
| | <ul style="list-style-type: none"> • webapi-ssl—Specify the Webapi service using HTTP secured by SSL. • xnm-clear-text—Specify the JUNOScript API for unencrypted traffic over TCP. • xnm-ssl—Specify the JUNOScript API Service over SSL. |
| Protocols | <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 | 351](#)
[Edit a Tenant | 360](#)
[Delete Tenant | 360](#)
[Search Text in Tenants Table | 361](#)

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 side of the page.

The Edit a Tenant page appears with editable fields. For more information on the options, see [“Add a Tenant” on page 353](#).

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

RELATED DOCUMENTATION

- [About the Tenants Page | 351](#)
- [Add a Tenant | 353](#)
- [Delete Tenant | 360](#)
- [Search Text in Tenants Table | 361](#)

Delete Tenant

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

To delete tenants:

1. Select the tenants that you want to delete on the Tenants page.
2. Click the delete icon available on the upper right side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

- [About the Tenants Page | 351](#)
- [Add a Tenant | 353](#)

[Edit a Tenant | 360](#)

[Search Text in Tenants Table | 361](#)

Search Text in Tenants Table

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

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

To search for text:

1. 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 | 351](#)

[Add a Tenant | 353](#)

[Edit a Tenant | 360](#)

[Delete Tenant | 360](#)

License Management

IN THIS CHAPTER

- [Manage Your Licenses | 362](#)

Manage Your Licenses

IN THIS SECTION

- [About License Management Page | 362](#)
- [Add License | 363](#)
- [Delete Installed Licenses | 364](#)
- [Update Installed Licenses | 364](#)
- [Update Trial Licenses | 364](#)
- [Display License Keys | 364](#)
- [Download License Keys | 364](#)
- [Software Feature Licenses | 365](#)

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 144 on page 362](#) describes the fields on the License Management page.

Table 144: Fields on the License Maintenance Page

| Field | Function |
|---------|--|
| Feature | Displays the name of the licensed feature. |

Table 144: Fields on the License Maintenance Page (*continued*)

| Field | Function |
|--------------------|--|
| 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 UTM) 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**.
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.

[Table 145 on page 365](#) describes the Junos OS features that require licenses.

Table 145: Junos OS Services Feature Licenses

| Junos OS License Requirements | Device | | | | | | | | |
|---|----------|--------|--------|--------|--------|--------|-------------|-------------|-------------|
| Feature | J Series | SRX100 | SRX210 | SRX220 | SRX240 | SRX650 | SRX100 Line | SRX300 Line | SRX500 Line |
| Access Manager | | | X | | X | | | | |
| BGP Route Reflectors | X | | X | | X | X | | | |
| Dynamic VPN | | X | X | X | X | X | | | |
| IDP Signature Update | X | X * | X * | X * | X * | X | X | X | X |
| Application Signature Update (Application Identification) | | | | | | | X | X | X |
| Juniper-Kaspersky Anti-Virus | X | X | X | X | X | X | | | |
| Juniper-Sophos Anti-Spam | X | X | X | X | X | X | | | |
| Juniper-WebSense Integrated Web Filtering | X | X | X | X | X | X | | | |
| SRX100 Memory Upgrade | | X | | | | | | | |
| UTM | X | | X * | | X * | X | | | |

RELATED DOCUMENTATION

Manage Device Certificates

Manage Trusted Certificate Authority

[Manage Rescue Configuration](#) | **385**

ATP Management

IN THIS CHAPTER

- [Enroll Your Device with Juniper ATP Cloud | 367](#)
- [About the Diagnostics Page | 370](#)

Enroll Your Device with Juniper ATP Cloud

You are here: **Device Administration** > **ATP Management** > **Enrollment**.

Use this page to enroll your SRX device with Juniper Advanced Threat Prevention (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 devices to simplify its deployment and enhance the anti-threat capabilities of the SRX device.

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 Sky Advanced Threat Prevention 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 Juniper ATP Cloud 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 Juniper ATP Cloud.

To enroll your device to Juniper ATP Cloud using J-Web:

- Optional. Configure proxy profile.
- Enroll SRX device with Juniper ATP Cloud.

To enroll your device to Juniper ATP Cloud using J-Web:

1. Use either of the following methods to configure the proxy profile:
 - 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 device and Juniper ATP Cloud communicates through the proxy server if a proxy profile is configured. Otherwise, they directly communicate with each other.

- b. Click **Create Proxy** to create a proxy profile.

The Create Proxy Profile page appears.

1. Complete the configuration by using the guidelines in [Table 146 on page 368](#).
 2. Click **OK**.

A new proxy profile is created.

3. Click **Apply Proxy**.

Applying proxy enables the SRX device and Juniper ATP Cloud to communicate through the proxy server.

Table 146: 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 your device to Juniper ATP Cloud:

- a. Click **Enroll**.

The ATP 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 147 on page 369](#).
- c. Click **OK**.

The SRX Series device enrollment progress, successful message, or any errors will be shown at the end of the ATP Enrollment page.

NOTE:

- A new realm is created if you have enabled **Create New Realm** and then the SRX device is enrolled to Juniper ATP Cloud. If there is any existing enrollment for the same SRX device, 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.

Table 147: Fields on the ATP Enrollment Page

| Field | Description |
|------------------|---|
| Create New Realm | By default, this option is disabled if you have a Juniper ATP Cloud account with an associated license. Enable this option to add a new realm if you do not have a Juniper ATP Cloud account with an associated license. |
| 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. Include both uppercase and lowercase letters, at least one number, and at least one special character; 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). |

Table 147: Fields on the ATP Enrollment Page (*continued*)

| Field | Description |
|-------|---|
| Realm | Enter a name for the security realm. This should be a name that is meaningful to your organization. A realm name can contain only 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 148 on page 370](#) describes the fields on the Diagnostics page.

Table 148: 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. |

Table 148: Fields on the Diagnostics Page (*continued*)

| Field | Description |
|-----------------------------|--|
| Connection Status | Specify the connection status. |
| Service Plane | |
| Card Info | Specify the card number. |
| Connection Active Number | Specify the connection active numbers. |
| Connection Relay statistics | Specify the connection relay statistics. |
| Other Details | |
| Configured Proxy Server | Specify the configured proxy server. |
| Port Number | Specify the port number of the proxy server. |

RELATED DOCUMENTATION

| [Monitor Advanced Threat Prevention—Statistics](#) | 198

Operations

IN THIS CHAPTER

- [Maintain Files | 372](#)
- [Maintain Reboot Schedule | 375](#)
- [Maintain System Snapshots | 377](#)

Maintain Files

IN THIS SECTION

- [About Files Page | 372](#)
- [Clean Up Files | 372](#)
- [Download and Delete Files | 373](#)
- [Delete Backup JUNOS Package | 374](#)

About Files Page

You are here: **Device Administration** > **Operations** > **Files**.

You can clean up files, download, or delete files and delete the Junos package backup.

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 149 on page 373 provides the maintenance options to download and delete files.

Table 149: Download and Delete Files Maintenance Options

| File Type | Function |
|-----------------|--|
| Log Files | <div>Lists the log files located in the /var/log directory on the device.</div> <div>Select an option:</div> <div><ul style="list-style-type: none">• Delete—Deletes files.• Download—Downloads files.</div> |
| Temporary Files | <div>Lists the temporary files located in the /var/tmp directory on the device.</div> <div>Select an option:</div> <div><ul style="list-style-type: none">• Delete—Deletes files.• Download—Downloads files.</div> |

Table 149: 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 (*.tgz files)</code> 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. |

Delete Backup JUNOS Package

[Table 150 on page 375](#) provides the maintenance options to delete the JUNOS Package backup.

Table 150: Delete Backup JUNOS Package Files Maintenance Options

| Field | Function |
|-----------------------------|---|
| Delete backup Junos package | <p>Reviews the backup image information listed.</p> <p>Click Delete backup JUNOS package and then select an option.</p> <p>NOTE: The Delete backup option is hidden if the router is in dual-root partitioning scheme</p> <p>The available options are:</p> <ul style="list-style-type: none"> • OK—Deletes the backup image and returns to the Files page. • Cancel—Cancels the deletion of the backup image and returns to the Files page. |

SEE ALSO

[Maintain Reboot Schedule | 375](#)

[Maintain System Snapshots | 377](#)

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 151 on page 375](#).

Table 151: Reboot Schedule Maintenance Options

| Field | Action |
|---------------------------|--|
| Reboot Immediately | Select this option to reboot the device immediately. |

Table 151: Reboot Schedule Maintenance Options (*continued*)

| Field | Action |
|--|---|
| 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. |
| Reboot From Media NOTE: This option is not available in SRX4600 device. | Choose the boot device from the Reboot From Media list: <ul style="list-style-type: none"> ● internal—Reboots from the internal media (default). ● usb—Reboots from the USB storage device. |
| Message | Type a message to be displayed to the user on the device before the reboot occurs. |

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](#) | 377

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 152 on page 378](#).

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 152: 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> |
| Factory | <p>Copies only the default files that were loaded on the internal media when it was shipped from the factory, plus the rescue configuration if one has been set.</p> <p>Select the check box.</p> <p>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 379 |
| Install Software Packages 380 |
| Rollback Software Package Version 381 |

Software Management

IN THIS CHAPTER

- Upload Software Packages | 379
- Install Software Packages | 380
- Rollback Software Package Version | 381

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 153 on page 379](#).

Table 153: 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. |
| 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 380 |
| Rollback Software Package Version 381 |

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 154 on page 380](#).

Table 154: 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 format: <i>ftp://hostname/pathname/package-name</i> <i>http://hostname/pathname/package-name</i> |
| 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](#) | 381

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 375](#).

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](#) | 379

[Install Software Packages](#) | 380

Configuration Management

IN THIS CHAPTER

- [Manage Upload Configuration Files | 382](#)
- [Manage Configuration History | 383](#)
- [Manage Rescue Configuration | 385](#)

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

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 155 on page 383](#).

Table 155: 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. |
| Client | Indicates the method by which the configuration was committed. The available options are: <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. |

Table 155: History Maintenance Options (*continued*)

| Field | Function |
|-------------|---|
| Comment | Indicates comments. |
| Log Message | <p>Indicates the method used to edit the configuration.</p> <ul style="list-style-type: none"> • Imported via paste—Configuration was edited and loaded with the Device Administration > Tools > CLI Editor option. • Imported upload [filename]—Configuration was uploaded with the Device Administration > Configuration Management > Upload option. • Modified via quick-configuration—Configuration was modified with the specified version of the J-Web user interface. • Rolled back via user-interface—Configuration was rolled back to a previous version through the user interface specified by <i>user-interface</i>, which can be Web Interface or CLI. |
| 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. Select the options on your Web browser to save the configuration file to a target directory on your local system. The file is saved as an ASCII file. • Rollback—Rolls back the configuration to any of the previous versions stored on the device. The 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 | 385](#)

[Manage Upload Configuration Files | 382](#)

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:

1. 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 | 362](#)

Manage Device Certificates

Alarm Management

IN THIS CHAPTER

- [Monitor Chassis Alarm | 386](#)
- [Monitor System Alarm | 391](#)

Monitor Chassis Alarm

IN THIS SECTION

- [About Chassis Alarm Page | 386](#)
- [Create Chassis Alarm Definition | 386](#)
- [Edit Chassis Alarm Definition | 390](#)

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 156 on page 387](#) to create Chassis Alarm Definition.

Table 156: 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 |
| 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 |

Table 156: Chassis Alarm Definition Options (*continued*)

| Chassis Component | Alarm Configuration Option |
|--|--|
| Optical Transport Network Optical channel Data Unit (OTN ODU) | Backward defect indication (odu-bdi) Payload type mismatch (odu-ptim) Trail trace identifier mismatch (odu-ttim) Select an alarm condition from the list for OTN ODU: <ul style="list-style-type: none"> • Ignore • Red • Yellow • None |
| 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 an alarm condition from the list for OTN OTU: <ul style="list-style-type: none"> • Ignore • Red • Yellow • None |

Table 156: Chassis Alarm Definition Options (*continued*)

| Chassis Component | Alarm Configuration Option |
|-------------------|---|
| Serial | <p>Clear-to-send (CTS) signal absent (cts-absent)</p> <p>Data carrier detect (DCD) signal absent (dcd-absent)</p> <p>Data set ready (DSR) signal absent (dsr-absent)</p> <p>Loss of receive clock (loss-of-rx-clock)</p> <p>Loss of transmit clock (loss-of-tx-clock)</p> <p>Select an alarm condition from the list for Serial:</p> <ul style="list-style-type: none"> • Ignore • Red • Yellow • None |
| 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 156: 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 on the upper right side of the Chassis Alarm Definition page.

See [Table 156 on page 387](#) for the options available for editing the Chassis Alarm Definition page.

2. Click **OK**.

RELATED DOCUMENTATION

Monitor System Alarm

IN THIS SECTION

- About System Alarm Page | 391
- Create System Alarm Configuration | 391
- Edit System Alarm Configuration | 394

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 157 on page 391](#) to create System Alarm Configuration.

Table 157: 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 157: 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. |
| 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 | |

Table 157: RPM Information Troubleshooting Options (*continued*)

| Field | Function |
|--------------------------------------|---|
| Samples | <p>Total number of probes used for the data set.</p> <p>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.</p> |
| Earliest Sample | System time when the first probe in the sample was received. |
| Latest Sample | System time when the last probe in the sample was received. |
| Mean Value | Average round-trip time for the 50-probe sample. |
| Standard Deviation | Standard deviation of the round-trip times for the 50-probe sample. |
| Lowest Value | Shortest round-trip time from the device to the remote server, as measured over the 50-probe sample. |
| Time of Lowest Sample | System time when the lowest value in the 50-probe sample was received. |
| Highest Value | Longest round-trip time from the J Series device to the remote server, as measured over the 50-probe sample. |
| Time of Highest Sample | System time when the highest value in the 50-probe sample was received. |
| Cumulative Jitter for a Probe | |
| Samples | <p>Total number of probes used for the data set.</p> <p>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.</p> |
| Earliest Sample | System time when the first probe in the sample was received. |
| Latest Sample | System time when the last probe in the sample was received. |
| Mean Value | Average jitter for the 50-probe sample. |
| Standard Deviation | Standard deviation of the jitter values for the 50-probe sample. |

Table 157: RPM Information Troubleshooting Options *(continued)*

| Field | Function |
|------------------------|--|
| 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 on the upper right side of the System Alarm Configuration page.
See [Table 157 on page 391](#) for the options available for editing the System Alarm Configuration page.
2. Click **OK**.

SEE ALSO

| [Monitor Chassis Alarm | 386](#)

RPM

IN THIS CHAPTER

- [Setup RPM | 395](#)
- [View RPM | 402](#)

Setup RPM

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 158 on page 395](#) 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 158: RPM Setup Troubleshooting Options

| Field | Function |
|----------------|----------|
| Probe Owners | |
| Identification | |

Table 158: RPM Setup Troubleshooting Options (*continued*)

| Field | Function |
|--------------------------------|---|
| 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> |
| 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 icmp and icmp-timestamp. The default routing instance is inet.0.</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 | |

Table 158: RPM Setup Troubleshooting Options (*continued*)

| Field | Function |
|---------------------|---|
| 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"> • http-get • http-get-metadata • icmp-ping • icmp-ping-timestamp • tcp-ping • udp-ping |
| 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> |
| 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> |

Table 158: RPM Setup Troubleshooting Options (*continued*)

| Field | Function |
|---------------------------------|--|
| Data Size | Specifies the size of the data portion of the ICMP probes. Type a size (in bytes) between 0 and 65507. |
| Data Fill | Specifies the contents of the data portion of the ICMP probes. Type a hexadecimal value between 1 and 800h to use as the contents of the ICMP probe data. |
| Hardware Timestamp | |
| One Way Hardware Timestamp | Specifies the hardware timestamps for one-way measurements. To enable one-way timestamping, select the check box. |
| Hardware Timestamp | Specifies timestamping of RPM probe messages. You can timestamp the following RPM probes to improve the measurement of latency or jitter: <ul style="list-style-type: none"> • ICMP ping • ICMP ping timestamp • UDP ping—destination port UDP-ECHO (port 7) only • UDP ping timestamp—destination port UDP-ECHO (port 7) only To enable timestamping, select the check box. |
| Destination Interface | Specifies the name of an output interface for probes. Select the interface from the list. |
| Maximum Probe Thresholds | |
| Successive Lost Probes | Specifies the total number of probes that must be lost successively to trigger a probe failure and generate a system log message. Type a number between 0 and 15. |
| Lost Probes | Specifies the total number of probes that must be lost to trigger a probe failure and generate a system log message. Type a number between 0 and 15. |

Table 158: 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> |
| 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> |

Table 158: RPM Setup Troubleshooting Options (*continued*)

| Field | Function |
|------------------------------------|--|
| 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. |
| 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. |

Table 158: RPM Setup Troubleshooting Options (*continued*)

| Field | Function |
|-------------------------------------|---|
| 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. |
| 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. |

Table 158: RPM Setup Troubleshooting Options (*continued*)

| Field | Function |
|--|---|
| 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 | |
| Maximum Number of Concurrent Probes | <p>Specifies the maximum number of concurrent probes allowed.</p> <p>Type a number between 1 and 500.</p> |
| Probe Server | |
| TCP Probe Server | <p>Specifies the port on which the device is to receive and transmit TCP probes.</p> <p>Type number 7, or a port number from 49160 through 65535.</p> |
| UDP Probe Server | <p>Specifies the port on which the device is to receive and transmit UDP probes.</p> <p>Type number 7, or a port number from 49160 through 65535.</p> |

RELATED DOCUMENTATION

[View RPM](#) | [402](#)

View RPM

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 159 on page 403](#).

Table 159: 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. |
| Probe Type | Type of RPM probe configured for the specified test. Following are valid probe types: <ul style="list-style-type: none"> • http-get • http-get-metadata • icmp-ping • icmp-ping-timestamp • tcp-ping • udp-ping |
| Target Address | IP address or URL of the remote server that is being probed by the RPM test. |

Table 159: RPM Information Troubleshooting Options (*continued*)

| Field | Function |
|------------------------------------|---|
| 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. |
| 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 | <p>Total number of probes used for the data set.</p> <p>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.</p> |
| 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. |

Table 159: RPM Information Troubleshooting Options (*continued*)

| Field | Function |
|--------------------------------------|---|
| Lowest Value | Shortest round-trip time from the device to the remote server, as measured over the 50-probe sample. |
| Time of Lowest Sample | System time when the lowest value in the 50-probe sample was received. |
| Highest Value | Longest round-trip time from the J Series device to the remote server, as measured over the 50-probe sample. |
| Time of Highest Sample | System time when the highest value in the 50-probe sample was received. |
| Cumulative Jitter for a Probe | |
| Samples | <p>Total number of probes used for the data set.</p> <p>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.</p> |
| 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

Tools

IN THIS CHAPTER

- [Troubleshoot Ping Host | 407](#)
- [Troubleshoot Ping MPLS | 410](#)
- [Troubleshoot Traceroute | 415](#)
- [Troubleshoot Packet Capture | 418](#)
- [Access CLI | 424](#)
- [View CLI Configuration | 425](#)
- [Edit CLI Configuration | 427](#)
- [Point and Click CLI | 428](#)

Troubleshoot Ping Host

IN THIS SECTION

- [About Ping Host Page | 407](#)

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 160 on page 408](#) 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 161 on page 409](#). 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 160: 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 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. |
| 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. |

Table 160: Ping Host Troubleshooting Options (*continued*)

| Field | Action |
|----------------|--|
| 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 161: 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. |

Table 161: Ping Host Results and Output Summary (*continued*)

| Field | Function |
|---|--|
| round-trip min/avg/max/stddev = <i>min-time</i> / <i>avg-time</i> / <i>max-time</i> / <i>std-dev</i> ms | <ul style="list-style-type: none"> • <i>min-time</i>—Minimum round-trip time (see time=time 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. |
| 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 | 410](#)
[Troubleshoot Traceroute | 415](#)
[Troubleshoot Packet Capture | 418](#)

Troubleshoot Ping MPLS

IN THIS SECTION

- [About Ping MPLS Page | 411](#)

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 162 on page 411](#) to troubleshoot the issue.
3. Click **Start**.

The results of the ping operation are displayed in [Table 163 on page 413](#).

4. Click **OK** to stop the ping operation before it is complete.

Table 162: 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. |
| Detailed Output | Select the check box to display detailed output rather than brief ping output. |
| Ping LSP to Layer 3 VPN prefix | |

Table 162: Ping MPLS Troubleshooting Options (*continued*)

| Field | Action |
|------------------|--|
| 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 2 VPN Name | Type the name of the Layer 2 VPN to ping. |
| 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

Table 162: Ping MPLS Troubleshooting Options (*continued*)

| Field | Action |
|-----------------|---|
| 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. |
| 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 163: Ping MPLS Results and Output Summary

| Field | Function |
|-----------------------|--------------------------|
| Exclamation point (!) | Echo reply was received. |

Table 163: Ping MPLS Results and Output Summary (continued)

| Field | Function |
|-------------------------------------|--|
| Period (.) | Echo reply was not received within the timeout period. |
| x | Echo reply was received with an error code. Errored packets are not counted in the received packets count and are accounted for separately. |
| number packets transmitted | number —Number of ping requests (probes) sent to a host. |
| number packets received | number —Number of ping responses received from a host. |
| percentage packet loss | percentage —Number of ping responses divided by the number of ping requests, specified as a percentage. |
| 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 | 415](#)
[Troubleshoot Packet Capture | 418](#)

Troubleshoot Traceroute

IN THIS SECTION

- [About Traceroute Page](#) | 415

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 164 on page 416](#).

The Remote Host field is the only required field.

3. Click **Start**.

The results of the traceroute operation are displayed in [Table 165 on page 416](#). 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 164: 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. |
| 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 165: 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. |

Table 165: Ping Traceroute Results and Output Summary (continued)

| Field | Function |
|--|--|
| <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. |
| 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

| [Troubleshoot Packet Capture](#) | 418

Troubleshoot Packet Capture

IN THIS SECTION

- [About Packet Capture Page](#) | 418

About Packet Capture Page

You are here: **Device Administration** > **Tools** > **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.

To use J-Web packet capture:

1. Enter the information specified in [Table 166 on page 419](#) 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 167 on page 423](#).

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 166: 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> |
| 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> |

Table 166: Packet Capture Troubleshooting Options (*continued*)

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

Table 166: Packet Capture Troubleshooting Options (*continued*)

| Field | Description |
|-------------------------|--|
| 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. |
| 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 166: 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. |
| 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 167: Packet Capture Results and Output Summary

| Field | Function |
|----------------------------|---|
| <i>timestamp</i> | <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> |
| <i>direction</i> | <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> |
| <i>protocol</i> | <p>Displays the protocol for the packet.</p> <p>In the sample output, IP indicates the Layer 3 protocol.</p> |
| <i>source address</i> | <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> |
| <i>destination address</i> | <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> |
| <i>protocol</i> | <p>Displays the protocol for the packet.</p> <p>In the sample output, TCP indicates the Layer 4 protocol.</p> |
| <i>data size</i> | <p>Displays the size of the packet (in bytes).</p> |

RELATED DOCUMENTATION

[Troubleshoot Traceroute](#) | 415

Access CLI

IN THIS SECTION

- [About CLI Terminal Page](#) | 424

About CLI Terminal Page

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](#) | 425

View CLI Configuration

IN THIS SECTION

- [About CLI Viewer Page](#) | 426

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](#) | 427

Edit CLI Configuration

IN THIS SECTION

- [About CLI Editor Page | 427](#)

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

IN THIS SECTION

- [About Point and Click CLI Page | 428](#)

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 168 on page 429](#). [Table 169 on page 429](#) 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 168: 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 169: 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. |

Table 169: J-Web Configuration Editor Page Details (*continued*)

| Field | Function |
|----------------------------|--|
| 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. |
| 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. |
| 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. |

Table 169: J-Web Configuration Editor Page Details (*continued*)

| Field | Function |
|-------------------|--|
| 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. |
| 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. |

Table 169: J-Web Configuration Editor Page Details (*continued*)

| Field | Function |
|-----------------------|--|
| Smtp | Specifies that you can configure Simple Mail Transfer Protocol. The option available is: <ul style="list-style-type: none"> • Configure—Configures the feature. |
| Snmp | Specifies that you can configure Simple Network Management Protocol for monitoring router operation and performance. The option available is: <ul style="list-style-type: none"> • Configure—Configures the feature. |
| System | 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: <ul style="list-style-type: none"> • Edit—Edits the feature. • Delete—Deletes the feature. |
| Vlans | Specifies that you can edit or delete a virtual LAN. The options available are: <ul style="list-style-type: none"> • Edit—Edits the feature. • Delete—Deletes the feature. |
| Wlan | Specifies that you can configure a wireless local area network. The option available is: <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 | 427](#)

5

PART

Network

- Connectivity—Ports | 435
- Connectivity—VLAN | 446
- Connectivity—Link Aggregation | 452
- Connectivity—PPPoE | 459
- Connectivity—Wireless LAN | 461
- DHCP Client | 469
- DHCP Server | 473
- Firewall Filters—IPv4 | 482
- Firewall Filters—IPv6 | 497
- Firewall Filters—Assign to Interfaces | 509
- Source NAT | 511
- Destination NAT | 523
- Static NAT | 533
- NAT Proxy ARP/ND | 540
- Static Routing | 547

[RIP Routing | 551](#)

[OSPF Routing | 559](#)

[BGP Routing | 570](#)

[Routing Instances | 583](#)

[Routing—Policies | 587](#)

[Routing—Forwarding Mode | 601](#)

[CoS—Value Aliases | 603](#)

[CoS—Forwarding Classes | 607](#)

[CoS Classifiers | 610](#)

[CoS—Rewrite Rules | 615](#)

[CoS—Schedulers | 619](#)

[CoS—Scheduler Maps | 623](#)

[CoS—Drop Profile | 627](#)

[CoS—Virtual Channel Groups | 631](#)

[CoS—Assign To Interface | 635](#)

[Application QoS | 641](#)

Connectivity—Ports

IN THIS CHAPTER

- [About the Ports Page | 435](#)
- [Add a Logical Interface | 438](#)
- [Edit a Logical Interface | 444](#)
- [Delete Logical Interface | 445](#)

About the Ports Page

You are here: **Network** > **Connectivity** > **Ports**.

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.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a logical interface. See [“Add a Logical Interface” on page 438](#).
- Edit a logical interface. See [“Edit a Logical Interface” on page 444](#).
- Delete a logical interface. See [“Delete Logical Interface” on page 445](#).

Field Descriptions

[Table 170 on page 436](#) describes the fields to view interface configuration on the ports page.

NOTE:

- J-Web also 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 also 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 170: View Interface Configuration Details on the Ports Page

| Field | Action |
|------------|--|
| Filter | <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. |
| Go | Displays the list of interfaces based on the interface type, interface state, or zone association that you have used to filter the interface information. |
| Clear | Clears the filter options that you have selected and displays all the interfaces. |
| Expand All | Expands the tree under the list of interfaces. |

Table 170: View Interface Configuration Details on the Ports Page (*continued*)

| Field | Action |
|-----------------|--|
| Global Settings | <p>To configure global setting for the interface ports:</p> <ol style="list-style-type: none"> 1. Click Global Settings. The Global Settings 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. • Packet 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 | Disables the selected interface. |
| Enable | Enables the selected disabled interface. |

Table 171 on page 437 describes the fields on the ports page.

Table 171: Fields on the Ports 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> |

Table 171: Fields on the Ports Page (*continued*)

| Field | Description |
|-----------------------|---|
| 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. |
| MTU | Displays the maximum transmission unit value for this physical interface. |
| Speed | Displays the Interface speed (10 Mbps, 100 Mbps, 1 Gbps, or Auto). |
| Link Mode | Displays the link mode status for this interface. Status can be Active, Passive, or None. |
| Auto Negotiation | Displays the auto negotiation status of the interface. Status can be either Enabled or Disabled. |
| Media Type | Displays the media type of the operating modes (copper or fiber) for the 2-Port 10 Gigabit Ethernet XPIM. |

RELATED DOCUMENTATION

[Add a Logical Interface](#) | 438

Add a Logical Interface

You are here: **Network** > **Connectivity** > **Ports**.

To add a logical interface:

1. Select an interface and click the add icon (+) available on the upper right side of the Ports page.
The Add Interface page appears.
2. Complete the configuration according to the guidelines provided in [Table 172 on page 439](#).
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 172 on page 439](#) provides guidelines on using the fields on the Add Interface page.

Table 172: 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. |
| 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). |

Table 172: Fields on the Add Interface Page (*continued*)

| Field | Description |
|----------------------------------|--|
| Enable address configuration | <p>Select this option to add IPv4 address.</p> <p>To add IPv4 address:</p> <ol style="list-style-type: none"> 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. <p>In the ARP Address page, click + and enter the IPv4 Address, MAC Address, and select Publish.</p> <p>Click OK to save the changes.</p> |
| IPv6 Address | |
| IPv6 Address/DHCP configuration | <p>Select the check box to enable this option.</p> <p>NOTE: Not available for irb interface</p> |
| Enable DHCP | Select this option to enable DHCP. |
| Enable address configuration | <p>Select this option to add IPv6 address.</p> <p>To add IPv6 address:</p> <ol style="list-style-type: none"> 1. Click +. 2. Enter an IPv6 address. |
| Ethernet Switching | |
| Ethernet Switching configuration | <p>Select the check box to enable this option.</p> <p>NOTE: Not available for irb interface</p> |
| Interface Mode | <p>Select an option from the list:</p> <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. |

Table 172: Fields on the Add Interface Page (*continued*)

| Field | Description |
|---------------------------|--|
| 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. |
| 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 172: 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. |
| 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. |

Table 172: Fields on the Add Interface Page (*continued*)

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

Table 172: Fields on the Add Interface Page (continued)

| Field | Description |
|--------------------------|---|
| 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 a Logical Interface 444 |
| Delete Logical Interface 445 |

Edit a Logical Interface

You are here: **Network > Connectivity > Ports.**

To edit a logical interface:

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

The interface options appears with editable fields. For more information on the options, see [“Add a Logical Interface” on page 438](#).
3. Click **OK**.

RELATED DOCUMENTATION

| |
|--|
| Delete Logical Interface 445 |
|--|

Delete Logical Interface

You are here: **Network** > **Connectivity** > **Ports**.

To delete a logical interface:

1. Select a logical interface that you want to delete from the Ports page.
2. Click the delete icon (X) available on the upper right side of the page.

A confirmation window appears.

3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

[Add a Logical Interface](#) | 438

[Edit a Logical Interface](#) | 444

Connectivity—VLAN

IN THIS CHAPTER

- [About the VLAN Page | 446](#)
- [Add a VLAN | 447](#)
- [Edit a VLAN | 449](#)
- [Delete VLAN | 450](#)
- [Assign an Interface to VLAN | 450](#)

About the VLAN Page

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 447](#).
- Edit a VLAN. See [“Edit a VLAN” on page 449](#).
- Delete a VLAN. See [“Delete VLAN” on page 450](#).
- Assign Interface. See [“Assign an Interface to VLAN” on page 450](#).
- Show or hide columns in the VLAN table. To do this, use the Show Hide Columns icon in the top right corner of the page and select the options you want to show or deselect to hide options on the page.
- 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 173 on page 447 describes the fields on the VLAN page.

Table 173: 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. |
| Description | Displays a brief description for the VLAN. |

RELATED DOCUMENTATION

| [Add a VLAN](#) | 447

Add a VLAN

You are here: **Network > Connectivity > VLAN.**

To add a VLAN:

- 1. Click the add icon (+) available on the upper right side of the VLAN page.

The Add VLAN page appears.

2. Complete the configuration according to the guidelines provided in [Table 174 on page 448](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

[Table 174 on page 448](#) provides guidelines on using the fields on the Add VLAN page.

Table 174: 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. |
| 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. |

Table 174: Fields on the Add VLAN Page (continued)

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

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. |
| Subnet | Enter the range of logical addresses within the address space that is assigned to an organization. For example, 255.255.255.0. You can also specify the address prefix. |
| IP Address | Enter the IP address of the VLAN. The available options are as follows: <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. |

IPv6 Address

NOTE: This option is available only when you select VLAN ID type as Single.

| | |
|--------------|--|
| IPv6 Address | Enter the IPv6 address of the VLAN. |
| Prefix | Select the destination prefix of the VLAN. |

RELATED DOCUMENTATION

[Edit a VLAN](#) | 449

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 side of the page.

The Edit VLAN page appears with editable fields. For more information on the options, see [“Add a VLAN” on page 447](#).

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

RELATED DOCUMENTATION

| [Delete VLAN | 450](#)

Delete 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 side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

| [Assign an Interface to VLAN | 450](#)

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 right side of the VLAN page.

The Assign Interfaces page appears.

3. Complete the configuration according to the guidelines provided in [Table 175 on page 451](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 175: 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 | 447](#)

Connectivity—Link Aggregation

IN THIS CHAPTER

- [About the Link Aggregation Page | 452](#)
- [Link Aggregation Global Settings | 453](#)
- [Add a Logical Interface to Link Aggregation | 454](#)
- [Add a Link Aggregation | 456](#)
- [Edit an Aggregated Interface | 457](#)
- [Delete Link Aggregation | 458](#)
- [Search for Text in the Link Aggregation Table | 458](#)

About the Link Aggregation Page

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 453](#).
- Add Logical Interface. See [“Add a Logical Interface to Link Aggregation” on page 454](#).
- Enable/Disable LACP link-protection. To do this, select a link aggregation and click **Enable/Disable** available at the upper right side of the Link Aggregation table.
- Add Link Aggregation. See [“Add a Link Aggregation” on page 456](#).
- Edit Link Aggregation. See [“Edit an Aggregated Interface” on page 457](#).
- Delete Link Aggregation. See [“Delete Link Aggregation” on page 458](#).

- Search for text in a link aggregation table. See [“Search for Text in the Link Aggregation Table” on page 458](#).
- Show or hide columns in the Link Aggregation table. To do this, use the Show Hide Columns icon in the top right corner of the page and select the options you want to show or deselect to hide options on the page.

Field Descriptions

[Table 176 on page 453](#) describes the fields on the Link Aggregation page.

Table 176: 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 | Displays whether the interface is VLAN-tagged (enabled) or untagged (disabled). |
| Enabled/Disabled | Displays whether the LACP link-protection is enabled or disabled. |
| Description | Provides a description of the LAG. |

RELATED DOCUMENTATION

[Link Aggregation Global Settings](#) | 453

Link Aggregation Global Settings

You are here: **Network > Connectivity > Link Aggregation**.

To add link aggregation global settings:

- 1. Complete the configuration according to the guidelines provided in [Table 177 on page 454](#).

Table 177: Fields on the Link Aggregation Global Settings page

| Field | Action |
|---|--|
| Global Settings | |
| Device Count | Enter the device count. The range is 1 through 28. |
| Advanced Settings | |
| NOTE: This option is not available for SRX5000 line of devices. | |
| LACP Configuration | Specifies global Link Aggregation Control Protocol configuration. |
| System Priority | Click the arrow button to select the priority level that you want to associate with the LAG. |
| Link Protection | Select the option to protect the link. NOTE: You can configure only two member links for an aggregated Ethernet interface, that is, one active and one standby. |
| Non-Revertive | Enable or disable the option to not to choose even if a higher priority link is available. |

RELATED DOCUMENTATION

| [Add a Logical Interface to Link Aggregation](#) | 454

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 right side of the Link Aggregation page.

The Add Logical Interface page appears.

3. Complete the configuration according to the guidelines provided in [Table 178 on page 455](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 178: Fields on the Add Logical Interface Page

| Field | Action |
|---------------------------|---|
| Aggregated Interface Name | Displays aggregated interface name. |
| Logical Interface Unit | Enter the logical interface unit. |
| 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 | Enter a valid IPv6 address. |
| Subnet Mask | Enter a valid subnet mask for IPv6 address. |

RELATED DOCUMENTATION

| [Add a Link Aggregation](#) | 456

Add a Link Aggregation

You are here: **Network > Connectivity > Link Aggregation.**

To add a link aggregation:

1. Click the add icon (+) on the upper right side of the Link Aggregation page.
The Create Link Aggregation page appears.
2. Complete the configuration according to the guidelines provided in [Table 179 on page 456](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 179: Fields on the Create Link Aggregation Page

| Field | Action |
|--------------------------|---|
| General Settings | |
| AE Name | Enter the aggregated interface name. NOTE: If an aggregated interface already exists, then the field is displayed as read-only. |
| Interfaces | Select the interface available for aggregation and move to Selected column using right arrow. NOTE: Only interfaces that are configured with the same speed can be selected together for a LAG. |
| Advanced Settings | |
| LACP Configuration | Specifies global Link Aggregation Control Protocol configuration. |
| LACP Mode | Select a mode in which Link Aggregation Control Protocol packets are exchanged between the interfaces. The modes are: <ul style="list-style-type: none"> ● Active—Indicates that the interface initiates transmission of LACP packets ● Passive—Indicates that the interface only responds to LACP packets. |
| Periodic | Select a periodic transmissions of link aggregation control PDUs occur at different transmission rate. The options available are: <ul style="list-style-type: none"> ● fast—Transmit link aggregation control PDUs every second. ● slow—Transmit link aggregation control PDUs every 30 seconds. |

Table 179: Fields on the Create Link Aggregation Page (*continued*)

| Field | Action |
|-----------------|--|
| System Priority | Click the arrow button to select the priority level that you want to associate with the LAG. |
| Link Protection | Enable or disable the option to protect the link. NOTE: You can configure only two member links for an aggregated Ethernet interface, that is, one active and one standby. |
| Non-Revertive | Enable or disable the option to not to choose even if a higher priority link is available. |
| Description | Enter a description for the LAG. |
| VLAN Tagging | Enable or disable VLAN tagging for a LAG. |

RELATED DOCUMENTATION

[Edit an Aggregated Interface](#) | 457

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 side 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 456](#).

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

RELATED DOCUMENTATION

[Delete Link Aggregation](#) | 458

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 side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the Link Aggregation Page](#) | 452

Search for Text in the Link Aggregation Table

You are here: **Network** > **Connectivity** > **Link Aggregation**.

You can use the search icon in the top 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](#) | 452

Connectivity—PPPoE

IN THIS CHAPTER

- [Configure PPPoE | 459](#)

Configure PPPoE

NOTE: This menu is available only for SRX300 lines of devices and SRX550M device.

You are here: **Network > Connectivity > PPPoE.**

PPPoE connects multiple hosts on an Ethernet LAN to a remote site through a single customer premises equipment (CPE) device (Juniper Networks device).

Use the configure PPPoE tasks to configure the PPPoE connection. The PPPoE wizard guides you to set up a PPPoE client over the Ethernet connection.

NOTE: On all branch SRX Series devices, the PPPoE wizard has the following limitations:

- While you use the load and save functionality, the port details are not saved in the client file.
- The Non Wizard connection option cannot be edited or deleted through the wizard. Use the CLI to edit or delete the connections.
- The PPPoE wizard cannot be launched if the backend file is corrupted.
- The PPPoE wizard cannot be loaded from the client file if non-wizard connections share the same units.
- The PPPoE wizard cannot load the saved file from one platform to another platform.
- There is no backward compatibility between PPPoE wizard Phase 2 to PPPoE wizard Phase 1. As a result, the PPPoE connection from Phase 2 will not be shown in Phase 1 when you downgrade to an earlier release.

RELATED DOCUMENTATION

Configure VPN.

Connectivity—Wireless LAN

IN THIS CHAPTER

- [About the Settings Page | 461](#)
- [Create an Access Point | 462](#)
- [Edit an Access Point | 463](#)
- [Delete Access Point | 464](#)
- [Create an Access Point Radio Settings | 465](#)
- [Edit an Access Point Radio Settings | 467](#)
- [Delete Access Point Radio Settings | 468](#)

About the Settings Page

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 462](#).
- Edit an access point. See [“Edit an Access Point” on page 463](#).
- Delete an access point. See [“Delete Access Point” on page 464](#).
- Create access point radio settings. See [“Create an Access Point Radio Settings” on page 465](#).

- Edit access point radio settings. See [“Edit an Access Point Radio Settings”](#) on page 467.
- Delete access point radio settings. See [“Delete Access Point Radio Settings”](#) on page 468.

Field Descriptions

[Table 180 on page 462](#) describes the fields on the Settings page.

Table 180: 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. |

Release History Table

| 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. See [Create an Access Point](#) | 462.

Create an Access Point

You are here: **Network** > **Connectivity** > **Wireless LAN** > **Settings**.

To create an access point:

1. Click the add icon (+) on the upper right side of the Settings page.

The Create Access Point Configuration page appears.

2. Complete the configuration according to the guidelines provided in [Table 181 on page 463](#).
3. Click **OK** to save the changes.

An access point is created.

If you want to discard your changes, click **Cancel**.

Table 181: : 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. |
| 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 461 |
| Edit an Access Point 463 |
| Delete Access Point 464 |
| Create an Access Point Radio Settings 465 |

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 side 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 462](#).

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

RELATED DOCUMENTATION

[About the Settings Page | 461](#)

[Delete Access Point | 464](#)

Delete 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 side 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 | 461](#)

[Create an Access Point | 462](#)

[Edit an Access Point | 463](#)

Create an Access Point Radio Settings

You are here: **Network** > **Connectivity** > **Wireless LAN** > **Settings**.

To create an access point radio setting:

1. Click the add icon (+) on the upper right side of the Radio Settings table.

The Create Access Point Radio Settings page appears.

2. Complete the configuration according to the guidelines provided in [Table 182 on page 465](#).

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

The access point radio settings are created.

If you want to discard your changes, click **Cancel**.

Table 182: Fields on the Create Access Point Radio Settings Page

| Field | Action |
|--------------|------------------------------------|
| Radio | |
| Radio Type | Select a radio type from the list. |
| Radio State | Select the radio state to enable. |

Table 182: 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: <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: <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. |

Table 182: Fields on the Create Access Point Radio Settings Page (*continued*)

| Field | Action |
|-------------------------------------|--|
| | <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 | 461](#)
[Edit an Access Point Radio Settings | 467](#)
[Delete Access Point Radio Settings | 468](#)

Edit an Access Point Radio Settings

You are here: **Network > Connectivity > Wireless LAN > Settings.**

To edit an access point radio setting:

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 side 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 Settings” on page 465](#).

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

RELATED DOCUMENTATION

[About the Settings Page | 461](#)

[Delete Access Point Radio Settings | 468](#)

Delete Access Point Radio Settings

You are here: **Network** > **Connectivity** > **Wireless LAN** > **Settings**.

To delete an access point radio setting:

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 side 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 | 461](#)

[Create an Access Point Radio Settings | 465](#)

[Edit an Access Point Radio Settings | 467](#)

DHCP Client

IN THIS CHAPTER

- About the DHCP Client Page | 469
- Add DHCP Client Information | 470
- Delete DHCP Client Information | 471

About the DHCP Client Page

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 470.](#)
- Delete DHCP client information. See [“Delete DHCP Client Information” on page 471.](#)

Field Descriptions

[Table 183 on page 469](#) describes the fields on the DHCP Client page.

Table 183: 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. |

Table 183: Fields on the DHCP Client Page *(continued)*

| Field | Description |
|------------|--|
| 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](#) | 470

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 184 on page 470](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 184: 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. |

Table 184: Fields on the DHCP Client Information Page (*continued*)

| Field | Action |
|------------------------|---|
| 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 | <p>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.</p> |

RELATED DOCUMENTATION

[Delete DHCP Client Information](#) | 471

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 | 469](#)

[Add DHCP Client Information | 470](#)

DHCP Server

IN THIS CHAPTER

- [About the DHCP Server Page | 473](#)
- [Add a DHCP Pool | 475](#)
- [Edit a DHCP Pool | 478](#)
- [Delete DHCP Pool | 479](#)
- [DHCP Groups Global Settings | 479](#)
- [Add a DHCP Group | 480](#)
- [Edit a DHCP Group | 480](#)
- [Delete DHCP Group | 481](#)

About the DHCP Server Page

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 475](#).
- Edit a DHCP Pool. See [“Edit a DHCP Pool” on page 478](#).
- Delete a DHCP Pool. See [“Delete DHCP Pool” on page 479](#).
- Configure DHCP group global settings. See [“DHCP Groups Global Settings” on page 479](#).
- Add a DHCP group. See [“Add a DHCP Group” on page 480](#).
- Edit a DHCP group. See [“Edit a DHCP Group” on page 480](#).
- Delete a DHCP group. See [“Delete DHCP Group” on page 481](#).

Field Descriptions

Table 185 on page 474 describes the fields on the DHCP Server page.

Table 185: 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. |
| 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](#) | 475

Add a DHCP Pool

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

To add a DHCP Pool:

1. Click the add icon (+) on the upper right side of the DHCP Pools table.
The Add DHCP Pool page appears.
2. Complete the configuration according to the guidelines provided in [Table 186 on page 475](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

[Table 186 on page 475](#) describes the Add DHCP Pool Page.

Table 186: 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. |

Table 186: Fields on the Add DHCP Pool Page. (continued)

| Field | Action |
|---------------------------|--|
| 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. |
| Maximum Lease Time (Secs) | Enter a from value 60 through 1,209,600. Specifies the maximum length of time in seconds, a client can hold a lease. (Dynamic BOOTP lease lengths can exceed this maximum time.) |
| 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) | Enter a number of seconds the lease is retained. range is 0 through 4,294,967,295. By default, 0 is no grace period. |
| DNS Name Servers | Specifies the DNS name to assign to the DHCP client in the address pool. Click any one of the following: <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 | Specifies the WINS servers to assign to the DHCP client in the address pool. Click any one of the following: <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 186: 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.

| | |
|------|--|
| 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. |

Table 186: Fields on the Add DHCP Pool Page. (continued)

| Field | Action |
|---|---|
| <p>Static Bindings</p> <p>Click + to add DHCP static bindings. After configuring the attributes, click OK to save the changes.</p> <p>Selected a DHCP static binding and click the pencil icon to edit it or click X to delete it.</p> | |
| 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](#) | 478.

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 side 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 475.](#)

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

RELATED DOCUMENTATION

[Delete DHCP Pool](#) | 479.

Delete 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 side of the DHCP Pools table.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

| [DHCP Groups Global Settings](#) | 479.

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 side 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 480 |
| Edit a DHCP Group 480 |
| Delete DHCP Group 481 |

Add a DHCP Group

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

To add a DHCP Group:

1. Click the add icon (+) on the upper right side of the DHCP Groups table.
The Add DHCP Group page appears.
2. Complete the configuration according to the guidelines provided in [Table 187 on page 480](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

[Table 187 on page 480](#) describes the fields on the Add DHCP Group.

Table 187: 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 | 480](#)
- [Delete DHCP Group | 481](#)
- [DHCP Groups Global Settings | 479](#)

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 side 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 480](#).

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

RELATED DOCUMENTATION

| |
|---|
| DHCP Groups Global Settings 479 |
| Add a DHCP Group 480 |
| Delete DHCP Group 481 |

Delete 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 side of the DHCP Groups table.
- 3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

| |
|---|
| DHCP Groups Global Settings 479 |
| Add a DHCP Group 480 |
| Edit a DHCP Group 480 |

Firewall Filters—IPv4

IN THIS CHAPTER

- About the IPv4 Page | 482
- Add IPv4 Firewall Filters | 483

About the IPv4 Page

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 483.](#)

Field Descriptions

[Table 188 on page 482](#) describes the fields on the IPv4 page.

Table 188: 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. |

Table 188: Fields on the IPv4 Page (*continued*)

| Field | Description |
|----------|---|
| Location | Specifies the position of the new filter. |

RELATED DOCUMENTATION

[Add IPv4 Firewall Filters](#) | 483.

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 189 on page 483](#) and [Table 190 on page 485](#).
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 189: 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. |

Table 189: Fields on the Add IPv4 Firewall Filter Page (*continued*)

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

Table 189: Fields on the Add IPv4 Firewall Filter Page (*continued*)

| Field | Action |
|-----------|---|
| 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. |
| 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 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 | <p>Positions the new term in one of the following locations:</p> <ul style="list-style-type: none"> • After Final IPv4 Filter—At the end of all term. • After IPv4 Filter—After a specified term. • Before IPv4 Filter—Before a specified term. |
| Add | Opens the Filter Term page allowing you to define the match conditions and the action for this term. |

Table 190: Fields on the Match Criteria for IPv4 Firewall Filter

| Field | Action |
|--------------|--------|
| Match Source | |

Table 190: 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. |
| 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 | |

Table 190: Fields on the Match Criteria for IPv4 Firewall Filter (*continued*)

| Field | Action |
|------------------------------------|--|
| 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> |
| 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 190: 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 190: 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> |
| 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> |

Table 190: Fields on the Match Criteria for IPv4 Firewall Filter (*continued*)

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

Table 190: Fields on the Match Criteria for IPv4 Firewall Filter (*continued*)

| Field | Action |
|-----------|---|
| 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> |
| 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. |

Table 190: Fields on the Match Criteria for IPv4 Firewall Filter (*continued*)

| Field | Action |
|---|--|
| 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. |
| Precedence | <p>Enter IP precedences to be included in, or excluded from, the match condition. Allows you to remove an IP precedence entry from the match condition.</p> <p>The options available are:</p> <ul style="list-style-type: none"> • Add—To include the precedence in the match condition. • Except—To exclude the precedence from the match condition and then select Add—To include the precedence in the match condition. • Delete—To remove an IP precedence from the match condition. |
| 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 NOTE: This option is not available in SRX5600 device. | <p>Enter an IPv4 TTL value by entering a number from 1 through 255, and select an option.</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 190: 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. |
| 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 | |

Table 190: Fields on the Match Criteria for IPv4 Firewall Filter (*continued*)

| Field | 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> |
| 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> |

Table 190: Fields on the Match Criteria for IPv4 Firewall Filter (*continued*)

| Field | Action |
|---|---|
| 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 NOTE: This option is not available in SRX345 of devices. | Enter a string identifying the virtual channel. |
| Prefix Action NOTE: This option is not available in SRX4100 and SRX345 devices. | Enter the prefix action. |
| 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> |
| Port Mirror NOTE: This option is not available in SRX5600 and SRX345 devices. | <p>Select Port Mirror.</p> <p>Port mirrors the packet.</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](#) | [482](#).

Firewall Filters—IPv6

IN THIS CHAPTER

- About the IPv6 Page | 497
- Add IPv6 Firewall Filters | 498

About the IPv6 Page

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 498.](#)

Field Descriptions

[Table 191 on page 497](#) describes the fields on IPv6 page.

Table 191: 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. |

Table 191: Fields on the IPv6 Page (continued)

| Field | Description |
|----------|---|
| Location | Specifies the position of the new filter. |

RELATED DOCUMENTATION

| [Add IPv6 Firewall Filters](#) | 498.

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 192 on page 498](#) and [Table 193 on page 501](#).
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 192 on page 498](#) describes the fields on the Add IPv6 page.

Table 192: 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. |

Table 192: 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 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 | |
| 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> |

Table 192: Fields on the Add IPv6 Firewall Filter Page (*continued*)

| Field | Action |
|----------------------------|---|
| Add New IPv6 Filter | |
| 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. |
| 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 | |

Table 192: Fields on the Add IPv6 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 IPv6 Filter—After a specified filter. • Before IPv6 Filter—Before a specified filter. |
| Add | Click Add . Opens the Filter Term page allowing you to define the match conditions and the action for this term. |

Table 193: Fields on the Match Criteria for IPv6 Firewall Filter

| Field | Action |
|---------------------|---|
| Match Source | |
| Source Address | 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. 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. Enter an IP source address and prefix length, and select an option: <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 | 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. Select an option: <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. |

Table 193: Fields on the Match Criteria for IPv6 Firewall Filter (*continued*)

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

Table 193: Fields on the Match Criteria for IPv6 Firewall Filter (*continued*)

| Field | Action |
|------------------------------------|---|
| 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 | |
| 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 193: 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. |
| 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. |

Table 193: Fields on the Match Criteria for IPv6 Firewall Filter (*continued*)

| Field | Action |
|---------------------------------|---|
| 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> |
| 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. <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. |

Table 193: 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 193: 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> |
| 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> |

Table 193: Fields on the Match Criteria for IPv6 Firewall Filter (*continued*)

| Field | Action |
|-------------------------|---|
| 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 | 497.](#)

Firewall Filters—Assign to Interfaces

IN THIS CHAPTER

- About the Assign to Interfaces Page | 509

About the Assign to Interfaces Page

You are here: You are here: **Network** > **Firewall Filters** > **Assign To Interfaces**.

Use this page to configure interface for firewall filters.

Field Descriptions

Table 194 on page 509 describes the fields on the Assign Interfaces page.

Table 194: 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. |

Table 194: Fields on the Assign Interfaces Page (continued)

| Field | Description |
|-------------------------|--|
| 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 483 |
| Add IPv6 Firewall Filters 498 |

Source NAT

IN THIS CHAPTER

- [About the Source Page | 511](#)
- [Global Settings | 514](#)
- [Add a Source Rule Set | 515](#)
- [Edit a Source Rule Set | 518](#)
- [Delete Source Rule Set | 519](#)
- [Add a Source NAT Pool | 519](#)
- [Edit a Source NAT Pool | 521](#)
- [Delete Source NAT Pool | 521](#)

About the Source Page

You are here: **Network** > **NAT** > **Source**.

Use this page to configure source NAT.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a global setting. See [“Global Settings” on page 514](#).
- Add a source rule set. See [“Add a Source Rule Set” on page 515](#).
- Edit a source rule set. See [“Edit a Source Rule Set” on page 518](#).
- Delete a source rule set. See [“Delete Source Rule Set” on page 519](#).
- Add a source NAT pool. See [“Add a Source NAT Pool” on page 519](#).
- Edit a source NAT pool. See [“Edit a Source NAT Pool” on page 521](#).

- Delete a source NAT pool. See [“Delete Source NAT Pool” on page 521](#).
- Launch NAT wizard. To do this, click **Launch Wizard** option at the right side 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 195 on page 512](#) describes the fields on the Source Page.

Table 195: Fields on the Source Page.

| Field | Description |
|-----------------------------------|---|
| Source NAT Rule Set | |
| From | Displays the source NAT sort options from which the packets flow. The options available are: <ul style="list-style-type: none"> • Routing Instance • Zone • Interface |
| To | Displays the source NAT sort options to which the packets flow. The options available are: <ul style="list-style-type: none"> • Routing Instance • Zone • Interface |
| Filter | Displays the filter option. |
| Name | Displays the name of the source NAT rule set. |
| From | Displays the name of the routing instance, zone, or interface from which the packets flow. |
| To | Displays the name of the routing instance, zone, or interface to which the packets flow. |
| Rule | Displays the name of the rule in the selected source NAT rule set. |
| Description | Displays a description of the source NAT rule set. |
| Rules in Selected Rule-Set | |

Table 195: Fields on the Source Page. (continued)

| Field | Description |
|------------------------|--|
| Rule Name | Displays the name of the rule in the selected source NAT rule set. |
| Source Addresses | Displays the match source address. |
| Source Ports | Displays the match source ports. |
| Destination Addresses | Displays the match destination address. |
| Destination Ports | Displays the match destination port. |
| IP Protocol | Displays the match IP protocol. |
| Action | Displays the action of the rule. |
| Persistent | Displays the persistent NAT address in the source NAT pool |
| Upper Threshold | Displays the upper threshold value at which an SNMP trap is triggered. |
| Lower Threshold | Displays the lower threshold value at which an SNMP trap is triggered. |
| Description | Displays the description of the rule. |
| Source NAT Pool | |
| Name | Displays the name of the source NAT pool. |
| Address | Displays the IP address of the source NAT pool. |
| Port | Displays the port address of the source NAT pool. |
| Description | Displays the description of the source NAT pool. |
| Upper Threshold | Displays the upper threshold at which an SNMP trap is triggered. Range: 50 through 100. |
| Lower Threshold | Displays the lower threshold at which an SNMP trap is triggered. Range: 40 through 100. |

RELATED DOCUMENTATION

| [Global Settings](#) | 514.

Global Settings

You are here: **Network** > **NAT** > **Source**.

To add global settings for a source NAT rule set:

1. Click the **Global Settings** available on the upper right side of the page.
The Global Settings page appears.
2. Complete the configuration according to the guidelines provided in [Table 196 on page 514](#).
3. Click **OK** to save the changes.

Table 196: Fields on the Global Settings Page

| Field | Action |
|-----------------------------------|--|
| Address Persistent | Select check box to the enable address persistence. Provides source address to maintain same translation. |
| Port randomization | Select check box to the enable source NAT port randomization. |
| Pool Utilization Alarm | |
| Clear Threshold | Enter the clear threshold value for pool utilization. Range: 40 through 100. |
| Raise Threshold | Enter the raise threshold value for pool utilization. Range: 50 through 100. |
| Interface Port-Overloading | |
| On | Select to the enable source NAT interface with port overloading. |
| Factor | Enter a value for the port overloading capacity for the source NAT interface. |
| Off | Select to the disable source NAT interface with port overloading. |

RELATED DOCUMENTATION

| [Add a Source Rule Set](#) | 515.

Add a Source Rule Set

You are here: **Network** > **NAT** > **Source**.

To add a source rule set:

1. Click the add icon (+) on the upper right side of the Source page.
The Add Rule Set page appears.
2. Complete the configuration according to the guidelines provided in [Table 197 on page 515](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 197: Fields on the Add Rule Set Page

| Field | Action |
|----------------------|---|
| Rule Set Name | Enter a rule set name. |
| Rule Set Description | Enter a description for the rule set. |
| From | <div>Select an option from the list:<ul style="list-style-type: none">• Routing Instance• Zone• Interface<div>Select the source routing instances, zones, or interfaces in the Available column and use the right arrow to move them to the Selected column.</div></div> |
| To | <div>Select an option from the list:<ul style="list-style-type: none">• Routing Instance• Zone• Interface<div>Select the destination routing instances, zones, or interfaces in the Available column and use the right arrow to move them to the Selected column.</div></div> |

Table 197: Fields on the Add Rule Set Page (*continued*)

| Field | Action |
|---------------------------------|---|
| Rules | |
| Rules | Specifies the rules added to the selected source rule set. |
| Add Rules | |
| + | Click + available at the upper right of the Rules table. The Add Rule page appears. |
| Rule Name | Enter a rule name. |
| Rule Description | Enter a description for the rule. |
| Match | Displays the match source and destination addresses. |
| Source addresses and Ports | <p>Enter the following details:</p> <ul style="list-style-type: none"> • Source Address—Select an IPv4 or IPv6 address from the list and move it from the Available column to the Selected column using the right arrow. Or enter an IP address in the Selected column and click + to add it. • Ports—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. • IP Protocol—Select a protocol from the list or enter a protocol number and click +. |
| Destination addresses and Ports | <p>Enter the following details:</p> <ul style="list-style-type: none"> • Destination Address—Select an IPv4 or IPv6 address from the list and move it from the Available column to the Selected column using the right arrow. Or enter an IP address in the Selected column and click + to add it. • 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. |
| Action | |
| No Source NAT | None |

Table 197: Fields on the Add Rule Set Page (*continued*)

| Field | Action |
|---|--|
| Do Source NAT With Egress Interface Address | <p>Enable the Persistent check box and enter the following:</p> <ul style="list-style-type: none"> • Permit—Select an option from the list: <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. (The reflexive transport address is the public IP address and port created by the NAT device closest to the STUN server.) 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 host's 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 host's IP address and port. <p>NOTE: The target-host-port configuration is not supported for NAT64 when configured with IPv6 address.</p> • Inactivity Timeout—Enter the value in seconds for the persistent NAT binding remains in the SRX device memory when all the sessions of the binding entry are gone. When the configured timeout is reached, the binding is removed from memory. Range: 60 through 7200. • Max Session Number—Enter the number of the sessions with which a persistent NAT binding can be associated. Range: 8 through 65,536. |
| Utilization Alarm | |
| Upper Threshold | <p>Enter an upper threshold value at which an SNMP trap is triggered.</p> <p>Range: 1 through 4294967295.</p> |
| Lower Threshold | <p>Enter a lower threshold value at which an SNMP trap is triggered.</p> <p>Range: 1 through 4294967295.</p> <p>NOTE: This option can be set only if you configure the upper threshold value.</p> |
| Edit Rules | <p>Select an existing rule and click the edit icon at the top right corner of the Rules table.</p> <p>The Edit Interface page appears with editable fields.</p> |

Table 197: Fields on the Add Rule Set Page (*continued*)

| Field | Action |
|--------------|---|
| Delete Rules | <p>Select an interface and click the delete icon at the top 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

[Edit a Source Rule Set](#) | 518.

Edit a Source Rule Set

You are here: **Network** > **NAT** > **Source**.

To edit a source rule set and its rules:

1. Select an existing source rule set profile that you want to edit on the Source page.
2. Click the pencil icon available on the upper right side of the page.

The Edit Source Rule Set page appears with editable fields. For more information on the options, see [“Add a Source Rule Set” on page 515](#).

NOTE: Alternatively, you can select the rule directly and click the pencil icon available on the upper right side of the Rules table to edit a rule for the selected rule set.

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

RELATED DOCUMENTATION

[Delete Source Rule Set](#) | 519.

Delete Source Rule Set

You are here: **Network** > **NAT** > **Source**.

To delete a source rule set and its rules:

1. Select one or more rule sets that you want to delete on the Source page.
2. Click the delete icon available on the upper right side of the page.

A confirmation window appears.

NOTE: Alternatively, you can select the rule directly and click the delete icon available on the upper right side 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

| [Add a Source NAT Pool](#) | 519.

Add a Source NAT Pool

You are here: **Network** > **NAT** > **Source**.

To add a source NAT pool:

1. Click the add icon (+) on the upper right side of the Source NAT Pool page.
The Add Source NAT Pool page appears.
2. Complete the configuration according to the guidelines provided in [Table 198 on page 520](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 198: Fields on the Add Source NAT Pool Page

| Field | Description |
|--------------------------|--|
| Pool Name | Enter a source NAT pool name. |
| Pool Description | Enter a description for the source NAT pool. |
| Routing Instance | Select a routing instance from the list. |
| Pool Address Family | Select a source NAT pool IPv4 or IPv6 address family. |
| Pool Addresses | <p>Enter the source NAT pool address range in the From and To text boxes. Click + to add the addresses.</p> <p>To delete any addresses, select the address you want to delete and click X.</p> |
| Port Translation | <p>Select a port translation option from the list:</p> <ul style="list-style-type: none"> • No Translation • Translation with Default Port Range (1024–65535) • Translation with Specified Port Range—Enter a port range from low to high. • Translation with Port Overloading Factor—Enter a value for the port overloading capacity for the source NAT interface. |
| Address Assignment | <p>Select an option:</p> <ul style="list-style-type: none"> • Enable Address Shared—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. <p>When a source NAT pool configured with no port translation has few external IP addresses available, or only one external IP address, the address shared option, with a many-to-one mapping, increases NAT resources and improves traffic.</p> <ul style="list-style-type: none"> • Enable Address Pooling—Select an option: <ul style="list-style-type: none"> • paired—Allows address-pooling paired. • no-paired—Allow address-pooling no-paired. |
| Utilization Alarm | |
| Upper Threshold | <p>Enter an upper threshold percentage at which an SNMP trap is triggered.</p> <p>Range: 50 through 100.</p> |

Table 198: Fields on the Add Source NAT Pool Page *(continued)*

| Field | Description |
|-----------------|--|
| Lower Threshold | Enter a lower threshold percentage at which an SNMP trap is triggered. Range: 40 through 100. NOTE: This option can be set only if you configure the upper threshold value. |

RELATED DOCUMENTATION

| [Edit a Source NAT Pool](#) | 521.

Edit a Source NAT Pool

You are here: **Network** > **NAT** > **Source**.

To edit a source NAT pool:

1. Select an existing source NAT pool that you want to edit on the Source page.
2. Click the pencil icon available on the upper right side of the page.

The Edit Source NAT Pool page appears with editable fields. For more information on the options, see [“Add a Source NAT Pool” on page 519](#).

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

RELATED DOCUMENTATION

| [Delete Source NAT Pool](#) | 521.

Delete Source NAT Pool

You are here: **Network** > **NAT** > **Source**.

To delete a source NAT pool:

1. Select one or more source NAT pools that you want to delete on the Source page.
2. Click the delete icon available on the upper right side of the page.
A confirmation message window appears.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

| [About the Source Page](#) | 511.

Destination NAT

IN THIS CHAPTER

- [About the Destination Page](#) | 523
- [Add a Destination Rule Set](#) | 525
- [Edit a Destination Rule Set](#) | 528
- [Delete Destination Rule Set](#) | 528
- [Add a Destination NAT Pool](#) | 529
- [Edit a Destination NAT Pool](#) | 531
- [Delete Destination NAT Pool](#) | 532

About the Destination Page

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 525.
- Add a Destination Rule Set. See [“Edit a Destination Rule Set”](#) on page 528.
- Delete a Destination Rule Set. See [“Delete Destination Rule Set”](#) on page 528.
- Add a Destination NAT Pool. See [“Add a Destination NAT Pool”](#) on page 529.
- Edit a Destination NAT Pool. See [“Edit a Destination NAT Pool”](#) on page 531.
- Delete a Destination NAT Pool. See [“Delete Destination NAT Pool”](#) on page 532.
- Launch NAT wizard. To do this, click **Launch Wizard** option at the right side 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 199 on page 524 describes the fields on the Destination Page.

Table 199: 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 |
| To | Displays the destination NAT sort options to which the packets flow. The options available are: <ul style="list-style-type: none"> • Routing Instance • Zone • Interface |
| Filter | Displays the filter option. |
| Name | Displays the name of the 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 199: 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. |
| Description | Displays a description of the rule in the selected destination NAT rule set. |
| Destination NAT Pool | |
| Name | Displays the name of the destination NAT pool. |
| Address | Displays the IP address of the destination NAT pool. |
| Port | Displays the port address of the destination NAT pool. |
| Description | Displays a description of the destination NAT pool. |

RELATED DOCUMENTATION

[Add a Destination Rule Set](#) | 525.

Add a Destination Rule Set

You are here: **Network > NAT > Destination.**

To add a destination Rule Set:

1. Click the add icon (+) on the upper right side of the Destination page.
The Add Rule Set page appears.
2. Complete the configuration according to the guidelines provided in [Table 200 on page 526](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

[Table 200 on page 526](#) describes the fields on the Add Rule Set page.

Table 200: Fields on the Add Rule Set page.

| Field | Action |
|-----------------------------|--|
| Destination Rule Set | |
| Add Rule Set | |
| 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 Add to add the protocol to the IP Protocol column. |
| Actions | <p>Specifies the actions for the destination NAT pool. Select an option:</p> <ul style="list-style-type: none"> • No Destination NAT. • Do Destination NAT With Pool. |

Table 200: Fields on the Add Rule Set page. (continued)

| Field | Action |
|-------------------------------------|--|
| Do Destination NAT With Pool | |
| Add New Pool | Specifies the add option for the Do Destination NAT With Pool option. Click Add New Pool . |
| Add Destination Pool | |
| Pool Name | 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. |
| Destination NAT Pool | |
| 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. |

RELATED DOCUMENTATION

| [Edit a Destination Rule Set](#) | 528.

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 side 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 525](#).

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

RELATED DOCUMENTATION

| [Delete Destination Rule Set](#) | 528.

Delete Destination Rule Set

You are here: **Network** > **NAT** > **Destination**.

To delete destination rule set:

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 side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

| [Add a Destination NAT Pool](#) | 529.

Add a Destination NAT Pool

You are here: **Network > NAT > Destination.**

To add a Destination NAT Pool:

1. Click the add icon (+) on the upper right side of the Destination page.
The Add Rule Set page appears.
2. Complete the configuration according to the guidelines provided in [Table 201 on page 529](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

[Table 201 on page 529](#) describes the fields on the Add Rule Set Page.

Table 201: Fields on the Add Rule Set Page

| Field | Action |
|-----------------------------|--|
| Destination Rule Set | |
| Add Rule Set | |
| Rule Set Name | Specifies the name of the rule set. Enter the rule set name. |
| Rule Set Description | Specifies a description for the rule set. Enter a description for the rule set. |
| From | Specifies the filter options. Select an option: <ul style="list-style-type: none">• Routing Instance• Zone• Interface Select the routing instances/zones/interfaces in the Available column and the use the right arrow to move them to the Selected column. |
| Add Rule | |
| Rule Name | Specifies the name of the rule. Enter the rule name. |

Table 201: Fields on the Add Rule Set Page (*continued*)

| Field | Action |
|-------------------------------------|--|
| Rule Description | <p>Specifies a description for the rule.</p> <p>Enter a description for the rule.</p> |
| Match | |
| Source Address | <p>Specifies the source IP address. The options available are:</p> <ul style="list-style-type: none"> • Available—Specifies the available source addresses. • Selected—Specifies the selected source addresses. <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 | <p>Specifies the IP protocol for the destination NAT rule.</p> <p>Enter the protocol name in the text box and click Add to add the protocol to the IP Protocol column.</p> |
| Actions | <p>Specifies the actions for the destination NAT pool. Select an option:</p> <ul style="list-style-type: none"> • No Destination NAT. • Do Destination NAT With Pool. |
| Do Destination NAT With Pool | |
| Add New Pool | <p>Specifies the add option for the Do Destination NAT With Pool option.</p> <p>Click Add New Pool.</p> |
| Add Destination Pool | |
| Pool Name | Enter the name of the destination pool. |
| Pool Description | Enter a description for the destination pool. |
| Routing Instance | Select an option. |

Table 201: Fields on the Add Rule Set Page (continued)

| Field | Action |
|--------------------------------|--|
| 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. |
| Destination NAT Pool | |
| 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. |

RELATED DOCUMENTATION

[Edit a Destination NAT Pool](#) | 531.

Edit a Destination NAT Pool

You are here: **Network** > **NAT** > **Destination**.

To edit a Destination NAT Pool:

1. Select an existing destination NAT pool that you want to edit on the Destination page.

2. Click the pencil icon available on the upper right side 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 529](#).

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

RELATED DOCUMENTATION

| [Delete Destination NAT Pool | 532](#).

Delete Destination NAT Pool

You are here: **Network > NAT > Destination**.

To delete a Destination NAT Pool:

1. Select one or more destination NAT pools that you want to delete on the Destination page.
2. Click the delete icon available on the upper right side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

| [About the Destination Page | 523](#).

Static NAT

IN THIS CHAPTER

- [About the Static Page | 533](#)
- [Add a Static Rule Set | 535](#)
- [Edit a Static Rule Set | 538](#)
- [Delete Static Rule Set | 539](#)

About the Static Page

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 535](#).
- Edit a static rule set and its rules. See [“Edit a Static Rule Set” on page 538](#).
- Delete a static rule set and its rules. See [“Delete Static Rule Set” on page 539](#).
- Launch NAT wizard. To do this, click **Launch Wizard** option at the right side of the page. The NAT wizard leads you through the basic required steps to configure NAT for the SRX Series security device.
- 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 202 on page 534 describes the fields on the Static page.

Table 202: 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 | |
| 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. |

Table 202: Fields on the Static Page (continued)

| Field | Description |
|-----------------|---|
| 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 | 535](#)

[Edit a Static Rule Set | 538](#)

[Delete Static Rule Set | 539](#)

Add a Static Rule Set

You are here: **Network > NAT > Static.**

To add a static rule set:

1. Click the add icon (+) on the upper right side of the Static page.
The Add Rule Set page appears.
2. Complete the configuration according to the guidelines provided in [Table 203 on page 535](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 203: 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. |

Table 203: Fields on the Add Static Rule Set Page *(continued)*

| Field | Action |
|--------------|---|
| 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 203: 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. NOTE: You can select Translate to ipv4 address if you have selected IPv6 in the destination address. 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. NOTE: This option can be set only if you configure the upper threshold value. Click OK to save the changes. If you want to discard your changes, click Cancel. |

Table 203: Fields on the Add Static Rule Set Page *(continued)*

| Field | Action |
|--------|--|
| Edit | Select an existing rule and click the edit icon at the top right corner of the Rules table. The Edit Interface page appears with editable fields. |
| Delete | Select an interface and click the delete icon at the top right corner of the Rules table. A confirmation window appears. Click Yes to delete the selected interface or click No to discard. |

RELATED DOCUMENTATION

| |
|--|
| About the Static Page 533 |
| Edit a Static Rule Set 538 |
| Delete Static Rule Set 539 |

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 side 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 535.](#)

NOTE: Alternatively, you can select the rule directly and click the pencil icon available on the upper right side 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 | 533](#)

[Add a Static Rule Set | 535](#)

[Delete Static Rule Set | 539](#)

Delete 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 side 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 side 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 | 533](#)

[Add a Static Rule Set | 535](#)

[Edit a Static Rule Set | 538](#)

NAT Proxy ARP/ND

IN THIS CHAPTER

- [About the Proxy ARP/ND Page | 540](#)
- [Add a Proxy ARP | 541](#)
- [Edit a Proxy ARP | 542](#)
- [Delete a Proxy ARP | 543](#)
- [Add a Proxy ND | 544](#)
- [Edit a Proxy ND | 545](#)
- [Delete Proxy ND | 545](#)

About the Proxy ARP/ND Page

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 541](#).
- Edit a proxy ARP. See [“Edit a Proxy ARP” on page 542](#).
- Delete a proxy ARP. See [“Delete a Proxy ARP” on page 543](#).
- Create a proxy ND. See [“Add a Proxy ND” on page 544](#).
- Edit a proxy ND. See [“Edit a Proxy ND” on page 545](#).
- Delete a proxy ND. See [“Delete Proxy ND” on page 545](#).
- Launch NAT wizard. To do this, click **Launch Wizard** option at the right side 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 204 on page 541 describes the fields on the Proxy ARP/ND Configuration page.

Table 204: 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 541 |
| Edit a Proxy ARP 542 |
| Delete a Proxy ARP 543 |
| Add a Proxy ND 544 |
| Edit a Proxy ND 545 |
| Delete Proxy ND 545 |

Add a Proxy ARP

You are here: **Network > NAT > Proxy ARP/ND.**

To add a proxy ARP:

1. Click the add icon (+) on the upper right side 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 205 on page 542](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 205: 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 |
| Address | Enter the proxy ARP IP address. Click Delete to deleted the proxy ARP address. |
| Address/Range | Enter the source IP address range. Click Add to add the range address. |
| To | Enter the end IP address that the device can be assigned to. Click Add to add the port address. |

RELATED DOCUMENTATION

[About the Proxy ARP/ND Page | 540](#)

[Edit a Proxy ARP | 542](#)

[Delete a Proxy ARP | 543](#)

[Add a Proxy ND | 544](#)

[Edit a Proxy ND | 545](#)

[Delete Proxy ND | 545](#)

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 side 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 541](#).

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

RELATED DOCUMENTATION

| |
|---|
| About the Proxy ARP/ND Page 540 |
| Add a Proxy ARP 541 |
| Delete a Proxy ARP 543 |
| Add a Proxy ND 544 |
| Edit a Proxy ND 545 |
| Delete Proxy ND 545 |

Delete a Proxy ARP

You are here: **Network** > **NAT** > **Proxy ARP/ND**.

To delete proxy ARP:

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 side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

| |
|---|
| About the Proxy ARP/ND Page 540 |
| Add a Proxy ARP 541 |
| Edit a Proxy ARP 542 |
| Add a Proxy ND 544 |
| Edit a Proxy ND 545 |
| Delete Proxy ND 545 |

Add a Proxy ND

You are here: **Network** > **NAT** > **Proxy ARP/ND**.

To add a proxy ND:

1. Click the add icon (+) on the upper right side of the proxy ARP/ND page.
The Add Proxy ND page appears.
2. Complete the configuration according to the guidelines provided in [Table 206 on page 544](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 206: 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 |
| Address | Enter the proxy ND IP address. Click Delete to deleted the proxy ND address. |
| Address/Range | Enter the source IPv6 address range. Click Add to add the range address. |
| To | Enter the end IPv6 address that the device can be assigned to. Click Add to add the port address. |

RELATED DOCUMENTATION

[About the Proxy ARP/ND Page | 540](#)

[Add a Proxy ARP | 541](#)

[Edit a Proxy ARP | 542](#)

[Delete a Proxy ARP | 543](#)

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 side 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 544](#).

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

RELATED DOCUMENTATION

[About the Proxy ARP/ND Page | 540](#)

[Add a Proxy ARP | 541](#)

[Edit a Proxy ARP | 542](#)

[Delete a Proxy ARP | 543](#)

[Add a Proxy ND | 544](#)

[Delete Proxy ND | 545](#)

Delete Proxy ND

You are here: **Network** > **NAT** > **Proxy ARP/ND**.

To delete a proxy ND:

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 side of the page.

3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

| |
|---|
| About the Proxy ARP/ND Page 540 |
| Add a Proxy ARP 541 |
| Edit a Proxy ARP 542 |
| Delete a Proxy ARP 543 |
| Add a Proxy ND 544 |
| Edit a Proxy ND 545 |

Static Routing

IN THIS CHAPTER

- [About the Static Routing Page | 547](#)
- [Add a Static Route | 548](#)
- [Edit a Static Route | 549](#)
- [Delete Static Route | 550](#)

About the Static Routing Page

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 548](#).
- Edit a static route. See [“Edit a Static Route” on page 549](#).
- Delete a static route. See [“Delete Static Route” on page 550](#).

Field Descriptions

[Table 207 on page 547](#) describes the fields on the Static Routing page.

Table 207: Fields on the Static Routing Page

| Field | Description |
|----------|---|
| Route | Displays the static route selected. |
| Next-hop | Displays the selected next-hop address. |

Table 207: Fields on the Static Routing Page (continued)

| Field | Description |
|------------------|--|
| Routing Instance | Displays the routing instance selected for this route. |

RELATED DOCUMENTATION

[Add a Static Route](#) | 548

Add a Static Route

You are here: **Network** > **Routing** > **Static Routing**.

To add a static route:

1. Click the add icon (+) on the upper right side of the Static Routing page.
The Add Static Route page appears.
2. Complete the configuration according to the guidelines provided in [Table 208 on page 548](#).
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 208: Fields on the Add Static Route Page

| Field | Description |
|------------------|---|
| Routing Instance | Select the routing instance from the list. The selected destination routing instance that points to the routing table containing the tunnel destination address. NOTE: If you log in as a tenant user, routing instance is not displayed as tenant context supports only one routing instance. |
| 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. |

Table 208: Fields on the Add Static Route Page (continued)

| Field | Description |
|--------------|--|
| 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](#) | 549

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 side 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 548](#).

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

RELATED DOCUMENTATION

| [Delete Static Route](#) | 550

Delete 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 side of the Static Routing page.

A confirmation window appears.

3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

| [About the Static Routing Page](#) | 547

RIP Routing

IN THIS CHAPTER

- [About the RIP Page | 551](#)
- [Add a RIP Instance | 552](#)
- [Edit a RIP Instance | 554](#)
- [Delete RIP Instance | 555](#)
- [Edit RIP Global Settings | 555](#)
- [Delete RIP Global Settings | 558](#)

About the RIP Page

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 552](#).
- Edit a RIP instance. See [“Edit a RIP Instance” on page 554](#).
- Delete a RIP instance. See [“Delete RIP Instance” on page 555](#).
- Edit RIP global settings. See [“Edit RIP Global Settings” on page 555](#).
- Delete RIP global settings. See [“Delete RIP Global Settings” on page 558](#).

Field Descriptions

[Table 209 on page 552](#) describes the fields on the RIP page.

Table 209: 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](#) | [552](#)

Add a RIP Instance

You are here: **Network** > **Routing** > **RIP**.

To add a RIP instance:

1. Click the add icon (+) on the upper right side of the RIP page.

The Add page appears.

2. Complete the configuration according to the guidelines provided in [Table 210 on page 553](#).
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 210: Fields on the Add Page

| Field | Action |
|-------------------|---|
| General | |
| Routing Instance | Select a routing instance from the list to display only the master 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 | |
| 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. |

Table 210: Fields on the Add Page (continued)

| Field | Action |
|--|--|
| 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](#) | 554

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 side of the RIP page.

The Edit page appears with editable fields. For more information on the options, see [“Add a RIP Instance” on page 552](#).

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

RELATED DOCUMENTATION

| [Delete RIP Instance](#) | 555

Delete 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 side of the RIP page.

A confirmation window appears.

3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

| [Edit RIP Global Settings](#) | 555

Edit RIP Global Settings

You are here: **Network** > **Routing** > **RIP**.

To edit RIP global settings:

1. Click the pencil icon on the upper right side of the RIP Global Settings table.
The Edit RIP Global Settings page appears.
2. Complete the configuration according to the guidelines provided in [Table 211 on page 556](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 211: Fields on the Edit RIP Global Settings Page

| Field | Action |
|-----------------------|---|
| General | |
| Send | <p>Select a RIP send options from the list:</p> <ul style="list-style-type: none"> • Broadcast • Multicast • None • Version-1 |
| Receive | <p>Select a RIP receive options from the list:</p> <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. |
| 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. |

Table 211: Fields on the Edit RIP Global Settings Page (*continued*)

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

Table 211: Fields on the Edit RIP Global Settings Page (*continued*)

| Field | Action |
|-------|--|
| 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](#) | 558

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 side of the RIP Global settings table.
A confirmation window appears.
3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

| [About the RIP Page](#) | 551

OSPF Routing

IN THIS CHAPTER

- [About the OSPF Page | 559](#)
- [Add an OSPF | 561](#)
- [Edit an OSPF | 568](#)
- [Delete OSPF | 569](#)

About the OSPF Page

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 561](#).
- Edit an OSPF. See [“Edit an OSPF” on page 568](#).
- Delete OSPF. See [“Delete OSPF” on page 569](#).
- 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 top 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 212 on page 560 describes the fields on the OSPF page.

Table 212: 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). |
| 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](#) | 561

Add an OSPF

You are here: **Network** > **Routing** > **OSPF**.

To add an OSPF routing:

1. Click the add icon (+) on the upper right side of the OSPF page.
The Create OSPF page appears.
2. Complete the configuration according to the guidelines provided in [Table 213 on page 561](#).
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 213: Fields on the Add an OSPF Page

| Field | Action |
|----------------|--------|
| Basic Settings | |

Table 213: 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> Click OK to save changes. |
| Routing Options | |
| Router ID | Enter the ID of the routing device. |
| Traffic Engineering | Enable this option if you want the traffic to be managed or engineered. |
| NOTE: This option is not available for OSPFv3. | |
| Area Details | |

Table 213: Fields on the Add an OSPF Page (continued)

| Field | Action |
|---------|---|
| Area Id | <p>Specifies the uniquely identified area within its AS.</p> <p>Type a 32-bit numeric identifier for the area.</p> <p>Type an integer or select and edit the value.</p> <p>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.</p> |

Table 213: 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"> To add an area range form: <ol style="list-style-type: none"> Click +. The Create Area Range form page appears. Enter the following details: <ul style="list-style-type: none"> Area Range—Enter the area range address. NOTE: For OSPF, enter an IPv4 address and for OSPFv3 enter an IPv6 address. Subnet mask—Enter the subnet mask area address. NOTE: This option is available only for IPv4 address. Override metric—Select a value to override the metric for the IP address range. Range: 1025 through 65534. Select Restrict Advertisements of this area range to specify that the routes contained within a summary must not be displayed. Select Enforce exact match for advertisements of this area range to specify that the summary of a route must be advertised only when an exact match is made within the configured summary range. Click OK. To edit the selected are range: <ol style="list-style-type: none"> Select the existing area range. Click the pencil icon to edit the selected area range. The Edit Area Range form page appears with editable fields. Click OK to save the changes. To delete an area range: <ol style="list-style-type: none"> Select the area range that you want to delete. Click the delete icon. A confirmation message appears. Click Yes to delete the selected area range. |
| 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. |

Table 213: Fields on the Add an OSPF Page (*continued*)

| Field | Action |
|---|---|
| <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> |
| 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. <p>NOTE: This option is not available for OSPFv3.</p> <ul style="list-style-type: none"> • p2mp—Point-to-multipoint interface. • p2p—Point-to-point interface. • p2mp-over-lan—Point-to-multipoint over LAN mode. <p>NOTE: This option is not available for OSPF.</p> |
| Interface Metric | Type the metric that you want for measuring the interface. |

Table 213: Fields on the Add an OSPF Page (*continued*)

| Field | Action |
|---------------------------------|---|
| 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 | |
| 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 213: 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. The MD5 key values can be from 1 through 16 characters long. Characters can include ASCII strings. If you include spaces, enclose all characters in quotation marks (" "). • Start Time—MD5 start time. <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.

| | |
|---------------|--|
| 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. |
|---------------|--|

Table 213: Fields on the Add an OSPF Page (*continued*)

| Field | Action |
|----------------------|--|
| 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> |
| 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](#) | 568

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 side of the OSPF page.

The Create OSPF page appears with editable fields. For more information on the options, see [“Add an OSPF” on page 561](#).

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

RELATED DOCUMENTATION

| [Delete OSPF | 569](#)

Delete 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 side of the OSPF page.
A confirmation window appears.
3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

| [About the OSPF Page | 559](#)

BGP Routing

IN THIS CHAPTER

- [About the BGP Page | 570](#)
- [Add a BGP Group | 572](#)
- [Edit a BGP Group | 577](#)
- [Delete a BGP Group | 578](#)
- [Edit Global Information | 578](#)

About the BGP Page

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 572.](#)
- Edit a routing instance. See [“Edit a BGP Group” on page 577.](#)
- Delete a routing instance. See [“Delete a BGP Group” on page 578.](#)
- Disable group information. To do this, select an existing group information and click **Disable**.
- Edit global information. See [“Edit Global Information” on page 578.](#)
- Disable global information. To do this, select an existing global information and click **Disable**.

Field Descriptions

[Table 214 on page 571](#) describes the fields on the BGP page.

Table 214: 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: Primary 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. |
| Export Policy | Displays the export policy selected. NOTE: If you log in as a tenant user, Routing Instance, Import Policy, and Export Policy are not displayed. |

Global Information

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 | Edits the Global settings which lists the following fields. See “Edit Global Information” on page 578 . |
|------|---|

Table 214: 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. <p>NOTE: If you log in as a tenant user, Confederation is not displayed.</p> <ul style="list-style-type: none"> • Confederation Members—Specifies the AS numbers for the confederation members. <p>NOTE: If you log in as a tenant user, Confederation Members is not displayed.</p> <ul style="list-style-type: none"> • 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. <p>NOTE: If you log in as a tenant user, Import Policy is not displayed.</p> <ul style="list-style-type: none"> • Export Policy—Specifies one or more policies to routes being exported from the routing table into BGP. <p>NOTE: If you log in as a tenant user, Export Policy is not displayed.</p> |

RELATED DOCUMENTATION

| [Add a BGP Group](#) | 572

Add a BGP Group

You are here: **Network** > **Routing** > **BGP**.

To add a BGP Group:

1. Click the add icon (+) on the upper right side of the BGP Group page.

The Add a Group page appears.

2. Complete the configuration according to the guidelines provided in [Table 215 on page 573](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 215: 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. |
| Cluster Id | Enter the IPv6 or IPv4 address to be used as the cluster identifier. The cluster identifier is used by the route reflector cluster in an internal BGP group. |
| 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 215: 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"> To add a dynamic neighbor: <ol style="list-style-type: none"> Click +. The Add Dynamic Neighbor window appears. Select one of the following options in the Addresses field: <ul style="list-style-type: none"> All IPv4 IPv6 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. 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. Click OK to save changes. To edit a dynamic neighbor: <ol style="list-style-type: none"> Select the existing dynamic neighbor address. Click the pencil icon to edit the selected dynamic neighbor address. The Edit Dynamic Neighbor window appears with editable fields. Click OK to save changes. To delete a dynamic neighbor: <ol style="list-style-type: none"> Select the existing dynamic neighbor address. Click the delete icon (X) to delete the selected dynamic neighbor address. |

Table 215: Fields on the Add a Group Page *(continued)*

| Field | Action |
|------------------|--------|
| Static Neighbors | |

Table 215: Fields on the Add a Group Page (*continued*)

| Field | Action |
|-------|--|
| | <p>Configures a static neighbor (peer).</p> <p>Select one of the following options:</p> <ol style="list-style-type: none"> To add a static neighbor: <ol style="list-style-type: none"> Click +. The Add Static Neighbor window appears. 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. Range: 0 through 65,535 seconds. 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. 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. Click OK to save changes. To edit a static neighbor: <ol style="list-style-type: none"> Select the existing static neighbor address. Click the pencil icon to edit the selected static neighbor address. The Edit Static Neighbor window appears with editable fields. |

Table 215: Fields on the Add a Group Page (continued)

| Field | Action |
|---------------------|--|
| | <p>c. Click OK to save changes.</p> <p>3. To delete a static neighbor:</p> <p>a. Select the existing static neighbor address.</p> <p>b. Click the delete icon (X) to delete the selected static neighbor address.</p> |
| Policies Tab | |
| 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](#) | 577

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 side 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 572](#).

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

RELATED DOCUMENTATION

| [Delete a BGP Group | 578](#)

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 side of the BGP page.

A confirmation window appears.

3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

| [Edit Global Information | 578](#)

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 side of the Global Information table.

The Edit Global Settings page appears.

- 3. Complete the configuration according to the guidelines provided in [Table 216 on page 579](#).
- 4. Click **OK** to save the changes.

Table 216: 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 216: 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"> To add a member ASN: <ol style="list-style-type: none"> Click +. The Confederation Members window appears. Enter member ASN value in the Member ASN field. Click OK to save changes. To edit a member ASN: <ol style="list-style-type: none"> Select an existing member ASN value and click the pencil icon. The Confederation Members window appears. Edit member ASN value in the Member ASN field. Click OK to save changes. To delete a member ASN: <ol style="list-style-type: none"> Select an existing member ASN value. The Confederation Members window appears. 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 | Select the check box to enable MTU discovery. |
| 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. |

Table 216: Fields on the Edit Global Settings Page (*continued*)

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

| | |
|---------------|---|
| 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 216: 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](#) | 570

Routing Instances

IN THIS CHAPTER

- [About the Routing Instances Page | 583](#)
- [Add a Routing Instance | 584](#)
- [Edit a Routing Instance | 585](#)
- [Delete Routing Instance | 586](#)

About the Routing Instances Page

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 584](#).
- Edit a routing instance. See [“Edit a Routing Instance” on page 585](#).
- Delete a routing instance. See [“Delete Routing Instance” on page 586](#).
- Show or hide columns in the Routing Instance table. To do this, use the Show Hide Columns icon in the top right corner of the page and select the options you want to show or deselect to hide options on the page.
- 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 217 on page 584 describes the fields on the Routing Instances page.

Table 217: 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](#) | 584.

Add a Routing Instance

You are here: **Network > Routing > Routing Instances.**

To add a routing interface:

- 1. Click the add icon (+) available on the upper right side of the Routing Instances page.
The Create Routing Instance page appears.

2. Complete the configuration according to the guidelines provided in [Table 218 on page 585](#).
 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 218: 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 | <p>Select the type of routing instance from the list:</p> <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 | <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 | 583](#)
- [Edit a Routing Instance | 585](#)

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 side 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 584](#).

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

RELATED DOCUMENTATION

[About the Routing Instances Page | 583](#)

[Delete Routing Instance | 586](#)

Delete 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 side of the page.
A confirmation window appears.
3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

[About the Routing Instances Page | 583](#)

[Add a Routing Instance | 584](#)

[Edit a Routing Instance | 585](#)

Routing—Policies

IN THIS CHAPTER

- [About the Policies Page | 587](#)
- [Global Options | 588](#)
- [Add a Policy | 590](#)
- [Clone a Policy | 598](#)
- [Edit a Policy | 599](#)
- [Delete Policy | 599](#)
- [Test a Policy | 600](#)

About the Policies Page

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 588](#).
- Create a policy. See [“Add a Policy” on page 590](#).
- Clone a policy. See [“Clone a Policy” on page 598](#).
- Edit a policy. See [“Edit a Policy” on page 599](#).
- Delete a policy. See [“Delete Policy” on page 599](#).
- 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 600](#).

Field Descriptions

Table 219 on page 588 describes the fields on the Policies page.

Table 219: 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](#) | 588

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 side of the page.

The Edit Global Options page appears. You can modify any previous changes done. For more information on the options, see [Table 220 on page 589](#).

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

Table 220: 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 +. The Add Prefix List Members page appears. 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> |
| 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> |

Table 220: Fields on the Global Options Page (*continued*)

| Field | Action |
|---------|--|
| Members | Click + to add a BGP community member. Community ID—Enter the BGP community ID. |

RELATED DOCUMENTATION

| [Add a Policy](#) | [590](#).

Add a Policy

You are here: **Network** > **Routing** > **Policies**.

To add a policy:

1. Click + > **New** on the right side of the Policies page.
The Add Policy page appears.
2. Complete the configuration according to the guidelines provided in [Table 221 on page 590](#).
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 221: 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. |

Table 221: Fields on the Policy Page (*continued*)

| Field | Description |
|------------------|--|
| 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. |
| 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"> To add an interface <ol style="list-style-type: none"> Click + and select Interface. The Available Interfaces page appears. Select an interface from the list and click OK. The selected interface is added. To add an IP address <ol style="list-style-type: none"> Click + and select Address. The Add IP Address page appears. Enter IP address from the list and click OK. The selected IP address is added. To delete an interface or an IP address: <ol style="list-style-type: none"> Select an existing interface or address from Interfaces. Click X. The selected interface or IP address is deleted. |

Table 221: 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"> To add a prefix list: <ol style="list-style-type: none"> Click +. The Available Prefix List page appears. Select a prefix list from the list and click OK. The selected prefix list is added. To delete a prefix list: <ol style="list-style-type: none"> Select an existing prefix list. 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"> To add a protocol: <ol style="list-style-type: none"> Click +. The Available Protocols page appears. Select a protocol from the list and click OK. The selected protocol is added. To delete a protocol: <ol style="list-style-type: none"> Select an existing protocol. Click X. The selected protocol is deleted. |

Table 221: 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"> To add a policy: <ol style="list-style-type: none"> Click +. The Available Policies page appears. Select a policy from the list and click OK. The selected policy is added. To delete a policy: <ol style="list-style-type: none"> Select an existing policy. 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 221: 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"> To add an As path: <ol style="list-style-type: none"> Click +. The Available AS Paths page appears. Select an As path from the list and click OK. The selected As path is added. To delete an As path: <ol style="list-style-type: none"> Select an existing As path. Click X. The selected As path is deleted. |
| 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. |
| 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"> To add a community: <ol style="list-style-type: none"> Click +. The Available Communities page appears. Select a community from the list and click OK. The selected community is added. To delete a community: <ol style="list-style-type: none"> Select an existing community. Click X. The selected community is deleted. |
| 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. |

Table 221: Fields on the Policy Page (*continued*)

| Field | Description |
|------------|--|
| Preference | Type a preference value for the route. |
| Metric | Type a metric value. |
| 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"> To add an interface: <ol style="list-style-type: none"> Click + and select Interface. The Available Interfaces page appears. Select an interface from the list and click OK. The selected interface is added. To add an IP address: <ol style="list-style-type: none"> Click + and select Address. The Add IP Address page appears. Enter IP address from the list and click OK. The selected IP address is added. To delete an interface or an IP address: <ol style="list-style-type: none"> Select an existing interface or address from Interfaces. Click X. The selected interface or IP address 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"> To add a protocol: <ol style="list-style-type: none"> Click +. The Available Protocols page appears. Select a protocol from the list and click OK. The selected protocol is added. To delete a protocol: <ol style="list-style-type: none"> Select an existing protocol. Click X. The selected protocol is deleted. |

Table 221: Fields on the Policy Page (*continued*)

| Field | Description |
|----------------|--|
| Policy | <p>Displays the name of the policy.</p> <p>Choose one of the following options:</p> <ol style="list-style-type: none"> To add a policy: <ol style="list-style-type: none"> Click +. The Available Policies page appears. Select a policy from the list and click OK. The selected policy is added. To delete a policy: <ol style="list-style-type: none"> Select an existing policy. 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> |
| 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> |

Table 221: Fields on the Policy Page (*continued*)

| Field | Description |
|-------------------------|--|
| 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> |
| 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 221: 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. Specifies the tag value. The tag action sets the 32-bit tag field in OSPF external link-state advertisement (LSA) packets. • 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. Specifies the class-of-service parameters to be applied to routes installed into the routing table. • Source Class—Enter the source class. Specifies that the value entered here maintains the packet counts for a route passing through your network, based on the source address. • Destination Class—Enter the destination class. Specifies the value entered here maintains packet counts for a route passing through your network, based on the destination address in the packet. • Forwarding Class—Enter the forwarding class. Specifies that the value of queue number entered here maintains packet counts for a route passing through your network, based on the internal queue number assigned in the packet. |

RELATED DOCUMENTATION

| [Clone a Policy](#) | 598

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 590](#).

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

RELATED DOCUMENTATION

| [Edit a Policy](#) | 599

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 side of the Policies page.

The Edit Policy page appears with editable fields. For more information on the options, see [“Add a Policy” on page 590](#).

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

RELATED DOCUMENTATION

| [Delete Policy](#) | 599.

Delete 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 side of the Policies page.

A confirmation window appears.

- 3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

| [Test a Policy](#) | [600](#).

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 side 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](#) | [590](#).

| [Edit a Policy](#) | [599](#).

| [Delete Policy](#) | [599](#).

Routing—Forwarding Mode

IN THIS CHAPTER

- About the Forwarding Mode Page | 601

About the Forwarding Mode Page

You are here: **Network** > **Routing** > **Forwarding Mode**.

Use this page to view the forwarding configuration details.

Field Descriptions

Table 222 on page 601 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 222: 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">Nonedrop—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> |

Table 222: Fields on the Forwarding Mode Page (*continued*)

| Field | Description |
|--|--|
| Family ISO | Supports IS-IS traffic. |
| NOTE: This option is not available for SRX5000 line of devices. | Select an option from the list: <ul style="list-style-type: none"> • None • packet-based |
| Family MPLS | Supports MPLS traffic. |
| NOTE: This option is not available for SRX5000 line of devices. | Select an option from the list: <ul style="list-style-type: none"> • None • flow-based • packet-based |

CoS—Value Aliases

IN THIS CHAPTER

- [About the Value Aliases Page | 603](#)
- [Add a Code Point Alias | 604](#)
- [Edit a Code Point Alias | 605](#)
- [Delete Code Point Alias | 605](#)

About the Value Aliases Page

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 604.](#)
- Edit a code point alias. See [“Edit a Code Point Alias” on page 605.](#)
- Delete a code point alias. See [“Delete Code Point Alias” on page 605.](#)

Field Descriptions

[Table 223 on page 603](#) describes the fields on the Value Alias page.

Table 223: Fields on the Value Alias Page

| Field | Description |
|------------|---|
| Alias name | Displays the name given to CoS values. For example, af11 or be. |

Table 223: Fields on the Value Alias Page (*continued*)

| Field | Description |
|----------------|--|
| 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](#) | 604.

Add a Code Point Alias

You are here: **Network** > **Class of Service(CoS)** > **Value Aliases**.

To add a code point alias:

1. Click the add icon (+) available on the right side of the Value Aliases page.

The Add Code Point Alias page appears.

2. Complete the configuration according to the guidelines provided in [Table 224 on page 605](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 224: 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](#) | 605.

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 side 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 604](#).

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

RELATED DOCUMENTATION

[Delete Code Point Alias](#) | 605.

Delete 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 side of the Value Aliases page.
A confirmation window appears.
3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

| [About the Value Aliases Page](#) | 603.

CoS—Forwarding Classes

IN THIS CHAPTER

- [About the Forwarding Classes Page | 607](#)
- [Add a Forwarding Class | 608](#)
- [Edit a Forwarding Class | 609](#)
- [Delete Forwarding Class | 609](#)

About the Forwarding Classes Page

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 608.](#)
- Edit a forwarding class. See [“Edit a Forwarding Class” on page 609.](#)
- Delete forwarding class. See [“Delete Forwarding Class” on page 609.](#)

Field Descriptions

[Table 225 on page 607](#) describes the fields on the Forwarding Classes page.

Table 225: 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). |

Table 225: Fields on the Forwarding Classes Page (*continued*)

| Field | Description |
|-----------------------|--|
| 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](#) | 608.

Add a Forwarding Class

You are here: **Network** > **Class of Service(CoS)** > **Forwarding Classes**.

To add a forwarding class:

1. Click the add icon (+) available on the right side of the Forwarding Class page.
The Add Forwarding Class page appears.
2. Complete the configuration according to the guidelines provided in [Table 226 on page 608](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 226: 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](#) | 609.

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 side 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 608](#) for options available for editing.

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

RELATED DOCUMENTATION

| [Delete Forwarding Class](#) | 609.

Delete 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 side of the Forwarding Classes page.

A confirmation window appears.

3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

| [About the Forwarding Classes Page](#) | 607.

CoS Classifiers

IN THIS CHAPTER

- [About the Classifiers Page | 610](#)
- [Add a Classifier | 611](#)
- [Edit a Classifier | 613](#)
- [Delete Classifier | 613](#)

About the Classifiers Page

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 611](#).
- Edit a classifier. See [“Edit a Classifier” on page 613](#).
- Delete classifier. See [“Delete Classifier” on page 613](#).

Field Descriptions

[Table 227 on page 610](#) describes the fields on the Classifiers page.

Table 227: Fields on the Classifiers Page

| Field | Description |
|-----------------|------------------------------------|
| Classifier name | Displays the name of a classifier. |

Table 227: Fields on the Classifiers Page (*continued*)

| Field | Description |
|-------------------------------|---|
| 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). <p>NOTE: This option is not available on SRX4000 lines of devices.</p> <ul style="list-style-type: none"> • exp—MPLS experimental (EXP) bits classifier <p>NOTE: This option is not available on SRX4000 lines of devices and SRX5000 lines of devices.</p> <ul style="list-style-type: none"> • ieee-802.1—IEEE-802.1 classifier • ieee-802.1ad—IEEE-802.1ad classifier <p>NOTE: This option is not available on SRX4000 lines of devices.</p> <ul style="list-style-type: none"> • 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](#) | **611**.

Add a Classifier

You are here: **Network** > **Class of Service(CoS)** > **Classifiers**.

To add a classifier:

1. Click the add icon (+) available on the right side of the Classifiers page.

The Add Classifier page appears.

2. Complete the configuration according to the guidelines provided in [Table 228 on page 612](#).

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

Table 228: 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). <p>NOTE: This option is not available on SRX4000 lines of devices.</p> <ul style="list-style-type: none"> • exp—MPLS experimental (EXP) bits classifier <p>NOTE: This option is not available on SRX4000 lines of devices and SRX5000 lines of devices.</p> <ul style="list-style-type: none"> • ieee-802.1—IEEE-802.1 classifier • ieee-802.1ad—IEEE-802.1ad classifier <p>NOTE: This option is not available on SRX4000 lines of devices.</p> <ul style="list-style-type: none"> • inet-precedence—IPv4 precedence classifier (default and compatibility) |
| 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](#) | 613.

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 side of the Classifiers page.

The Edit Classifiers page appears with editable fields. For more information on the options, see [“Add a Classifier” on page 611](#).

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

RELATED DOCUMENTATION

| [Delete Classifier](#) | 613.

Delete 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 side of the Classifiers page.

A confirmation window appears.

3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

CoS—Rewrite Rules

IN THIS CHAPTER

- [About the Rewrite Rules Page | 615](#)
- [Add a Rewrite Rule | 616](#)
- [Edit a Rewrite Rule | 618](#)
- [Delete Rewrite Rule | 618](#)

About the Rewrite Rules Page

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 616.](#)
- Edit a rewrite rule. See [“Edit a Rewrite Rule” on page 618.](#)
- Delete rewrite rule. See [“Delete Rewrite Rule” on page 618.](#)

Field Descriptions

[Table 229 on page 615](#) describes the fields on the Rewrite Rules page.

Table 229: 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. |

Table 229: Fields on the Rewrite Rules Page *(continued)*

| Field | Description |
|----------------------------|---|
| 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](#) | 616.

Add a Rewrite Rule

You are here: **Network** > **Class of Service(CoS)** > **Rewrite Rules**.

To add a rule configuration:

1. Click the add icon (+) available on the right side of the Forwarding Class page.
The Add Rewrite Rule page appears.
2. Complete the configuration according to the guidelines provided in [Table 230 on page 616](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 230: Fields on the Add Rewrite Rule Page

| Field | Action |
|-------------------|---|
| Rewrite rule name | Enter the name of a defined rewrite rule. |

Table 230: Fields on the Add Rewrite Rule Page (*continued*)

| Field | Action |
|----------------------------|---|
| 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. |
| 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](#) | [618](#).

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 side 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 616](#).

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

RELATED DOCUMENTATION

| [Delete Rewrite Rule](#) | [618](#).

Delete 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 side 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](#) | [615](#).

CoS—Schedulers

IN THIS CHAPTER

- [About the Schedulers Page | 619](#)
- [Add a Scheduler | 620](#)
- [Edit a Scheduler | 622](#)
- [Delete Scheduler | 622](#)

About the Schedulers Page

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 620.](#)
- Edit a scheduler. See [“Edit a Scheduler” on page 622.](#)
- Delete scheduler. See [“Delete Scheduler” on page 622.](#)

Field Descriptions

[Table 231 on page 619](#) describes the fields on the Schedulers page.

Table 231: Fields on the Schedulers Page

| Field | Description |
|----------------------------------|---|
| Schedulers Global Setting | |
| Enable Non Strict Priority | Applies non-strict priority policy to all the schedulers. |

Table 231: Fields on the Schedulers Page (*continued*)

| Field | Description |
|---------------------------------|--|
| 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](#) | 620

Add a Scheduler

You are here: **Network** > **Class of Service(CoS)** > **Schedulers**.

To add a scheduler:

1. Click the add icon (+) available on the right side of the Scheduler page.
The Add Scheduler page appears.
2. Complete the configuration according to the guidelines provided in [Table 232 on page 620](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 232: Fields on the Add Scheduler Page

| Field | Action |
|----------------|---------------------------|
| Scheduler name | Enter the scheduler name. |

Table 232: Fields on the Add Scheduler Page (*continued*)

| Field | Action |
|--------------------|--|
| 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. |
| 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](#) | [622](#).

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 side of the Schedulers page.

The Edit Scheduler appears with editable fields. For more information on the options, see [“Add a Scheduler” on page 620](#).

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

RELATED DOCUMENTATION

| [Delete Scheduler](#) | [622](#).

Delete 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 side of the Schedulers page.

A confirmation window appears.

3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

| [About the Schedulers Page](#) | [619](#).

CoS—Scheduler Maps

IN THIS CHAPTER

- [About the Scheduler Maps Page | 623](#)
- [Add a Scheduler Map | 624](#)
- [Edit a Scheduler Map | 625](#)
- [Delete Scheduler Map | 626](#)

About the Scheduler Maps Page

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 624.](#)
- Edit a scheduler map. See [“Edit a Scheduler Map” on page 625.](#)
- Delete a scheduler map. See [“Delete Scheduler Map” on page 626.](#)

Field Descriptions

[Table 233 on page 623](#) describes the fields on the Scheduler Maps page.

Table 233: 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. |

Table 233: Fields on the Scheduler Maps Page (*continued*)

| Field | Description |
|------------------------------|--|
| 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](#) | [624](#).

Add a Scheduler Map

You are here: **Network** > **Class of Service(CoS)** > **Scheduler Maps**.

To add a scheduler map:

1. Click the add icon (+) available on the right side of the Scheduler Map page.
The Add Scheduler Map page appears.
2. Complete the configuration according to the guidelines provided in [Table 234 on page 624](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 234: 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. |

Table 234: Fields on the Add Scheduler Map Page (*continued*)

| Field | Action |
|----------------------|--|
| 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](#) | 625.

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 side 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 624](#).

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

RELATED DOCUMENTATION

[Delete Scheduler Map](#) | 626.

Delete 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 side of the Schedulers page.
A confirmation window appears.
3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

[About the Scheduler Maps Page](#) | 623.

CoS—Drop Profile

IN THIS CHAPTER

- [About the Drop Profile Page | 627](#)
- [Add a Drop Profile | 628](#)
- [Edit a Drop Profile | 629](#)
- [Delete Drop Profile | 630](#)

About the Drop Profile Page

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 628.](#)
- Edit a drop profile. See [“Edit a Drop Profile” on page 629.](#)
- Delete a drop profile. See [“Delete Drop Profile” on page 630.](#)

Field Descriptions

[Table 235 on page 627](#) describes the fields on the Drop Profile page.

Table 235: 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. |

Table 235: Fields on the Drop Profile Page *(continued)*

| Field | Description |
|-------------|--|
| Data points | Displays information about the data point types. |

RELATED DOCUMENTATION

| [About the Drop Profile Page](#) | 627.

Add a Drop Profile

You are here: **Network** > **Class of Service(CoS)** > **Drop Profile**.

To add a drop profile:

1. Click the add icon (+) available on the right side of the Drop Profile page.
The Add Drop Profile page appears.
2. Complete the configuration according to the guidelines provided in [Table 236 on page 628](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 236: Fields on the Add Drop Profile Page

| Field | Action |
|-------------------|--|
| Drop Profile Name | Enter a drop profile name. |
| 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. |

Table 236: Fields on the Add Drop Profile Page *(continued)*

| Field | Action |
|------------|---|
| Data point | <p>To add a data point:</p> <ol style="list-style-type: none"> 1. Click +. The Add Data Point page appears. 2. 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. 3. Click OK to save changes. <p>To edit a data point:</p> <ol style="list-style-type: none"> 1. Select the existing data point and click the pencil icon. The Edit Data Point page appears. 2. Enter a percentage value for Drop Probability. 3. 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](#) | 629.

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 side 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 628](#).

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

RELATED DOCUMENTATION

| [Delete Drop Profile | 630](#).

Delete 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 side of the Drop Profile page.

A confirmation window appears.

3. Click **Yes** to delete or click **No**.

RELATED DOCUMENTATION

| [About the Drop Profile Page | 627](#).

CoS—Virtual Channel Groups

IN THIS CHAPTER

- [About the Virtual Channel Groups Page | 631](#)
- [Add a Virtual Channel | 632](#)
- [Edit a Virtual Channel | 633](#)
- [Delete Virtual Channel | 634](#)

About the Virtual Channel Groups Page

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 632](#).
- Edit a virtual channel. See [“Edit a Virtual Channel” on page 633](#).
- Delete a virtual channel. See [“Delete Virtual Channel” on page 634](#).

Field Descriptions

[Table 237 on page 632](#) describes the fields on the Virtual Channel Groups page.

Table 237: 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](#) | 632.

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 238 on page 632](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 238: 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. |

Table 238: Fields on the Virtual Channel Information Page (*continued*)

| Field | Action |
|---------------|---|
| Scheduler Map | <p>Select a scheduler map from the list.</p> <p>Specifies a predefined scheduler map to assign to a virtual channel. The scheduler maps associate schedulers with forwarding classes.</p> |
| Shaping Rate | <p>Enter the shaping rate for a virtual channel.</p> <p>Configuring a shaping rate is optional. If no shaping rate is configured, a virtual channel without a shaper can use the full logical interface bandwidth. The options available are:</p> <p>Select an option from the list:</p> <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](#) | 633.

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 632](#).
2. Click **OK** to save the changes.

RELATED DOCUMENTATION

[Delete Virtual Channel](#) | 634.

Delete 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](#) | 631.

CoS—Assign To Interface

IN THIS CHAPTER

- [About the Assign To Interface Page | 635](#)
- [Edit a Port | 636](#)
- [Add a Logical Interface | 637](#)
- [Edit a Logical Interface | 639](#)
- [Delete Logical Interface | 639](#)

About the Assign To Interface Page

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 636](#).
- Add a Logical Interface. See [“Add a Logical Interface” on page 637](#).
- Edit a Logical Interface. See [“Edit a Logical Interface” on page 639](#).
- Delete Logical Interface. See [“Delete Logical Interface” on page 639](#).

Field Descriptions

[Table 239 on page 635](#) describes the fields on the Assign To Interface page.

Table 239: Fields on the Assign To Interface Page

| Field | Description |
|-------|---------------------------------------|
| Port | Displays the port and interface name. |

Table 239: Fields on the Assign To Interface Page (*continued*)

| Field | Description |
|--------------------------------------|---|
| 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](#) | 636

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 240 on page 637](#).
3. Click **OK** to save the changes.

Table 240: 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](#) | 637

Add a Logical Interface

You are here: **Network > Class of Service(CoS) > Assign To Interface**.

To add a logical interface:

1. Click the add icon (+) available on the right side of the Logical Interface page.
The Add Logical Interface page appears.
2. Complete the configuration according to the guidelines provided in [Table 241 on page 637](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 241: 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. |

Table 241: Fields on the Add Logical Interface (*continued*)

| Field | Action |
|-----------------------|---|
| Virtual channel group | Select a virtual channel group from the list. |
| Classifiers | |
| dscp | <p>Select a classifier DSCP value from the list.</p> <p>Specifies the Differentiated Services Code Point of the classifier type assigned to a particular interface.</p> |
| dscp v6 | <p>Select a classifier DSCPv6 value from the list.</p> <p>Specifies the Differentiated Services Code Point version 6 of the classifier type assigned to a particular interface.</p> |
| exp | <p>Select an EXP classifier value from the list.</p> <p>Specifies the EXP classifier type assigned to a particular interface.</p> |
| inet precedence | <p>Select an IPv4 precedence classifier value from the list.</p> <p>Specifies the IPv4 precedence classifier type assigned to a particular interface.</p> |
| Rewrite rules | |
| dscp | <p>Select a rewrite rule DSCP value from the list.</p> <p>Specifies the Differentiated Services Code Point of the rewrite rule type assigned to a particular interface</p> |
| dscp v6 | <p>Select a rewrite rule DSCPv6 value from the list.</p> <p>Specifies the Differentiated Services Code Point version 6 of the rewrite rule type assigned to a particular interface.</p> |
| exp | <p>Select an EXP rewrite rule value from the list.</p> <p>Specifies the EXP rewrite rule type assigned to a particular interface.</p> |
| inet precedence | <p>Select an IPv4 precedence rewrite rule value from the list.</p> <p>Specifies the IPv4 precedence rewrite rule type assigned to a particular interface.</p> |

RELATED DOCUMENTATION

| [Edit a Logical Interface](#) | 639.

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 side 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 637](#).

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

RELATED DOCUMENTATION

| [Delete Logical Interface](#) | 639.

Delete 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 side 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](#) | 635.

Application QoS

IN THIS CHAPTER

- [About the Application QoS Page | 641](#)
- [Add an Application QoS Profile | 643](#)
- [Edit an Application QoS Profile | 645](#)
- [Clone an Application QoS Profile | 646](#)
- [Delete Application QoS Profile | 646](#)
- [Add a Rate Limiter Profile | 647](#)
- [Edit a Rate Limiter Profile | 648](#)
- [Clone a Rate Limiter Profile | 649](#)
- [Delete Rate Limiter Profile | 649](#)

About the Application QoS Page

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 643](#).
- Edit an AppQoS profile. See [“Edit an Application QoS Profile” on page 645](#).
- Clone an AppQoS profile. See [“Clone an Application QoS Profile” on page 646](#).

- Delete AppQoS profile. See [“Delete Application QoS Profile” on page 646](#).
- Add a rate limiter profile. See [“Add a Rate Limiter Profile” on page 647](#).
- Edit a rate limiter profile. See [“Edit a Rate Limiter Profile” on page 648](#).
- Clone a rate limiter profile. See [“Clone a Rate Limiter Profile” on page 649](#).
- Delete rate limiter profile. See [“Delete Rate Limiter Profile” on page 649](#).
- Show or hide columns in the AppQoS Profile or Rate Limiter Profile table. To do this, click Show Hide Columns icon in the top 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 242 on page 642](#) describes the fields on the Application QoS page.

Table 242: Fields on the Application QoS Page

| Field | Description |
|-----------------------|-----------------------------------|
| AppQoS Profile | |
| Name | Displays the AppQoS profile name. |

Table 242: Fields on the Application QoS Page (*continued*)

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

RELATED DOCUMENTATION

[Add an Application QoS Profile | 643](#)
[Add a Rate Limiter Profile | 647](#)

Add an Application QoS Profile

You are here: **Network** > **Application QoS**.

To add an AppQoS profile:

1. Click the add icon (+) on the upper right side of the Application QoS page.

The Add AppQoS Profile page appears.

2. Complete the configuration according to the guidelines provided in [Table 243 on page 644](#) through [Table 244 on page 645](#).

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

Table 243: 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 | <p>Select a rate limiter from the list to be associated with client-to-server traffic for this application.</p> <p>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 647.</p> |
| Server to Client | <p>Select a rate limiter from the list to be associated with server-to-client traffic for this application.</p> <p>Click Add New to add a new rate limiter profile. For fields information, see “Add a Rate Limiter Profile” on page 647.</p> |
| 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 244 on page 645.</p> <p>NOTE: Add New is not supported for the logical systems and tenants. You can only select the predefined value.</p> |

Table 243: Fields on the Add AppQoS Profile Page (*continued*)

| Field | Action |
|----------------------|--|
| Packet Loss Priority | Select an option from the list to mark loss priority with matching applications. 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. |
| Logs | Enable this option to log AppQoS events. |

Table 244: Fields on the Add Forwarding Class page

| Field | Action |
|--------------|---|
| Name | Enter a name for the forwarding class. |
| Queue Number | Enter an output queue number to associate with the forwarding class. Range is 0 through 7. |
| Priority | Select the forwarding class queuing priority from the list. |

RELATED DOCUMENTATION

[About the Application QoS Page | 641](#)
[Edit an Application QoS Profile | 645](#)
[Clone an Application QoS Profile | 646](#)
[Delete Application QoS Profile | 646](#)

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 643](#).

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

RELATED DOCUMENTATION

[About the Application QoS Page | 641](#)

[Clone an Application QoS Profile | 646](#)

[Delete Application QoS Profile | 646](#)

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 643](#).

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

RELATED DOCUMENTATION

[About the Application QoS Page | 641](#)

[Edit an Application QoS Profile | 645](#)

[Delete Application QoS Profile | 646](#)

Delete Application QoS Profile

You are here: **Network** > **Application QoS**.

To delete AppQoS profiles:

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 side 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 641 |
| Add an Application QoS Profile 643 |
| Edit an Application QoS Profile 645 |
| Clone an Application QoS Profile 646 |

Add a Rate Limiter Profile

You are here: **Network > Application QoS.**

To add a rate limiter profile:

- 1. Click the add icon (+) on the upper right side of the Application QoS page.
The Add Rate Limiter Profile page appears.
- 2. Complete the configuration according to the guidelines provided in [Table 245 on page 647](#).
- 3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 245: 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> |

Table 245: Fields on the Add Rate Limiter Profile Page (*continued*)

| Field | Action |
|--------------------|--|
| 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 | 641](#)
[Edit a Rate Limiter Profile | 648](#)
[Clone a Rate Limiter Profile | 649](#)
[Delete Rate Limiter Profile | 649](#)

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 647](#).

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

RELATED DOCUMENTATION

[About the Application QoS Page | 641](#)
[Clone a Rate Limiter Profile | 649](#)
[Delete Rate Limiter Profile | 649](#)

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 647](#).

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

RELATED DOCUMENTATION

[About the Application QoS Page | 641](#)

[Edit a Rate Limiter Profile | 648](#)

[Delete Rate Limiter Profile | 649](#)

Delete Rate Limiter Profile

You are here: **Network** > **Application QoS**.

To delete rate limiter profiles:

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 side 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 | 641](#)

[Add a Rate Limiter Profile | 647](#)

[Edit a Rate Limiter Profile | 648](#)

| [Clone a Rate Limiter Profile](#) | 649



Security Policies and Objects

Security Policies | **652**

Zones/Screens | **673**

Zone Addresses | **687**

Global Addresses | **693**

Services | **698**

Dynamic Applications | **706**

Application Tracking | **720**

Schedules | **722**

Proxy Profiles | **728**

Security Policies

IN THIS CHAPTER

- [About the Security Policies Page | 652](#)
- [Global Options | 657](#)
- [Add a Rule | 659](#)
- [Clone a Rule | 671](#)
- [Edit a Rule | 671](#)
- [Delete Rules | 672](#)

About the Security Policies Page

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 657](#).
- Add a Rule. See [“Add a Rule” on page 659](#).
- Edit a Rule. See [“Edit a Rule” on page 671](#).
- Clone a Rule. See [“Clone a Rule” on page 671](#).
- Delete a Rule. See [“Delete Rules” on page 672](#).

- 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:

a. 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

b. 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*.

c. 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 top 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 246 on page 654](#) describes few more options on Rules.

Table 246: 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. |

Table 246: More Options on the Security Policies Page (*continued*)

| Field | Description |
|-------------------|--|
| 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 | Clones or copies the selected firewall policy configuration and enables you to update the details of the rule. |
| Clear All | Clears the selection of those rules that are selected. |

Field Descriptions

Table 247 on page 655 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 247: 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. |

Table 247: Fields on the Security Policies Page (*continued*)

| Field | Description |
|---------------------|---|
| 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. |
| 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](#) | 657.

Global Options

You are here: **Security Policies & Objects > Security Policies.**

To add global options:

1. Click **Global Options** available on the upper right side of the Security Policies page.
The Global Options page appears.
2. Complete the configuration according to the guidelines provided in [Table 248 on page 657](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

[Table 248 on page 657](#) describes the fields on the Global Options page.

Table 248: 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 others 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> |

Table 248: Fields on the Global Options Page (*continued*)

| Field | Action |
|--|--|
| 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 device 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. | |
| Early Ageout | <p>Enter a value from 1 through 65,535 seconds. The default value is 20 seconds.</p> <p>Specifies the amount of time before the device aggressively ages out a session from its session table.</p> |
| Low watermark | <p>Enter a value from 0 through 100 percent. The default value is 100 percent.</p> <p>Specifies the percentage of session table capacity at which the aggressive aging-out process ends.</p> |
| High watermark | <p>Enter a value from 0 through 100 percent. The default value is 100 percent.</p> <p>Specifies the percentage of session table capacity at which the aggressive aging-out process begins.</p> |
| SYN Flood Protection | |
| SYN Flood Protection | Enable this option to defend against SYN attacks. |
| Mode | <p>Select one of the following options:</p> <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. |

Table 248: Fields on the Global Options Page (*continued*)

| Field | Action |
|-----------------------------------|---|
| 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. |
| 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](#) | 659.

Add a Rule

You are here: **Security Policies & Objects** > **Security Policies**.

NOTE: To reference UTM policies and AppQoS profiles in a security policy rules, you can create them before creating or editing security policy rules if required. To create UTM policies, go to **Security Services** > **UTM** > **UTM Policies** and to create AppQoS profiles, go to **Network** > **Application QoS**.

To add a rule:

1. Click the add icon (+) on the upper right side of the Security Policies page.
The inline editable fields will appear.
2. Complete the configuration according to the guidelines provided in [Table 249 on page 660](#).
3. Click the tick icon on the right-side of the row once done with the configuration.

NOTE: Scroll back the horizontal bar if the inline tick and 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 249: 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 249: 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. To select a specific address, 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 the selected address from the list. To create a new address, click +. The Create Address page appears. For more information on fields, see Table 250 on page 666.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 new source identity, click +. Enter a new username or identity in the Create Source Identity page and click OK. |

Table 249: 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. To select a specific address, 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 the selected address from the list. To create a new address, click +. For more information on fields, see Table 250 on page 666. NOTE: Dynamic Applications—Select Any, Specific, or None. NOTE: The Dynamic Applications option is not supported for tenants. 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. NOTE: The select all check box is only available when you search for specific dynamic applications. To create a new application, click +. The Create Application Signature page appears. For more information on fields, see “Add Application Signatures” on page 711. NOTE: For logical systems, you cannot create a new dynamic application inline. Services—Select Any, Specific, or None. 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. To create a new service, click +. The Create Service page appears. For more information on fields, see Table 251 on page 667. URL Category—Select any, Specific, or None to match criteria for web filtering category. 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. NOTE: This option is not available for logical systems and tenants. |

Table 249: Fields on the Security Policies Page (*continued*)

| Field | Action |
|--------|---|
| Action | <p>Select an option to specify the action to be taken 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. |

Advanced Security

Click +. The Select Advanced Security page appears.

NOTE:

- When the action is Reject:
 - 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 will not be supported for logical systems and tenants.
- When the action is Permit:
 - For logical systems, only IPS, IPS policy, UTM, threat prevention policy, and ICAP redirect profile and AppQOS options are supported.
 - For tenant systems, only threat prevention policy and AppQOS are supported.

| | |
|------------|--|
| IPS | <p>Select Off or On from the list. If you select On, the IPS Policy field will be disabled.</p> <p>NOTE: If IPS policy is already configured for rules, ensure you do not select On for IPS. If you select the IPS as On, the commit will fail.</p> |
| IPS Policy | <p>Select the IPS policy from the list.</p> <p>NOTE: If IPS is On and the IPS policy is not already configured for rules, ensure you do not select for IPS policy from the list. If you select the IPS policy from the list, the commit will fail.</p> |
| UTM | <p>Select the UTM policy you want to associate with this rule from the list. The list displays all the UTM policies available.</p> <p>If you want to create a new UTM policy, click Add New. The Create UTM Policies page appears. For more information on creating a new UTM policy, see “Add a UTM Policy” on page 793.</p> |
| SSL Proxy | <p>Select the SSL proxy policy to associate with this rule from the list.</p> |

Table 249: Fields on the Security Policies Page (*continued*)

| Field | Action |
|--------------------------|---|
| 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 will not be 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 will not be supported.</p> |
| 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. |
| 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 643.</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. |
| 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> |

Authentication

NOTE:

- If you select Dynamic applications in the destination, Authentication option will not be supported.
- This option is not supported for logical systems and tenant systems.

Table 249: Fields on the Security Policies Page (*continued*)

| Field | Action |
|-------------------------|---|
| Push Auth Entry to JIMS | 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 device to query JIMS to get IP/user mapping and device information. |
| Type | Select the firewall authentication type from the list. The options available are: None, Pass-through, User-firewall, and Web-authentication. |
| Access Profile | Select an access profile from the list. NOTE: This option is not supported if you select the authentication type as Web-authentication. |
| Client Name | Enter the client username or client user group name. NOTE: This option is not supported if you select the authentication type as User-firewall. |
| Domain | Select a domain name that must be in a client name from the list. NOTE: This option is supported only if you select the authentication type as User-firewall. |
| Web Redirect | 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. NOTE: This option is not supported if you select the authentication type as Web-authentication. |
| Web Redirect Https | Enable this option to redirect unauthenticated HTTP requests to the internal HTTPS webserver of the device. NOTE: This option is not supported if you select the authentication type as Web-authentication. |
| Auth Only Browser | 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. NOTE: This option is not supported if you select the authentication type as Web-authentication. |

Table 249: Fields on the Security Policies Page (*continued*)

| Field | Action |
|---------------------------------|---|
| 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 | Select the action to be taken on a destination address translation from the list. The options available are: None, Drop Translated, and Drop Untranslated. |
| Redirect Options | <p>Select a redirect action from the list. The options available are: None, Redirect Wx, and Reverse Redirect Wx.</p> <p>NOTE: This option is not supported for SRX5000 line of devices.</p> |
| 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 | <p>Click Schedule and select one of the configured schedules from the list.</p> <p>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 252 on page 668.</p> |

Table 250: 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 . |

Table 250: Fields on the Create Address Page (*continued*)

| Field | Action |
|---------------|---|
| IPv4 | |
| IPv4 Address | Enter a valid IPv4 address. |
| 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 251: 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. |
| 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. |

Table 251: Fields on the Create Service Page (*continued*)

| Field | Action |
|--------------------------|--|
| 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. |
| 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 252: Fields on the Add New Schedule Page

| Field | Action |
|-------|----------------------------------|
| Name | Enter the name for the schedule. |

Table 252: Fields on the Add New Schedule Page (*continued*)

| Field | Action |
|-------------|--|
| Description | Enter a description for the schedule. |
| Repeats | <p>Select an option from the list to repeat the schedule:</p> <ul style="list-style-type: none"> • Never • Daily • Weekly |
| All Day | <p>Enable this option to schedule an event for an entire day.</p> <p>This option is available only for Never and Daily repeat type schedule.</p> |
| Start Date | <p>Select the schedule start date in the YYYY-MM-DD format.</p> <p>This option is available only for Never repeat type schedule.</p> |
| 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> |

Table 252: Fields on the Add New Schedule Page (continued)

| Field | Action |
|-------------------|--|
| 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"> Click Set Time or Set Time to Selected Days. The Set Time to Selected Days page appears. 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. Click OK to save changes. <p>This option is available only for Weekly repeat type schedule.</p> |
| 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. Enter the following details: <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 Rule | 671](#)

[Clone a Rule | 671](#)

Clone a 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” on page 659](#).

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 Rules](#) | [672](#)

Edit a 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” on page 659](#).

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

RELATED DOCUMENTATION

| [Delete Rules](#) | [672](#)

Delete Rules

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-side of the page.
3. Click **Yes** to delete the rules or click **No** to retain the rules.

RELATED DOCUMENTATION

| [About the Security Policies Page](#) | 652

Zones/Screens

IN THIS CHAPTER

- [About the Zones/Screens Page | 673](#)
- [Add a Zone | 674](#)
- [Edit a Zone | 677](#)
- [Delete Zone | 677](#)
- [Add a Screen | 678](#)
- [Edit a Screen | 686](#)
- [Delete Screen | 686](#)

About the Zones/Screens Page

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 674.](#)
- Edit a Zone. See [“Edit a Zone” on page 677.](#)
- Delete Zone. See [“Delete Zone” on page 677.](#)
- Add a Screen. See [“Add a Screen” on page 678.](#)
- Edit a Screen. See [“Edit a Screen” on page 686.](#)
- Delete Screen. See [“Delete Screen” on page 686.](#)

Field Descriptions

[Table 253 on page 674](#) describes the fields on Zones/Screens page.

Table 253: 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. |
| Description | Displays a description of the screen. |

RELATED DOCUMENTATION

| [Add a Zone](#) | 674.

Add a Zone

You are here: **Security Policies & Objects > Zones/Screens.**

To add a zone:

1. Click the add icon (+) on the upper right side of the Zone List page.

The Add Zone page appears.

2. Complete the configuration according to the guidelines provided in [Table 254 on page 675](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 254: 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. |
| 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 | |

Table 254: Fields on the Add Zone page (*continued*)

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

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 side 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 674](#).

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

RELATED DOCUMENTATION

| [Delete Zone](#) | 677.

Delete 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 side 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](#) | 678.

Add a Screen

You are here: **Security Policies & Objects > Zones/Screens.**

To add a screen:

1. Click the add icon (+) on the upper right side of the Screen List page.
The Add Screen page appears.
2. Complete the configuration according to the guidelines provided in [Table 255 on page 678](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

[Table 255 on page 678](#) describes the fields on the Add Screen page.

Table 255: 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 | <p>Select the check box to enable this feature.</p> <p>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.</p> |
| IP sweep | <p>Select the check box to enable this feature.</p> <p>Specifies the number of ICMP address sweeps. An IP address sweep can occur with the intent of triggering responses from active hosts.</p> |
| Threshold | <p>Enter the time interval for an IP sweep.</p> <p>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.</p> <p>Range: 1000 through 1000000 microseconds. The default value is 5000 microseconds.</p> |

Table 255: 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> |
| 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> |

Table 255: Fields on the Add Screen Page (*continued*)

| Field | Action |
|-----------------------------------|--|
| Large size ICMP packet protection | Select the check box to enable this feature. |
| Block fragment traffic | Select the check box to enable this feature. |
| SYN-ACK-ACK proxy protection | Select the check box to enable this feature. |
| Threshold | Enter the threshold value for SYN-ACK-ACK proxy protection. NOTE: The range is from 1 through 250000 sessions. The default value is 512 sessions. |
| Anomalies | |
| 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. 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. • 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 255: 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> |
| UDP flood protection | <p>Select the check box to enable the User Datagram Protocol (UDP) flood counter.</p> <p>NOTE: UDP flooding occurs when an attacker sends IP packets containing UDP datagrams to slow system resources, such that valid connections can no longer be handled.</p> |

Table 255: Fields on the Add Screen Page (*continued*)

| Field | Action |
|---|---|
| Threshold | <p>Enter the threshold value for UDP flood protection.</p> <p>NOTE: Range: 1 through 100000 session. The default value is 1000 sessions.</p> |
| <p>UDP white list</p> <p>Starting Junos Release 18.1R1, the option to add UDP IP addresses and allowlist them is available.</p> | <ol style="list-style-type: none"> Click Select. A window appears. Click + to add IP addresses that you wish to allowlist. A window appears. 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> Click OK to save the changes. Select the allowlist name in the UDP White List page that you associated with the group of IP addresses from the Available column and move it to the Selected column using the right arrow. Click OK to save the changes. <p>NOTE:</p> <ul style="list-style-type: none"> The option is enabled only if you select UDP flood protection. The allowlist that you created in the UDP white list window will be available in the TCP white list window also for selection. <p>To edit an allowlist, select the allowlist name and click on the pencil icon.</p> <p>To delete an allowlist, 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 age 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 255: Fields on the Add Screen Page (*continued*)

| Field | Action |
|---|---|
| <p>TCP white list</p> <p>Starting Junos Release 18.1R1, the option to add TCP IP addresses and allowlist them is available.</p> | <ol style="list-style-type: none"> Click Select. A window appears. Click + to add IP addresses that you wish to allowlist. A window appears. 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> Click OK to save the changes. Select the allowlist name (that you associated with the group of IP addresses) from the Available column and move it to the Selected column using the right arrow. Click OK to save the changes. <p>NOTE:</p> <ul style="list-style-type: none"> This option is enabled only if you select SYN flood protection. The allowlist that you created in the TCP white list window will be available in the UDP white list window also for selection. <p>To edit an allowlist, select the allowlist name and click on the pencil icon.</p> <p>To delete an allowlist, 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> |
| 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> |

Table 255: Fields on the Add Screen Page (continued)

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

Table 255: Fields on the Add Screen Page (*continued*)

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

Release History Table

| Release | Description |
|------------------------|--|
| 18.1R1 | Starting Junos Release 18.1R1, the option to add UDP IP addresses and allowlist them is available. |
| 18.1R1 | Starting Junos Release 18.1R1, the option to add TCP IP addresses and allowlist them is available. |

RELATED DOCUMENTATION

[Edit a Screen](#) | [686](#).

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 side 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 678.](#)

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

RELATED DOCUMENTATION

| [Delete Screen](#) | [686.](#)

Delete 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 side of the Screen List page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

| [About the Zones/Screens Page](#) | [673.](#)

Zone Addresses

IN THIS CHAPTER

- [About the Zone Addresses Page | 687](#)
- [Add Zone Addresses | 689](#)
- [Clone Zone Addresses | 690](#)
- [Edit Zone Addresses | 691](#)
- [Delete Zone Addresses | 691](#)
- [Search Text in a Zone Addresses Table | 692](#)

About the Zone Addresses Page

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 689](#).
- Edit addresses or address sets. See [“Edit Zone Addresses” on page 691](#).
- Delete addresses or address sets. See [“Delete Zone Addresses” on page 691](#).
- Clone addresses or address sets. See [“Clone Zone Addresses” on page 690](#).
- 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 692](#).
- Show or hide columns in the Web filtering profiles table. To do this, click the Show Hide Columns icon in the top 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 256 on page 688](#) describes the fields on the Zone Addresses page.

Table 256: 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. |
| 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](#) | [689](#).

Add Zone Addresses

You are here: **Security Policies & Objects > Zone Addresses.**

To create a zone address or address set:

1. Click the add icon (+) on the upper right side of the Zone Addresses page.
The Create Addresses page appears.
2. Complete the configuration according to the guidelines provided in [Table 257 on page 689](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 257: Fields on the Create Addresses Page

| Field | Action |
|----------------------------------|---|
| Object Type | Select an option from the list: Address or Address Group. |
| 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. |

Table 257: Fields on the Create Addresses Page (*continued*)

| Field | Action |
|--------------------|---|
| DNS Name | <p>Enter a domain hostname.</p> <p>The string must include alphanumeric characters, periods, dashes, no spaces are allowed and must end with an alphanumeric character.</p> <p>NOTE: This option is available if you have selected DNS Host type.</p> |
| 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 | <p>Enter a name for address set.</p> <p>NOTE: This option is available if you have selected Address Group for Object type.</p> |
| 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](#) | 691.

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 side 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 689](#).

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

RELATED DOCUMENTATION

| [Delete Zone Addresses](#) | [691](#).

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 side 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 689](#).

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

RELATED DOCUMENTATION

| [Delete Zone Addresses](#) | [691](#).

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 side 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](#) | 692.

Search Text in a Zone Addresses Table

You are here: **Security Policies & Objects** > **Zone Addresses**.

You can use the search icon in the top 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](#) | 687.

Global Addresses

IN THIS CHAPTER

- [About the Global Addresses Page | 693](#)
- [Add an Address Book | 694](#)
- [Edit an Address Book | 697](#)
- [Delete Address Book | 697](#)

About the Global Addresses Page

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 694](#).
- Edit an Address Book. See [“Edit an Address Book” on page 697](#).
- Delete an Address Book. See [“Delete Address Book” on page 697](#).
- 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 258 on page 694](#) describes the fields on the Global Addresses Page.

Table 258: 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](#) | 694.

Add an Address Book

You are here: **Security Policies & Objects** > **Global Addresses**.

To add an address book:

1. Click the add icon (+) on the upper right side of the Global Addresses page.
The Add Address Book page appears.
2. Complete the configuration according to the guidelines provided in [Table 259 on page 695](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 259: 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 | |
| + | <p>To add an address:</p> <ol style="list-style-type: none"> 1. Click + available at the upper right side of the Addresses table. The Add Address page appears. 2. 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. 3. Click OK to save the changes. |
| Edit | <p>To edit an address:</p> <ol style="list-style-type: none"> 1. Select an existing address and click the pencil icon available at the upper right side of the Addresses table. The Add Address page appears with editable fields. 2. Click OK to save the changes. |

Table 259: Fields on the Global Addresses Page (*continued*)

| Field | Action |
|--------------------|--|
| Delete | Select an existing address and click the delete (X) icon available at the upper right side of the Addresses table to delete it. |
| Address Set | |
| + | <p>To add an address set:</p> <ol style="list-style-type: none"> Click + available at the upper right side 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 at the upper right side of the Address Set table. The Add Address Set page appears with editable fields. Click OK to save the changes. |
| Delete | Select an existing address set and click the delete (X) icon available at the upper right side of the Address Set table to delete it. |

RELATED DOCUMENTATION

[Edit an Address Book](#) | 697.

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 side 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 694](#).

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

RELATED DOCUMENTATION

[Delete Address Book](#) | 697.

Delete 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 side 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](#) | 693.

Services

IN THIS CHAPTER

- [About the Services Page | 698](#)
- [Add a Custom Application | 700](#)
- [Edit a Custom Application | 702](#)
- [Delete Custom Application | 703](#)
- [Add an Application Group | 703](#)
- [Edit an Application Group | 704](#)
- [Delete Application Group | 705](#)

About the Services Page

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 700.](#)
- Edit a custom application. See [“Edit a Custom Application” on page 702.](#)
- Delete custom application. See [“Delete Custom Application” on page 703.](#)
- Add an application group. See [“Add an Application Group” on page 703.](#)
- Edit an application group. See [“Edit an Application Group” on page 704.](#)
- Delete an application group. See [“Delete Application Group” on page 705.](#)

Field Descriptions

[Table 260 on page 699](#) describes the fields on the Services Page.

Table 260: 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. |
| 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](#) | 700.

Add a Custom Application

You are here: **Security Policies & Objects > Services.**

To add a custom application:

1. Click the **Custom-Applications** tab.
2. Click the add icon (+) on the upper right side of the Services page.
The Add an Application page appears.
3. Complete the configuration according to the guidelines provided in [Table 261 on page 700](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 261: 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. |

Table 261: Fields on the Add an Application Page (*continued*)

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

Table 261: Fields on the Add an Application Page (*continued*)

| Field | Action |
|--------|---|
| Edit | Select a term and click the pencil icon at the right corner of the table to modify the configuration. |
| 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](#) | 702.

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 side 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 700](#).

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

RELATED DOCUMENTATION

[Delete Custom Application](#) | 703.

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 side 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](#) | 700

[Add an Application Group](#) | 703.

Add an Application Group

You are here: **Security Policies & Objects** > **Services**.

To add an application group:

1. Click the **Application Group** tab.
2. Click the add icon (+) on the upper right side of the Application Group page.
The Add New Application Set page appears.
3. Complete the configuration according to the guidelines provided in [Table 262 on page 704](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 262: 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. |
| 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](#) | 704.

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 side 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 703](#).

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

RELATED DOCUMENTATION

| [Delete Application Group | 705](#).

Delete 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 side 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 | 698](#).

Dynamic Applications

IN THIS CHAPTER

- [About the Dynamic Applications Page | 706](#)
- [Global Settings | 709](#)
- [Add Application Signatures | 711](#)
- [Clone Application Signatures | 715](#)
- [Add Application Signatures Group | 716](#)
- [Edit Application Signatures | 717](#)
- [Delete Application Signatures | 718](#)
- [Search Text in an Application Signatures Table | 718](#)

About the Dynamic Applications Page

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 709](#).
- Create application signatures. See [“Add Application Signatures” on page 711](#).
- Create application signatures group. See [“Add Application Signatures Group” on page 716](#).
- Edit application signatures. See [“Edit Application Signatures” on page 717](#).
- Delete application signatures. See [“Delete Application Signatures” on page 718](#).
- Clone application signatures. See [“Clone Application Signatures” on page 715](#).
- Search text in an application signature. See [“Search Text in an Application Signatures Table” on page 718](#).
- 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 top right-hand 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 top 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.
- **Download**—Manually downloads the latest or predefined application signature package.
- **More**—Clone an existing application signature package, create group, or configure the page to show a detailed view.
- **Create Group**—Create a new application signature or application signatures group.
- **Uninstall**—Removes application signatures that are currently installed on your device.

On SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800 devices, specify the type of signature to uninstall. Choose one of the uninstall options:

- **Customized**—Uninstalls all customized application signatures on your device. This option does not uninstall predefined application signatures.
- **Predefined**—Uninstalls all predefined application signatures on your device. This option does not uninstall any customized applications.
- **All**—Uninstalls all customized and predefined application signatures on your device.

Field Descriptions

Table 263 on page 708 describes the fields on the Application Signatures page.

Table 263: 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 | 709](#)
- [Add Application Signatures | 711](#)
- [Add Application Signatures Group | 716](#)
- [Edit Application Signatures | 717](#)
- [Delete Application Signatures | 718](#)
- [Clone Application Signatures | 715](#)
- [Search Text in an Application Signatures Table | 718](#)

Global Settings

You are here: **Security Policies & Objects > Dynamic Applications.**

To add global settings:

1. Click the **Global Settings** on the upper right side of the Application Signatures page.
The Global Settings page appears.
2. Complete the configuration according to the guidelines provided in [Table 264 on page 709](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 264: Fields on the Global Settings Option page

| Field | Action |
|--|--|
| Application Signature | |
| Specifies run conditions, to enable or disable application signatures and the application system cache. You can also select a proxy profile or create a proxy profile. | |
| Application Identification | Disable the application identification of applications running on your network. Click the check box to Disable this option. |
| Proxy Profile | To create a proxy profile: 1. Click Create Profile . 2. Enter the following details: <ul style="list-style-type: none">• Profile Name—Enter a valid profile name.• Connection Type—Select any one option from the following:<ul style="list-style-type: none">• Server IP—Enter the server IP address• Host Name—Enter the host name.• Port Number—Enter the port number in the range 0 through 65535. Default port number is 80. 3. Click OK to save the changes. If you want to discard your changes, click Cancel . |

Table 264: Fields on the Global Settings Option page (*continued*)

| Field | Action |
|-------------------------------|--|
| Custom Application Byte Limit | <p>Select the byte limit in the range 0 through 10000. This helps in understanding when to stop the identification of custom applications.</p> <p>NOTE: Starting in Junos OS Release 20.2R1, Custom Application Byte Limit option is supported.</p> |

Download

Specifies the URL from where you can download the signature package, set up a schedule for automatic downloads of the latest predefined application signature package.

| | |
|------------------|--|
| URL | Enter the URL for the application package for downloading. |
| Automatic Update | Enable this option to schedule download and update. |

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. |
| Security Services | Enable this option for security services, such as security policies, application firewall (AppFW), Juniper Sky ATP, IDP, and UTM |
| 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. |

Release History Table

| Release | Description |
|------------------------|---|
| 20.2R1 | Starting in Junos OS Release 20.2R1, Custom Application Byte Limit option is supported. |

RELATED DOCUMENTATION

| | |
|--|-----|
| About the Dynamic Applications Page | 706 |
| Add Application Signatures | 711 |
| Add Application Signatures Group | 716 |
| Edit Application Signatures | 717 |
| Delete Application Signatures | 718 |
| Clone Application Signatures | 715 |
| Search Text in an Application Signatures Table | 718 |

Add Application Signatures

You are here: **Security Policies & Objects > Dynamic Applications.**

To add an application signature:

1. Click **Create > Signature** on the upper right side of the Dynamic Applications page.
The Create Application Signatures page appears.
2. Complete the configuration according to the guidelines provided in [Table 265 on page 711](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 265: 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 265: 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>Starting in Junos OS Release 20.2R1, 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 | Enter the risk as critical, high, moderate, low, or unsafe. |
| 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.</p> <p>The range is from 0 through 254.</p> |

Table 265: 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"> 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. Click the pencil icon at the top right side of the Address Mapping table. Then, edit the address mapping and click OK. 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> |
| Add Signature | |
| Over Protocol | <p>Displays the signature that matches the application protocol.</p> <p>Example: HTTP</p> |
| 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 | <p>Enter the port range for the application.</p> <p>Range is 0-65535.</p> |

Table 265: Fields on the Add Application Signatures Page (*continued*)

| Field | Action |
|--|---|
| 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) | <p>Select the service-specific context from the following list:</p> <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 |
| 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> |

Table 265: Fields on the Add Application Signatures Page (*continued*)

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

Release History Table

| Release | Description |
|------------------------|---|
| 20.2R1 | Starting in Junos OS Release 20.2R1, Depth option is supported. |

RELATED DOCUMENTATION

- [About the Dynamic Applications Page | 706](#)
- [Global Settings | 709](#)
- [Add Application Signatures Group | 716](#)
- [Edit Application Signatures | 717](#)
- [Delete Application Signatures | 718](#)
- [Clone Application Signatures | 715](#)
- [Search Text in an Application Signatures Table | 718](#)

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 711](#).

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

RELATED DOCUMENTATION

| |
|--|
| About the Dynamic Applications Page 706 |
| Global Settings 709 |
| Add Application Signatures 711 |
| Add Application Signatures Group 716 |
| Edit Application Signatures 717 |
| Delete Application Signatures 718 |
| Search Text in an Application Signatures Table 718 |

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 side 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 266 on page 716](#).
- 3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 266: Fields on the Add Application Signature Group Page

| Field | Action |
|-------|---|
| Name | Enter the application signature group name. |

Table 266: Fields on the Add Application Signature Group Page (continued)

| Field | Action |
|---------------|---|
| 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 706 |
| Edit Application Signatures 717 |
| Delete Application Signatures 718 |
| Clone Application Signatures 715 |
| Search Text in an Application Signatures Table 718 |

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 side of the page.

The Edit Application Signatures page appears with editable fields. For more information on the options, see [“Add Application Signatures” on page 711.](#)

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

RELATED DOCUMENTATION

| | |
|--|-----|
| About the Dynamic Applications Page | 706 |
| Global Settings | 709 |
| Add Application Signatures | 711 |
| Add Application Signatures Group | 716 |
| Add Application Signatures Group | 716 |
| Delete Application Signatures | 718 |
| Clone Application Signatures | 715 |
| Search Text in an Application Signatures Table | 718 |

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 side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

| | |
|--|-----|
| About the Dynamic Applications Page | 706 |
| Global Settings | 709 |
| Add Application Signatures | 711 |
| Add Application Signatures Group | 716 |
| Edit Application Signatures | 717 |
| Clone Application Signatures | 715 |
| Search Text in an Application Signatures Table | 718 |

Search Text in an Application Signatures Table

You are here: **Security Policies & Objects > Dynamic Applications.**

You can use the search icon in the top 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 706 |
| Global Settings 709 |
| Add Application Signatures 711 |
| Add Application Signatures Group 716 |
| Edit Application Signatures 717 |
| Delete Application Signatures 718 |
| Clone Application Signatures 715 |

Application Tracking

IN THIS CHAPTER

- About the Application Tracking Page | 720

About the Application Tracking Page

You are here: **Security Policies & Objects** > **Application Tracking**.

Use this page to configure application tracking.

Field Description

To configure application tracking:

- Complete the configuration according to the guidelines provided in [Table 267 on page 720](#).
- Click **Save** to save the changes.

[Table 267 on page 720](#) describes the fields on the Application Tracking page.

Table 267: Fields on the Application Tracking Page

| Field | Description |
|-----------------------------|--|
| Application tracking | Select this option to enable application tracking. |
| Logging Type | Select an option: <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. |

Table 267: Fields on the Application Tracking Page *(continued)*

| Field | Description |
|-------------------------------|--|
| 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 | 860](#)

Schedules

IN THIS CHAPTER

- [About the Schedules Page | 722](#)
- [Add a Schedule | 723](#)
- [Clone a Schedule | 725](#)
- [Edit a Schedule | 726](#)
- [Delete Schedule | 726](#)
- [Search Text in Schedules Table | 727](#)

About the Schedules Page

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 723](#).
- Clone a schedule. See [“Clone a Schedule” on page 725](#).
- Edit a schedule. See [“Edit a Schedule” on page 726](#).
- Delete a schedule. See [“Delete Schedule” on page 726](#).
- 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 727](#).
- Show or hide columns in the Schedules table. To do this, click the Show Hide Columns icon in the top 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 268 on page 723](#) describes the fields on the Schedules Page.

Table 268: 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](#) | 723

Add a Schedule

You are here: **Security Policies & Objects > Schedules.**

To add a schedule:

1. Click the add icon (+) on the upper right side of the Schedules page.

The Create Schedule page appears.

2. Complete the configuration according to the guidelines provided in [Table 269 on page 724](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 269: 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 hours format. |
| Stop Date | Select the stop date for the first day from the calendar and select the time in AM, PM, or 24 hours format. |
| Second Start Date | Select the start date for the second day from the calendar and select the time in AM, PM, or 24 hours format. |
| Second End Date | Select the stop date for the second day from the calendar and select the time in AM, PM, or 24 hours format. |
| Time Ranges | |
| Time Ranges | Select the check box to specify the time range. |

Table 269: Fields on the Create Schedule Page (continued)

| Field | Action |
|---------------|---|
| Daily Options | <ol style="list-style-type: none"> 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. 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> Click OK to save changes. |

RELATED DOCUMENTATION

[Edit a Schedule](#) | 726.

Clone a Schedule

You are here: **Security Policies & Objects > Schedules.**

To clone a schedule:

- 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 723.](#)

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](#) | 726.

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 side of the Schedules page.

The Edit Schedules page appears with editable fields. For more information on the options, see "[Add a Schedule](#)" on page 723.

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

RELATED DOCUMENTATION

| [Delete Schedule](#) | 726.

Delete 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 side 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 | 727.](#)

Search Text in Schedules Table

You are here: **Security Policies & Objects > Schedules.**

You can use the search icon in the top 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 | 722.](#)

Proxy Profiles

IN THIS CHAPTER

- [About the Proxy Profiles Page | 728](#)
- [Add a Proxy Profile | 729](#)
- [Edit a Proxy Profile | 730](#)
- [Delete Proxy Profile | 731](#)

About the Proxy Profiles Page

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 729](#).
- Edit a proxy profile. See [“Edit a Proxy Profile” on page 730](#).
- Delete a proxy profile. See [“Delete Proxy Profile” on page 731](#).
- Filter the proxy profile based on select criteria. To do this, select the filter icon at the top right-hand 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 top 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 270 on page 729](#) describes the fields on the Proxy Profiles Page.

Table 270: 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 | 729.](#)

Add a Proxy Profile

You are here: **Security Policies & Objects > Proxy Profiles.**

To add a proxy profile:

1. Click the add icon (+) on the upper right side of the Proxy Profiles page.
The Create Proxy Profile page appears.
2. Complete the configuration according to the guidelines provided in [Table 271 on page 730](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

[Table 271 on page 730](#) describes the fields on the Create Proxy Profile Page.

Table 271: 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 | 730](#).

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 side 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 729](#).

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

RELATED DOCUMENTATION

[Delete Proxy Profile | 731.](#)

Delete 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 side 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 | 729.](#)

[Edit a Proxy Profile | 730.](#)

7

PART

Security Services

UTM Default Configuration | **734**

UTM Antivirus Profiles | **738**

UTM Web Filtering Profiles | **747**

UTM Web Filtering Category Update | **758**

UTM Antispam Profiles | **764**

UTM Content Filtering Profiles | **770**

UTM Custom Objects | **778**

UTM Policies | **791**

IPS Signature Update | **798**

IPS Sensor | **804**

IPS Policy | **810**

ALG | **819**

Advanced Threat Prevention | **828**

SSL Initiation Profiles | **833**

SSL Proxy Profiles | **839**

Firewall Authentication—Access Profile | **851**

Firewall Authentication—Address Pools | **860**

Firewall Authentication Settings | **865**

Firewall Authentication—UAC Settings | **868**

Firewall Authentication—Active Directory | **871**

Firewall Authentication—Local Authentication | **876**

Firewall Authentication—Authentication Priority | **879**

Firewall Authentication—Identity Management | **881**

ICAP Redirect | **887**

UTM Default Configuration

IN THIS CHAPTER

- [About the Default Configuration Page | 734](#)
- [Edit a Default Configuration | 735](#)
- [Delete Default Configuration | 736](#)

About the Default Configuration Page

You are here: **Security Services > UTM > Default Configuration.**

The Default Configuration page describes the security features of Unified Treat Management (UTM).

This default configuration will be used, if there are multiple UTM policies present in the potential list. The global configuration will be used till the exact match is found in the potential list.

The following security features are parts of UTM default configuration:

- **Antivirus**—Antivirus is an in-the-cloud antivirus solution. The virus pattern and malware database is located on external servers maintained by Sophos (Sophos Extensible List) servers.
- **Web Filtering**—Web filtering lets you to manage Internet usage by preventing access to inappropriate Web content.
- **Antispam**—This feature examines transmitted messages to identify any e-mail spam.
- **Content Filtering**—This feature blocks or permits certain types of traffic based on the MIME type, file extension, protocol command, and embedded object type.

Tasks You Can Perform

You can perform the following tasks from this page:

- View the collapsed or expanded details of the UTM default configuration options. To do this, select any one of the UTM default configurations and click **Expand All** or **Collapse All** available on the upper right side of the page.

- Edit a default configuration. See [“Edit a Default Configuration” on page 735](#).
- Delete a default configuration. See [“Delete Default Configuration” on page 736](#).

Field Descriptions

[Table 272 on page 735](#) describes the fields on the Default Configuration page.

Table 272: 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. |
| 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 735 |
| Delete Default Configuration 736 |

Edit a Default Configuration

You are here: **Security Services > UTM > Default Configuration.**

You can edit all of the following UTM default configurations:

- Antivirus
- Web filtering
- Antispam
- Content filtering

To edit a default configuration:

1. Select any of the existing UTM default configurations that you want to edit on the Default Configuration page.
2. Click the pencil icon available on the upper right side 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 | 734](#)

[Delete Default Configuration | 736](#)

Delete Default Configuration

You are here: **Security Services > UTM > Default Configuration.**

You can delete all of the following UTM default configurations:

- Antivirus
- Web filtering
- Antispam
- Content filtering

To delete an individual default configuration:

1. Select any of the existing UTM default configurations that you want to delete on the Default Configuration page.
2. Click the delete icon available on the upper right side 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 side 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 | 734](#)

[Edit a Default Configuration | 735](#)

UTM Antivirus Profiles

IN THIS CHAPTER

- [About the Antivirus Profiles Page | 738](#)
- [Add an Antivirus Profile | 740](#)
- [Clone an Antivirus Profile | 744](#)
- [Edit an Antivirus Profile | 745](#)
- [Delete Antivirus Profile | 745](#)

About the Antivirus Profiles Page

You are here: **Security Services** > **UTM** > **Antivirus Profiles**.

Use this page to configure antivirus.

For an example use case, see the [In Focus - J-Web for SRX Series](#) Guide.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add an antivirus profile. See [“Add an Antivirus Profile” on page 740](#).
- Clone an antivirus profile. See [“Clone an Antivirus Profile” on page 744](#).
- Edit an antivirus profile. See [“Edit an Antivirus Profile” on page 745](#).
- Delete antivirus profile. See [“Delete Antivirus Profile” on page 745](#).
- 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 top right-hand 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 top 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 273 on page 739 describes the fields on the Antivirus Profiles page.

Table 273: Fields on the Antivirus Profiles Page

| Field | Function |
|----------------|---|
| Name | Displays the unique name of the antispam profile. |
| URL Whitelist | 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 740 |
| Edit an Antivirus Profile 745 |
| Delete Antivirus Profile 745 |

Add an Antivirus Profile

You are here: **Security Services > UTM > Antivirus Profiles.**

To add an antivirus profile:

1. Click the add icon (+) available on the upper right side 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 274 on page 740](#).
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 UTM policy. Within the UTM policy, you can apply either the same or different antivirus profiles to the Web, file transfer and E-mail traffic.

Table 274: 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. |

Table 274: Fields on the Create Antivirus Profile Page (*continued*)

| Field | Function |
|--------------------------|--|
| URL Whitelist | Select the customized object from the list for a given category that are to be bypassed for scanning. |
| MIME Whitelist | |
| MIME Whitelist | <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. The Add MIME Pattern List window appears. 2. Enter the following details: <ul style="list-style-type: none"> • Name—Enter a unique name for the MIME pattern list. 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. • 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. A new MIME list is created and added to the MIME allowlist. |
| Exception MIME Whitelist | <p>Select an exception MIME allowlist from the list.</p> <p>Click Create New MIMElist to create and add a MIME pattern list inline.</p> |

Table 274: 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 | 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. |
| Trickling Timeout | 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. |
| Out of Resources | 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. |
| Decompress Layer | 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. |
| Too many Requests | 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. |
| Default Action | Select a default action to take when an error occurs; Block or Log and Permit . |
| 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 | |

Table 274: Fields on the Create Antivirus Profile Page (*continued*)

| Field | Function |
|--------------------------|--|
| 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. |
| 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. |

Table 274: Fields on the Create Antivirus Profile Page (*continued*)

| Field | Function |
|------------------------|---|
| 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 | 738](#)
[Edit an Antivirus Profile | 745](#)
[Delete Antivirus Profile | 745](#)

Clone an Antivirus Profile

You are here: **Security Services** > **UTM** > **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 740](#).

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 | 738](#)[Edit an Antivirus Profile | 745](#)[Delete Antivirus Profile | 745](#)

Edit an Antivirus Profile

You are here: **Security Services > UTM > 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 side 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 740.](#)

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 | 738](#)[Edit an Antivirus Profile | 745](#)[Delete Antivirus Profile | 745](#)

Delete Antivirus Profile

You are here: **Security Services > UTM > 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 side 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 | 738](#)

[Add an Antivirus Profile | 740](#)

[Edit an Antivirus Profile | 745](#)

UTM Web Filtering Profiles

IN THIS CHAPTER

- [About the Web Filtering Profiles Page | 747](#)
- [Add a Web Filtering Profile | 749](#)
- [Clone a Web Filtering Profile | 755](#)
- [Edit a Web Filtering Profile | 756](#)
- [Delete Web Filtering Profile | 756](#)

About the Web Filtering Profiles Page

You are here: **Security Services > UTM > 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 the [In Focus - J-Web for SRX Series](#) Guide.

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 749](#).
- Edit a Web filtering profile. See [“Edit a Web Filtering Profile” on page 756](#).
- Clone a Web filtering profile. See [“Clone a Web Filtering Profile” on page 755](#).
- Delete a Web filtering profile. See [“Delete Web Filtering Profile” on page 756](#).
- Filter the Web filtering profiles based on select criteria. To do this, select the filter icon at the top right-hand 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 top 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.

Field Descriptions

Table 275 on page 748 describes the fields on the Web filtering page.

Table 275: 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. |

Table 275: Fields on the Web Filtering Page (*continued*)

| Field | Action |
|---------|---|
| Timeout | Displays the time interval to wait before the connection to the server is closed. |

RELATED DOCUMENTATION

[Add a Web Filtering Profile | 749](#)
[Edit a Web Filtering Profile | 756](#)
[Delete Web Filtering Profile | 756](#)

Add a Web Filtering Profile

You are here: **Security Services** > **UTM** > **Web Filtering Profiles**.

To create a new web filtering profile:

1. Click the add icon (+) available on the upper right side of the Web Filtering Profiles page.
The Create Web Filtering Profiles page appears.
2. Complete the configuration according to the guidelines provided in [Table 276 on page 749](#) through [Table 278 on page 754](#).
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 276: 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 276: 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 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 Enhanced.</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> |
| 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> |

Table 276: Fields on the General tab (*continued*)

| Field | Action |
|---------------------------|---|
| Custom Quarantine Message | <p>Define a custom message to allow or deny access to a blocked site based on a user's response to the message.</p> <p>Maximum length is 512 characters.</p> <p>NOTE: This option is available only for the Juniper Enhanced 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 engine type.</p> |

Table 277: 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"> Click Apply Actions. The Apply Actions page appears. 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"> Click Create New. Enter the following details: <ul style="list-style-type: none"> Name—Enter a unique name for the custom message list. Special characters such as hyphen, underscore, !, @, \$, *, + are allowed. The maximum length is 29 characters. 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. Click OK to add a new custom message list. Else, click Cancel. Click OK to apply actions for the category. Else, click Cancel. |

Table 277: 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 top 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 top right corner of the table |
| Search | Click the search icon in the top 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> |
| Action | Displays the action taken for the URL category. |
| Custom message | Displays the respective custom messages for the URL categories. |

Table 278: 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> |
| 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> |

Table 278: Fields on the Fallback Options Tab (*continued*)

| Field | Action |
|-----------------|--|
| 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 | 747](#)
[Clone a Web Filtering Profile | 755](#)
[Edit a Web Filtering Profile | 756](#)
[Delete Web Filtering Profile | 756](#)

Clone a Web Filtering Profile

You are here: **Security Services > UTM > 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 749](#).

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 | 747](#)

[Add a Web Filtering Profile | 749](#)

[Edit a Web Filtering Profile | 756](#)

[Delete Web Filtering Profile | 756](#)

Edit a Web Filtering Profile

You are here: **Security Services > UTM > 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 side 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 749](#).

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

RELATED DOCUMENTATION

[About the Web Filtering Profiles Page | 747](#)

[Add a Web Filtering Profile | 749](#)

[Clone a Web Filtering Profile | 755](#)

[Delete Web Filtering Profile | 756](#)

Delete Web Filtering Profile

You are here: **Security Services > UTM > 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 side 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 | 747](#)

[Add a Web Filtering Profile | 749](#)

[Clone a Web Filtering Profile | 755](#)

[Edit a Web Filtering Profile | 756](#)

UTM Web Filtering Category Update

IN THIS CHAPTER

- [About the Category Update Page | 758](#)
- [Category Update Settings | 760](#)
- [Download and Install Settings | 763](#)

About the Category Update Page

You are here: **Security Services > UTM > Web Filtering Category Update.**

Use the Category Update page to download and install a new Juniper Enhanced Web Filtering (EWF) category. You can also use the predefined base filter and all categories in the base filter have default actions.

A base filter is an object that contains a category action pair for all categories defined in the category file. predefined base filters, defined in a category file, are supported for individual EWF categories. Each EWF category has a default action in a base filter, which is attached to the user profile to act as a backup filter. If the categories are not configured in the user profile, then the base filter takes the action.

NOTE: If you have not installed the UTM license or if the license has expired, J-Web prompts you to install license to proceed with configuring the Category Update page. J-Web also provides the License Management page link for you to install the license on your device.

Tasks You Can Perform

You can perform the following tasks from this page:

- Configure URL settings and automatically download and install the category packages. See [“Category Update Settings” on page 760](#).
- Download a category package manually and install it on SRX Series devices with an EWF license. See [“Download and Install Settings” on page 763](#).

- Install a category file. To do this, click **Install** on the Category Update page to install the already downloaded category.
- Uninstall categories. To do this, select an existing category and click **Uninstall** on the Category Update page.

NOTE: The Uninstall option appears only when there is an installed version of the category package.

- Search a category name. To do this, enter the category name that you want to find and click the search icon in the top right corner of the Category Update page or above the base filters table.
- Show or hide columns in the base filters table. To do this, click the Show Hide Columns icon in the top right corner of the base filters table and select the options you want to view or deselect the options you want to hide on the page.

Field Descriptions

Table 279 on page 759 describes the fields on the Category Update page.

Table 279: Fields on the Category Update Page

| Field | Description |
|--------------------|--|
| Base Filters | Select a predefined base filter for your category. |
| Installed Versions | Displays the number of category package installed version. |
| Check Latest | Opens a new browser page and displays the latest list of EWF category files. |
| Download Completed | Displays the number of downloads completed status. |
| Name | Displays the category name of the base filter. |
| Action | Displays the action for each of the categories in the base filter. |

RELATED DOCUMENTATION

| |
|-------------------------------------|
| Category Update Settings 760 |
| Download and Install Settings 763 |

Category Update Settings

You are here: **Security Services > UTM > Web Filtering Category Update.**

Use this page to configure the URL to download, routing instances, proxy profiles, and auto-download settings.

To configure the category update settings:

1. Click **Settings**.
The Settings page appears.
2. Complete the configuration according to the guidelines provided in [Table 280 on page 760](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 280: Fields on the Settings Page

| Field | Action |
|--------------|--|
| Download URL | Enter the URL from where you want to download a category file. |

Table 280: Fields on the Settings Page (*continued*)

| Field | Action |
|------------------|--|
| Routing Instance | <p>Select an option from the list of configured routing instances or you can create a new routing instance inline.</p> <p>To create a new routing instance inline:</p> <ol style="list-style-type: none"> Click Create. The Create Routing Instance page appears. 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 the type of routing instance from the list: <ul style="list-style-type: none"> • Virtual Router—Used for non-VPN related applications. • VPLS—Lists the interfaces with Encapsulation Ethernet-VPLS. <p>NOTE: This instance is applicable only for root or super admin. This option will not be applicable for Logical system admin.</p> Interfaces—Select interfaces from the Available column and move it to the Selected column. <ul style="list-style-type: none"> • Name—Displays the interface name. • Zone—Displays the zone name corresponding to the interface name. Click OK. |

Table 280: Fields on the Settings Page (continued)

| Field | Action |
|----------------|---|
| Proxy Profile | <p>Select an option from the list of configured proxy profiles or you can create a new proxy profile inline.</p> <p>To create a new proxy profile inline:</p> <ol style="list-style-type: none"> Click Create. The 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 arrows. Range: 0 through 65535 Click OK. |
| Auto Download | <p>Enable this option to automatically detect a newer version of the UTM category file. If a newer version of UTM category is available, J-Web automatically downloads the file and installs it on your device.</p> |
| Start Time | <p>Specify a date and time (in MM/DD/YYYY and HH:MM:SS formats) to initiate automatic download and installation process for the category file.</p> |
| Interval (Hrs) | <p>Enter a time interval to download and check install category file.</p> <p>Range is 1 through 336.</p> |

RELATED DOCUMENTATION

[About the Category Update Page | 758](#)
[Download and Install Settings | 763](#)

Download and Install Settings

You are here: **Security Services > UTM > Web Filtering Category Update.**

Use this page to download or download and install URL category packages on your device.

To download and install URL category packages:

1. Click **Download**.
The Download and Install Settings page appears.
2. Complete the configuration according to the guidelines provided in [Table 281 on page 763](#).
3. Click **OK** to download the package. If you want to cancel the download, click **Cancel**.
If you have not selected the Download and Install option, then the package is only downloaded. You can install the package at a later time using **Install** available on the Category Update page.
If you have selected the Download and Install option, J-Web downloads the package and installs the URL categories on the SRX Series devices with an EWF license.

Table 281: Fields on the Download and Install Settings Page

| Field | Action |
|----------------------|--|
| Version | Select the latest version option or specify an available version number. |
| Download and Install | Enable this option if you want to install the categories after downloading them. |

RELATED DOCUMENTATION

- [About the Category Update Page | 758](#)
- [Category Update Settings | 760](#)

UTM Antispam Profiles

IN THIS CHAPTER

- [About the Antispam Profiles Page | 764](#)
- [Add an Antispam Profile | 766](#)
- [Clone an Antispam Profile | 767](#)
- [Edit an Antispam Profile | 768](#)
- [Delete Antispam Profile | 768](#)

About the Antispam Profiles Page

You are here: **Security Services > UTM > 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 766](#).
- Edit an antispam profile. See [“Edit an Antispam Profile” on page 768](#).
- Delete an antispam profile. See [“Delete Antispam Profile” on page 768](#).
- Clone an antispam profile. See [“Clone an Antispam Profile” on page 767](#).
- 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 top right-hand 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 top 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 282 on page 765 describes the fields on the Antispam Profiles page.

Table 282: Fields on the Antispam Profiles Page

| Field | Description |
|------------------|--|
| Name | Name of the antispam profile. |
| Sophos Blacklist | Indicates whether this option 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 | 766](#)
[Clone an Antispam Profile | 767](#)
[Edit an Antispam Profile | 768](#)
[Delete Antispam Profile | 768](#)

Add an Antispam Profile

You are here: **Security Services** > **UTM** > **Antispam Profiles**.

To add an antispam profile:

1. Click the add icon (+) on the upper right side of the Antispam Profiles page.
The Create Antispam Profiles page appears.
2. Complete the configuration according to the guidelines provided in [Table 283 on page 766](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 283: Fields on the Create Antispam Profiles Page

| Field | Action |
|----------------------------|---|
| General Information | |
| Name | Enter a unique name for your antispam profile. |
| Sophos Blacklist | 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. |

Table 283: Fields on the Create Antispam Profiles Page (*continued*)

| Field | Action |
|------------|--|
| 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 | 764](#)
[Clone an Antispam Profile | 767](#)
[Edit an Antispam Profile | 768](#)
[Delete Antispam Profile | 768](#)

Clone an Antispam Profile

You are here: **Security Services** > **UTM** > **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 766](#).

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 | 764](#)
[Add an Antispam Profile | 766](#)

[Edit an Antispam Profile | 768](#)[Delete Antispam Profile | 768](#)

Edit an Antispam Profile

You are here: **Security Services > UTM > 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 side of the page.

The Edit Antispam Profiles page appears. For more information on the options, see [“Add an Antispam Profile” on page 766.](#)

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

RELATED DOCUMENTATION

[About the Antispam Profiles Page | 764](#)[Add an Antispam Profile | 766](#)[Clone an Antispam Profile | 767](#)[Delete Antispam Profile | 768](#)

Delete Antispam Profile

You are here: **Security Services > UTM > Antispam Profiles.**

To delete antispam profiles:

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 side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the Antispam Profiles Page | 764](#)

[Add an Antispam Profile | 766](#)

[Clone an Antispam Profile | 767](#)

[Edit an Antispam Profile | 768](#)

UTM Content Filtering Profiles

IN THIS CHAPTER

- [About the Content Filtering Profiles Page | 770](#)
- [Add a Content Filtering Profile | 772](#)
- [Clone a Content Filtering Profile | 775](#)
- [Edit a Content Filtering Profile | 776](#)
- [Delete Content Filtering Profile | 776](#)

About the Content Filtering Profiles Page

You are here: **Security Services > UTM > 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 772.](#)
- Clone a content filtering profile. See [“Clone a Content Filtering Profile” on page 775](#)
- Edit a content filtering profile. See [“Edit a Content Filtering Profile” on page 776.](#)
- Delete a content filtering profile. See [“Delete Content Filtering Profile” on page 776.](#)
- 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 top right-hand 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 top 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 284 on page 771](#) describes the fields on the Content Filtering Profiles page.

Table 284: 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 772 |
| Edit a Content Filtering Profile 776 |
| Delete Content Filtering Profile 776 |

Add a Content Filtering Profile

You are here: **Security Services > UTM > Content Filtering Profiles.**

To add a content filtering profile:

1. Click the add icon (+) on the upper right side of the Content Filtering Profiles page.
The Create Content Filtering page appears.
2. Complete the configuration according to the guidelines provided in [Table 285 on page 772](#).
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 285: 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. |

Table 285: Fields on the Create Content Filtering Profiles Page (*continued*)

| Field | Action |
|-----------------------------|--|
| Custom Notification Message | <p>Specifies the customized message text for the content-block notification.</p> <p>Enter the text for this custom notification message (if you are using one).</p> |
| Protocol Commands | |
| 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. 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. 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. • Values—Click + and enter a value in the value list and click the tick mark. To delete any value list, select the value and click on the delete icon. 3. Click OK. 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 | |
| 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 |

Table 285: Fields on the Create Content Filtering Profiles Page (*continued*)

| Field | Action |
|------------------------|--|
| 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. The Add File Extension List window appears. 2. Enter the following details: <ul style="list-style-type: none"> • Name—Enter a unique name for the file extension list. 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. • Values—Select one or more values in the Available Column and move it to the Selected Column using the right arrow. 3. Click OK. A new file extension is created and added to the extension block list. |
| MIME Types | |
| 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"> 1. Click Create MIME List. The Add MIME Pattern List window appears. 2. Enter the following details: <ul style="list-style-type: none"> • Name—Enter a unique name for the MIME pattern list. 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. • Values—Click + and enter a value in the value list and click the tick mark. To delete any value list, select the value and click on the delete icon. 3. Click OK. A new MIME list is created and added to the MIME block list. |

Table 285: Fields on the Create Content Filtering Profiles Page (continued)

| Field | Action |
|------------------|--|
| 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 | 770](#)

[Edit a Content Filtering Profile | 776](#)

[Delete Content Filtering Profile | 776](#)

Clone a Content Filtering Profile

You are here: **Security Services > UTM > 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 772](#).

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 | 770](#)

[Edit a Content Filtering Profile | 776](#)

Edit a Content Filtering Profile

You are here: **Security Services > UTM > 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 side 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 772.](#)

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 | 770](#)

[Add a Content Filtering Profile | 772](#)

[Delete Content Filtering Profile | 776](#)

Delete Content Filtering Profile

You are here: **Security Services > UTM > 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 side 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 | 770](#)

[Add a Content Filtering Profile | 772](#)

[Edit a Content Filtering Profile | 776](#)

UTM Custom Objects

IN THIS CHAPTER

- [About the Custom Objects Page | 778](#)
- [Add a MIME Pattern List | 781](#)
- [Add a File Extension List | 782](#)
- [Add a Protocol Command List | 783](#)
- [Add a URL Pattern List | 784](#)
- [Add a URL Category List | 785](#)
- [Add a Custom Message List | 787](#)
- [Clone Custom Objects | 788](#)
- [Edit Custom Objects | 789](#)
- [Delete Custom Objects | 789](#)

About the Custom Objects Page

You are here: **Security Services > UTM > 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 781](#).
- Add a file extension list. See [“Add a File Extension List” on page 782](#).
- Add a protocol command list. See [“Add a Protocol Command List” on page 783](#).
- Add an URL pattern list. See [“Add a URL Pattern List” on page 784](#).
- Add an URL category list. See [“Add a URL Category List” on page 785](#).
- Add a custom message list. See [“Add a Custom Message List” on page 787](#).

- Edit custom objects. See [“Edit Custom Objects” on page 789](#).
- Delete custom objects. See [“Delete Custom Objects” on page 789](#).
- Clone custom objects. See [“Clone Custom Objects” on page 788](#).
- 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 top right-hand 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 top 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 286 on page 780](#) describes the fields on the Custom Objects page.

Table 286: 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 | |
| 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. |

Table 286: Fields on the Custom Objects Page (continued)

| Field | Description |
|---------|---|
| 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](#) | 781

Add a MIME Pattern List

You are here: **Security Services** > **UTM** > **Custom Objects**.

To add a MIME pattern list:

1. Click the **MIME Pattern List** tab.
2. Click the add icon (+) on the upper right side of the MIME Pattern List tab.
The Add MIME Pattern List page appears.
3. Complete the configuration according to the guidelines provided in [Table 287 on page 781](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 287: 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> |

Table 287: Fields on the Add MIME Pattern List Page (continued)

| Field | Action |
|-------|---|
| 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. NOTE: Value must be two strings separated by slash(/):<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 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 788 |
| Edit Custom Objects 789 |
| Delete Custom Objects 789 |

Add a File Extension List

You are here: **Security Services > UTM > Custom Objects.**

To add a file extension list:

1. Click the **File Extension List** tab.
2. Click the add icon (+) on the upper right side of the File Extension List tab.
The Add File Extension List page appears.

3. Complete the configuration according to the guidelines provided in [Table 288 on page 783](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 288: 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 | 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. |

RELATED DOCUMENTATION

[Clone Custom Objects | 788](#)

[Edit Custom Objects | 789](#)

[Delete Custom Objects | 789](#)

Add a Protocol Command List

You are here: **Security Services > UTM > Custom Objects**.

To add a protocol command list:

1. Click the **Protocol Command List** tab.
2. Click the add icon (+) on the upper right side of the Protocol Command List tab.
The Add Protocol Command List page appears.
3. Complete the configuration according to the guidelines provided in [Table 289 on page 784](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 289: 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 | 788](#)

[Edit Custom Objects | 789](#)

[Delete Custom Objects | 789](#)

Add a URL Pattern List

You are here: **Security Services > UTM > Custom Objects.**

To add a URL pattern list:

1. Click the **URL Pattern List** tab.
2. Click the add icon (+) on the upper right side of the URL Pattern List tab.

The Add URL Pattern List page appears.

3. Complete the configuration according to the guidelines provided in [Table 290 on page 785](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 290: 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 788 |
| Edit Custom Objects 789 |
| Delete Custom Objects 789 |

Add a URL Category List

You are here: **Security Services > UTM > Custom Objects.**

To add a URL category list:

1. Click the **URL Category List** tab.
2. Click the add icon (+) on the upper right side of the URL Category List tab.

The Add URL Category List page appears.

- 3. Complete the configuration according to the guidelines provided in [Table 291 on page 786](#).
- 4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

[Table 291 on page 786](#) provides guidelines on using the fields on the Add URL Category List page.

Table 291: 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. <p>The Add URL Pattern List page appears.</p> <ol style="list-style-type: none">2. Enter a URL pattern name. <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> <ol style="list-style-type: none">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 788 |
| Edit Custom Objects 789 |

Add a Custom Message List

You are here: **Security Services > UTM > Custom Objects.**

To add a custom message list:

1. Click the **Custom Message List** tab.
2. Click the add icon (+) on the upper right side of the Custom Message List tab.
The Add Custom Message List page appears.
3. Complete the configuration according to the guidelines provided in [Table 292 on page 787](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 292: 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 | 788](#)
- [Edit Custom Objects | 789](#)

Clone Custom Objects

You are here: **Security Services > UTM > 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 | 781](#)

[Add a File Extension List | 782](#)

[Add a Protocol Command List | 783](#)

[Add a URL Pattern List | 784](#)

[Add a URL Category List | 785](#)

[Add a Custom Message List | 787](#)

Edit Custom Objects

You are here: **Security Services > UTM > 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 side 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 | 781](#)

[Add a File Extension List | 782](#)

[Add a Protocol Command List | 783](#)

[Add a URL Pattern List | 784](#)

[Add a URL Category List | 785](#)

[Add a Custom Message List | 787](#)

Delete Custom Objects

You are here: **Security Services > UTM > 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 side of the page.
3. Click **Yes** to delete or click **No** to retain the selected custom object.

RELATED DOCUMENTATION

[About the Custom Objects Page | 778](#)

[Clone Custom Objects | 788](#)

[Edit Custom Objects | 789](#)

UTM Policies

IN THIS CHAPTER

- [About the UTM Policies Page | 791](#)
- [Add a UTM Policy | 793](#)
- [Clone a UTM Policy | 795](#)
- [Edit a UTM Policy | 796](#)
- [Delete UTM Policy | 797](#)

About the UTM Policies Page

You are here: **Security Services** > **UTM** > **UTM Policies**.

Use this page to configure UTM Policies.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a UTM policy. See [“Add a UTM Policy” on page 793](#).
- Clone a UTM policy. See [“Clone a UTM Policy” on page 795](#).
- Edit a UTM policy. See [“Edit a UTM Policy” on page 796](#).
- Delete a UTM policy. See [“Delete UTM Policy” on page 797](#).
- View the details of a UTM policy—To do this, select the UTM 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 UTM policy and select **Detailed View**.
 - Mouse over to the left of the selected UTM policy and click **Detailed View**.
- Advanced search for UTM 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 UTM policy table. To do this, click the Show Hide Columns icon in the top right corner of the UTM policies table and select the options you want to view or deselect the options you want to hide on the page.

Field Descriptions

Table 293 on page 792 describes the fields on the UTM policy page.

Table 293: Fields on the UTM Policy Page

| Field | Description |
|-------------------|--|
| Name | Displays the UTM 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

Add a UTM Policy

You are here: **Security Services** > **UTM** > **UTM Policies**.

To add a UTM policy:

1. Click the add icon (+) on the upper right side of the UTM Policy page.
The Create UTM Policies page appears.
2. Complete the configuration according to the guidelines provided in [Table 294 on page 793](#).
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 UTM policy is created.

Table 294: Fields on the Create UTM Policies Page

| Field | Action |
|---|---|
| General—General Information | |
| Name | Enter a UTM 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 UTM policy for the HTTP protocol to be scanned. |
| FTP Upload | Select an option from the list to specify the UTM policy for the FTP protocol to be scanned. |

Table 294: Fields on the Create UTM Policies Page (*continued*)

| Field | Action |
|------------------------|---|
| FTP Download | Select an option from the list to specify the UTM policy for the FTP protocol to be scanned. |
| IMAP | Select an option from the list to specify the UTM policy for the IMAP protocol to be scanned. |
| SMTP | Select an option from the list to specify the UTM policy for the SMTP protocol to be scanned. |
| POP3 | Select an option from the list to specify the UTM 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 740 . |

| Web Filterings—Web Filtering Profiles by Traffic Protocol | |
|---|---|
| HTTP | Select an option from the list to specify the UTM 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 749 . |

| Antispam—Antispam Profiles by Traffic Protocol | |
|--|--|
| SMTP profile | Select an option from the list to specify the UTM 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 766 . |

| Content Filtering—Content Filtering Profiles by Traffic Protocol | |
|--|--|
| Apply to all protocols | <p>Select the check box to apply the default profile to all protocols such as HTTP, FTP, IMAP, SMTP, and POP3.</p> <p>If you do not select the check box, you can apply different profiles to different protocols.</p> |
| HTTP | Select an option from the list to specify the UTM policy for the HTTP protocol to be scanned. |

Table 294: Fields on the Create UTM Policies Page (*continued*)

| Field | Action |
|------------------------|---|
| FTP Upload | Select an option from the list to specify the UTM policy for the FTP protocol to be scanned. |
| FTP Download | Select an option from the list to specify the UTM policy for the FTP protocol to be scanned. |
| IMAP | Select an option from the list to specify the UTM policy for the IMAP protocol to be scanned. |
| SMTP | Select an option from the list to specify the UTM policy for the SMTP protocol to be scanned. |
| POP3 | Select an option from the list to specify the UTM 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 772 . |

RELATED DOCUMENTATION

[About the UTM Policies Page | 791](#)
[Clone a UTM Policy | 795](#)
[Edit a UTM Policy | 796](#)
[Delete UTM Policy | 797](#)

Clone a UTM Policy

You are here: **Security Services** > **UTM** > **UTM Policies**.

To clone a UTM policy:

1. Select a UTM policy that you want to clone and select **Clone** from the More link.

NOTE: Alternatively, you can right-click on the selected UTM policy and select **Clone**.

The Clone UTM Policies page appears with editable fields. For more information on the fields, see [“Add a UTM Policy” on page 793](#).

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

A cloned UTM policy is created for the selected UTM policy. By default, the name of the cloned UTM policy is in the format: **<UTM policy name>_clone**.

RELATED DOCUMENTATION

[About the UTM Policies Page | 791](#)

[Edit a UTM Policy | 796](#)

[Delete UTM Policy | 797](#)

Edit a UTM Policy

You are here: **Security Services > UTM > UTM Policies**.

To edit a UTM policy:

1. Select an existing UTM policy that you want to edit on the UTM Policy page.
2. Click the pencil icon available on the upper right side of the page.

The Edit UTM Policy page appears with editable fields. For more information on the options, see [“Add a UTM Policy” on page 793](#).

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

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

RELATED DOCUMENTATION

[About the UTM Policies Page | 791](#)

[Delete UTM Policy | 797](#)

Delete UTM Policy

You are here: **Security Services** > **UTM** > **UTM Policies**.

To delete a UTM policy:

1. Select a UTM policy that you want to delete on the UTM Policy page.
2. Click the delete icon available on the upper right side of the page.

NOTE: Alternatively, you can right-click on the selected UTM policy and select **Delete Policy**.

3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the UTM Policies Page | 791](#)

[Clone a UTM Policy | 795](#)

[Add a UTM Policy | 793](#)

IPS Signature Update

IN THIS CHAPTER

- [About the Signature Update Page | 798](#)
- [Download an IPS Signature | 799](#)
- [Install an IPS Signature | 800](#)
- [Check Status of the IPS Signature | 801](#)
- [IPS Signature Download Setting | 802](#)

About the Signature Update Page

You are here: **Security Services > IPS > Signature Update.**

You can download, install, and check status of the latest version of signature database from the security server.

Tasks You Can Perform

You can perform the following tasks from this page:

- Download an IPS signature. See [“Download an IPS Signature” on page 799](#).
- Install an IPS signature. See [“Install an IPS Signature” on page 800](#).
- Check status of the IPS signature. See [“Check Status of the IPS Signature” on page 801](#).
- IPS signature download setting. See [“IPS Signature Download Setting” on page 802](#).

Field Descriptions

[Table 295 on page 799](#) describes the fields on the IPS signature page.

Table 295: Fields on the IPS Signature Page

| Field | Description |
|-------|--|
| Name | Displays the field values for install or download operation. |
| Value | Displays the install or download status of the operation. |

RELATED DOCUMENTATION

[Download an IPS Signature | 799](#)
[Install an IPS Signature | 800](#)
[Check Status of the IPS Signature | 801](#)
[IPS Signature Download Setting | 802](#)

Download an IPS Signature

You are here: **Security Services > IPS > Signature Update.**

To download an IPS signature:

1. Click **Download** on the upper right side of the Signature Update page.
The Security Package Manual Download page appears.
2. Complete the configuration according to the guidelines provided in [Table 296 on page 799](#).
3. Click **OK** to download the package. If you want to cancel the download, click **Cancel**.

Table 296: Fields on the Security Package Manual Download Page

| Field | Action |
|--------------|---|
| URL | Specifies the predefined default URL used by the device to download the signature database. |
| Version | Select the version from the list to specify the version number of the security package from the portal. |
| Full Package | Select the check box to enable the device to download the latest security package with the full set of attack signature tables from the portal. |

NOTE:

- It takes approximately one minute to retrieve the latest available version for download from the security server.
- To configure URL, click **Download Setting**.

RELATED DOCUMENTATION

[About the Signature Update Page | 798](#)

[Install an IPS Signature | 800](#)

[Check Status of the IPS Signature | 801](#)

[IPS Signature Download Setting | 802](#)

Install an IPS Signature

You are here: **Security Services > IPS > Signature Update**.

To download an IPS signature:

1. Click **Install** on the upper right side of the IPS Signature page.
The Install Signature page appears.
2. Complete the configuration according to the guidelines provided in [Table 297 on page 800](#).
3. Click **Install** to install the package. If you want to cancel the install, click **Cancel**.

Table 297: Fields on the Install Configuration Page

| Field | Action |
|--------------------------------------|--|
| Do not set to active after installed | Select the check box to specify whether or not to activate the installed security package. |
| Install | Click Install to install the existing signature database. |

RELATED DOCUMENTATION

| |
|---|
| About the Signature Update Page 798 |
| Download an IPS Signature 799 |
| Check Status of the IPS Signature 801 |
| IPS Signature Download Setting 802 |

Check Status of the IPS Signature

You are here: **Security Services > IPS > Signature Update.**

To check status of an IPS signature:

1. Click **Check Status** on the upper right side of the IPS Signature page.
The Check Status page appears.
2. Complete the configuration according to the guidelines provided in [Table 298 on page 801](#).
3. Click **OK**.

Table 298: Fields on the Check Status Page

| Field | Action |
|-----------------|---|
| Download Status | Shows the security package download status in the message box. Select Download Status from the Check Status list. |
| Install Status | Shows the security package install status in the message box. Select Install Status from the Check Status list. |

RELATED DOCUMENTATION

| |
|---|
| About the Signature Update Page 798 |
| Download an IPS Signature 799 |
| Install an IPS Signature 800 |
| IPS Signature Download Setting 802 |

IPS Signature Download Setting

You are here: **Security Services > IPS > Signature Update.**

To set the parameters of automatic download an IPS signature:

1. Click **Download Setting** on the upper right side of the IPS Signature page.
The Security Package Download Setting page appears.
2. Complete the configuration according to the guidelines provided in [Table 299 on page 802](#).
3. Click **OK** to set the parameters. If you want to cancel the settings, click **Cancel**.

Table 299: Fields on the Download Setting Page

| Field | Action |
|------------------------------|---|
| URL Setting | |
| URL | <p>Enter a URL to specify the URL to be used by the device to download the signature database.</p> <p>NOTE: The default URL is https://services.netscreen.com/cgi-bin/index.cgi.</p> |
| Proxy Profile | <p>Select an option from the list or create a new proxy profile inline.</p> <p>To create a new proxy profile inline:</p> <ol style="list-style-type: none"> 1. Click Create. Create Proxy Profile page appears. 2. Enter the following details: <ul style="list-style-type: none"> ● Profile Name—Enter a unique proxy profile name. ● Connection Type: <ul style="list-style-type: none"> ● Server IP—Enter the IP address of the server. ● Host Name—Enter the host name. ● Port Number—Select the port number by using top/down arrows. Range: 0 through 65535. 3. Click OK. |
| Auto Download Setting | |
| Interval | Enter an integer to specify the time interval for automatic download. |

Table 299: Fields on the Download Setting Page *(continued)*

| Field | Action |
|------------------------|--|
| Start Time | Specifies that the latest policy templates are to be installed from the portal. Enter a time value in YYYY-MM-DD HH:MM:SS format. |
| Enable Schedule Update | Select the check box to activate automatic download settings. |
| Reset Setting | Click Reset Setting to reset the values. |

RELATED DOCUMENTATION

[About the Signature Update Page | 798](#)

[Download an IPS Signature | 799](#)

[Install an IPS Signature | 800](#)

[Check Status of the IPS Signature | 801](#)

IPS Sensor

IN THIS CHAPTER

- About the Sensor Page | 804

About the Sensor Page

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 300 on page 804 describes the fields on the Sensor page.

Table 300: Fields on the Sensor Page

| Field | Description |
|------------------------|--|
| Basic Settings | Select to configure basic IPS sensor 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. |
| Intelligent Inspection | |
| IDP By Pass | Enable or disable the IDP Intelligent Bypass option. |

Table 300: Fields on the Sensor Page (*continued*)

| Field | Description |
|---------------------------|--|
| IDP By Pass CPU Threshold | <p>Enter the threshold value.</p> <p>Range: 0 through 99. Default value: 85.</p> |
| IDP By Pass CPU Tolerance | <p>Enter the CPU tolerance value.</p> <p>Range: 1 through 99. Default value: 5.</p> |
| 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 300: Fields on the Sensor Page (continued)

| Field | Description |
|--------------------------|--|
| Memory Upper Threshold | Enter the memory upper threshold limit percentage. Range: 1 through 100. |
| Flow | |
| 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. |
| Packet Log | |
| IP Address | Enter the IP address of the destination host to send packet log. |
| Port | Enter the UDP port number. Range: 0 through 65535. |
| Source Address | Enter the source IP address used to transport packet log to a host. |
| Advanced Settings | |
| 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. |
| 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. |

Table 300: Fields on the Sensor Page (*continued*)

| Field | Description |
|---------------------------------|--|
| Reject Timeout | <p>Enter a value to specify the amount of time in milliseconds within which a response must be received.</p> <p>Range: 1 through 65,535 seconds. Default value is 300 seconds.</p> |
| 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 | <p>Enter a value to specify the limit IDP memory usage at this percent of available memory.</p> <p>Range: 10 through 90 percent.</p> |
| 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. |
| 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 | <p>Enter an integer to specify a port on which the sensor executes protocol decoders.</p> <p>Range: 0 through 65535.</p> |

Table 300: Fields on the Sensor Page (*continued*)

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

Table 300: Fields on the Sensor Page (*continued*)

| Field | Description |
|--------------------|--|
| 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 | |
| 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 + and enter the following fields. |
| 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 Policy Page](#) | 810

IPS Policy

IN THIS CHAPTER

- [About the Policy Page | 810](#)
- [IDP Policy Template | 812](#)
- [Check Status of the IDP Policy | 813](#)
- [Add an IDP Policy | 813](#)
- [Clone an IDP Policy | 816](#)
- [Edit an IDP Policy | 817](#)
- [Delete IDP Policy | 817](#)

About the Policy Page

You are here: **Security Services > IPS > Policy.**

Use this page to configure IPS policies.

Tasks You Can Perform

You can perform the following tasks from this page:

- Download, install, load and unload a template. See [“IDP Policy Template” on page 812.](#)
- Check status of the IDP policy. See [“Check Status of the IDP Policy” on page 813.](#)
- Set an IPS policy as default policy. To do this, select an existing IPS policy and click **Set Default**.
- Create an IDP policy. See [“Add an IDP Policy” on page 813.](#)
- Edit an IDP policy. See [“Edit an IDP Policy” on page 817.](#)
- Delete an IDP policy. See [“Delete IDP Policy” on page 817.](#)
- Clone an IDP policy. See [“Clone an IDP Policy” on page 816.](#)

Field Descriptions

Table 301 on page 811 describes the fields on the IDP policy page.

Table 301: Fields on the IDP Policy Page

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

Policy List

NOTE: IDP policies that are created by root users in root-logical-system are not displayed in security profile advanced settings if you have logged in as a logical system user.

| | |
|--------------------|---|
| Name | Displays the IDP policy name. |
| Type | Displays the IDP policy type. |
| IPS Rule Number | Displays the number of rule based IP profiles that are configured. |
| Exempt Rule Number | Displays the number of rule based exempt profiles that are configured. |
| Rulebase-IPS | Displays the IPS rulebase to detect attacks based on stateful signature and protocol anomalies. |
| Rulebase-Exempt | Displays the exempt rulebase to skip detection of a set of attacks in certain traffic. |

Release History Table

| Release | Description |
|------------------------|--|
| 18.3R1 | IDP policies that are created by root users in root-logical-system are not displayed in security profile advanced settings if you have logged in as a logical system user. |

RELATED DOCUMENTATION

| |
|--|
| IDP Policy Template 812 |
| Check Status of the IDP Policy 813 |
| Add an IDP Policy 813 |
| Edit an IDP Policy 817 |
| Delete IDP Policy 817 |
| Clone an IDP Policy 816 |

IDP Policy Template

You are here: **Security Services > IPS > Policy.**

To download, install, load, and unload an IDP policy template:

1. Click **Template** on the upper right side of the Policy page.
The IDP policy template options appear.
2. [Table 302 on page 812](#) describes the fields on the IDP Policy Template page.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 302: Template Details

| Field | Action |
|-------------------|---|
| Download Template | <p>Downloads a template from the server.</p> <p>NOTE:</p> <ul style="list-style-type: none">• New template will overwrite existing predefined policies. Click OK to install the new template.• To configure URL, navigate to Security > IPS > Signature Update and click Download Setting. |
| Install Template | Installs the template to the router. |
| Load Template | Loads the predefined policies to the policy list. |
| Unload Template | Unloads the predefined policies from the policy list. |

RELATED DOCUMENTATION

- [About the Policy Page | 810](#)
- [Check Status of the IDP Policy | 813](#)
- [Add an IDP Policy | 813](#)
- [Edit an IDP Policy | 817](#)
- [Delete IDP Policy | 817](#)
- [Clone an IDP Policy | 816](#)

Check Status of the IDP Policy

You are here: **Security Services > IPS > Policy.**

To check status of the IDP policy:

1. Click **Check Status** on the upper right side of the Policy page.
The Check Status option appears.
2. [Table 303 on page 813](#) describes the fields on the IDP Policy Check Status page.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 303: Check Status Details

| Field | Action |
|-----------------|---|
| Download Status | Displays downloads status information from the Check Status list. |
| Install Status | Displays installs status information from the Check Status list. |

RELATED DOCUMENTATION

- [About the Policy Page | 810](#)
- [IDP Policy Template | 812](#)
- [Add an IDP Policy | 813](#)
- [Edit an IDP Policy | 817](#)
- [Delete IDP Policy | 817](#)
- [Clone an IDP Policy | 816](#)

Add an IDP Policy

You are here: **Security Services > IPS > Policy.**

To add an IDP policy:

1. Click the add icon (+) on the upper right side of the Policy page.
The Add IDP Policy page appears.

2. Complete the configuration according to the guidelines provided in [Table 304 on page 814](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 304: Fields on the Add IDP Policy Page

| Field | Action |
|------------------|--|
| Policy Name | Enter the name of the IPS policy. |
| IPS Rule | <p>Specifies the IPS rule created.</p> <p>Select an option from the list:</p> <ul style="list-style-type: none"> ● Add—Adds a new IPS rule. ● Edit—Edits the selected IPS rule. ● Delete—Deletes the selected record. ● Move—Organize rows. Select Move up, Move down, Move to top, or Move to down. |
| Basic | |
| Policy Name | Displays the name of the IDP policy. |
| Rule Name | Enter a rule name. |
| Rule Description | Enter the description for the rule. |
| Action | Select a rule action from the list to specify the list of all the rule actions for IDP to take when the monitored traffic matches the attack objects specified in the rules. |
| Application | <p>Specifies the list of one or multiple configured applications.</p> <p>Select the applications to be matched.</p> |
| Attack Type | <p>Specifies the attack type that you do not want the device to match in the monitored network traffic. The options available are:</p> <ul style="list-style-type: none"> ● Predefined Attacks ● Predefined Attack Groups <p>Select an option from the list and click the right arrow to match an attack object or attack group to the rule.</p> |
| Category | Select a category from the list to specify the category used for scrutinizing rules of sets. |
| Severity | Select a severity level from the list to specify the rule severity levels in logging to support better organization and presentation of log records on the log server. |

Table 304: Fields on the Add IDP Policy Page (continued)

| Field | Action |
|---|---|
| Direction | Select a direction level from the list to specify the direction of network traffic you want the device to monitor for attacks. |
| Search | Enables you to search a specific data from the list. |
| Advanced | |
| NOTE: This tab is not available for Rulebase exempt. | |
| IP Action | Specifies the action that IDP takes against future connections that use the same IP address. Select an IP action from the list. |
| IP Target | Select an IP target from the list. |
| Timeout | Specifies the number of seconds the IP action should remain effective before new sessions are initiated within that specified timeout value. Enter the timeout value, in seconds. The maximum value is 65,535 seconds. |
| Log IP Action | Select the check box to specify whether or not the log attacks are enabled to create a log record that appears in the log viewer. |
| Enable Attack Logging | Select the check box to specify whether or not the configuring attack logging alert is enabled. |
| Set Alert Flag | Select the check box to specify whether or not an alert flag is set. |
| Severity | Select an option from the list to specify the rule severity level. |
| Terminal | Select the check box to specify whether or not the terminal rule flag is set. |
| Match | |
| From Zone | Select the match criteria for the source zone for each rule. |
| To Zone | Select the match criteria for the destination zone for each rule. |

Table 304: Fields on the Add IDP Policy Page (*continued*)

| Field | Action |
|---------------------|---|
| Source Address | <p>Select the zone exceptions for the from-zone and source address for each rule. The options available are:</p> <ul style="list-style-type: none"> • Match—Matches the from-zone and source address/address sets to the rule. • Except—Enables the exception criteria. |
| Destination Address | <p>Select the zone exceptions for the to-zone and destination address for each rule. The options available are:</p> <ul style="list-style-type: none"> • Match—Matches the from-zone and destination address/address sets to the rule. • Except—Enables the exception criteria. |

RELATED DOCUMENTATION

[About the Policy Page | 810](#)
[IDP Policy Template | 812](#)
[Check Status of the IDP Policy | 813](#)
[Edit an IDP Policy | 817](#)
[Delete IDP Policy | 817](#)
[Clone an IDP Policy | 816](#)

Clone an IDP Policy

You are here: **Security Services > IPS > Policy.**

To clone an IDP policy:

1. Select an IDP policy that you want to clone and click **Clone** on the upper right side of the page.

NOTE: Alternatively, you can right-click on the selected IDP policy and select **Clone**.

The Clone IDP Policy page appears with editable fields. For more information on the fields, see [“Add an IDP Policy” on page 813](#).

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

RELATED DOCUMENTATION

| |
|--|
| About the Policy Page 810 |
| IDP Policy Template 812 |
| Check Status of the IDP Policy 813 |
| Add an IDP Policy 813 |
| Edit an IDP Policy 817 |
| Delete IDP Policy 817 |

Edit an IDP Policy

You are here: **Security Services > IPS > Policy.**

To edit an IDP policy:

1. Select an existing IDP policy that you want to edit on the IPS Policy page.
2. Click the pencil icon available on the upper right side of the page.

The Edit IDP Policy page appears with editable fields. For more information on the options, see [“Add an IDP Policy” on page 813.](#)

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

RELATED DOCUMENTATION

| |
|--|
| About the Policy Page 810 |
| IDP Policy Template 812 |
| Check Status of the IDP Policy 813 |
| Add an IDP Policy 813 |
| Delete IDP Policy 817 |
| Clone an IDP Policy 816 |

Delete IDP Policy

You are here: **Security Services > IPS > Policy.**

To delete an IDP policy:

- 1. Select an IDP policy that you want to delete on the IPS Policy page.
- 2. Click the delete icon available on the upper right side of the page.
- 3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

| |
|--|
| About the Policy Page 810 |
| IDP Policy Template 812 |
| Check Status of the IDP Policy 813 |
| Add an IDP Policy 813 |
| Edit an IDP Policy 817 |
| Clone an IDP Policy 816 |

ALG

IN THIS CHAPTER

- About the ALG Page | 819

About the ALG Page

You are here: **Security Services** > **ALG**.

Use this page to configure Application Layer Gateway (ALG).

Field Descriptions

Table 305 on page 819 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 305: Fields on the ALG Page

| Field | Description |
|-------------|---|
| Main | |
| Enable PPTP | Select the check box to enable the Point-to-Point Tunneling Protocol (PPTP) for ALG. 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. |
| Enable RSH | Select the check box to enable RSH for ALG. 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. |
| Enable RTSP | Select the check box to enable the Real-Time Streaming Protocol (RTSP) for ALG. |

Table 305: Fields on the ALG Page (*continued*)

| Field | Description |
|-------------------------------|---|
| 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> |
| Doctoring | <p>Select one of the following options:</p> <ul style="list-style-type: none"> • Sanity Check—Performs only DNS ALG sanity checks. • None—Disables all DNS ALG doctoring. |
| Maximum Message length | <p>Select a number to specify the maximum DNS message length.</p> <p>Range: 512 through 8192 bytes.</p> |
| Enable Oversize message drop. | <p>Select the check box to enable oversize message drop.</p> |
| FTP | |

Table 305: Fields on the ALG Page (*continued*)

| Field | Description |
|----------------------------------|--|
| Enable FTP | <p>Select the check box to enable the File Transfer Protocol (FTP) for ALG.</p> <p>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.</p> |
| 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 | <p>Select the check box to enable line-break-extension.</p> <p>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).</p> |
| H323 | |
| Enable H323 | Select the check box to enable the H.323 ALG. |

Table 305: Fields on the ALG Page (*continued*)

| Field | Description |
|--------------------|---|
| 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. 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. • 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. 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. 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. • Enable Permit Routed—Select the check box to specify 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. |
| 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> |
| 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. |

Table 305: Fields on the ALG Page (*continued*)

| Field | Description |
|---------------------------|---|
| 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> |
| 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 NTFY from the gateway to the call agent or a 200 OK from the call agent to the gateway. The device tracks these transactions and clears them when they time out.</p> |

Table 305: Fields on the ALG Page (*continued*)

| Field | Description |
|-------------------------|---|
| 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. 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. • Connection Flood Threshold—Enter a value from 2 through 10,000. Limits the number of new connection requests allowed per Media Gateway (MG) per second. Messages exceeding the ALG. • 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. 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. • Enable Permit Routed—Select the check box. Specifies that unknown messages be allowed to pass if the session is in route mode. (Sessions in transparent mode are treated as route mode.) |
| DSCP Code Rewrite | <p>Specifies a code-point alias or bit set to apply to a forwarding class for a rewrite rule.</p> <p>Code Point—Enter a six-bit DSCP code point value.</p> |
| MSRPC | |
| Enable MSRPC | <p>Select the check box to enable the MSRPC.</p> <p>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.</p> |
| 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. |

Table 305: Fields on the ALG Page (*continued*)

| Field | Description |
|--------------------------------------|--|
| SCCP | |
| Enable SCCP | Select the check box to enable the Skinny Client Control Protocol. |
| Inactive Media Timeout | <p>Select a value from 10 through 600 seconds.</p> <p>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.</p> |
| Application Screen | <p>Call Flood Threshold—Select a value from 2 through 1,000.</p> <p>Protects SCCP ALG clients from flood attacks by limiting the number of calls they attempt to process.</p> |
| Action On Receiving Unknown Messages | <ul style="list-style-type: none"> • Enable Permit NAT Applied—Select the check box. Specifies how unidentified SCCP messages are handled by the device. The default is to drop unknown (unsupported) messages. Permitting unknown messages can compromise security and is not recommended. However, in a secure test or production environment, this statement can be useful for resolving interoperability issues with disparate vendor equipment. By permitting unknown SCCP (unsupported) messages, you can get your network operational and later analyze your VoIP traffic to determine why some messages were being dropped. This statement applies only to received packets identified as supported VoIP packets. If a packet cannot be identified, it is always dropped. If a packet is identified as a supported protocol, the message is forwarded without processing. • Enable Permit Routed—Select the check box. 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.) |
| 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> |

Table 305: Fields on the ALG Page (*continued*)

| Field | Description |
|------------------------|--|
| 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> |
| 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 305: 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. 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. • 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. Specifies the time (in seconds) to make an attack table entry for each INVITE, which is listed in the application screen. • Enable Attack Protection—Select one of the options: All Servers, Selected Servers, or None. Protects servers against INVITE attacks. Configures the SIP application screen to protect the server at some or all destination IP addresses against INVITE attacks. 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. |
| 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> |
| 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. |

Advanced Threat Prevention

IN THIS CHAPTER

- [About the Advanced Threat Prevention Page | 828](#)
- [Add a Threat Prevention Policy | 830](#)
- [Edit a Threat Prevention Policy | 831](#)
- [Delete Threat Prevention Policy | 832](#)

About the Advanced Threat Prevention Page

You are here: **Security Services > Advanced Threat Prevention.**

You can view and configure threat prevention policies. Threat prevention policies provide protection and monitoring for configured threat profiles, including command and control server, infected hosts, and malware. Using threat intelligence feeds in policies, ingress and egress traffic is monitored for suspicious content and behavior.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a threat prevention policy. See [“Add a Threat Prevention Policy” on page 830](#).
- Edit a threat prevention policy. See [“Edit a Threat Prevention Policy” on page 831](#).
- Delete a threat prevention policy. See [“Delete Threat Prevention Policy” on page 832](#).
- Filter the threat prevention policies based on select criteria. To do this, select the filter icon at the top right-hand corner of the Threat Prevention Policies 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 Threat Prevention Policies table. To do this, use the Show Hide Columns icon in the top right corner of the page and select the options you want to show or deselect to hide options on the page.
- Advance search for threat prevention 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 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 306 on page 829 describes the fields on the Threat Prevention Policies page.

Table 306: Fields on the Threat Prevention Policies Page

| Field | Description |
|---------------|---|
| Name | <p>Enter a threat prevention policy name.</p> <p>Name must begin with an alphanumeric character; dashes and underscores are allowed; cannot exceed 63 characters.</p> |
| C&C Server | Displays the range value of threat score set for this policy on a C&C server. A C&C profile would provide information on C&C servers that have attempted to contact and compromise hosts on your network. If the threat score of a feed is between this range, the feed will be blocked or permitted based on the threat score. |
| Infected Host | Displays the range value of threat score set for this policy if . An infected host profile would provide information on compromised hosts and their associated threat levels. |
| Malware HTTP | A malware profile would provide information on files downloaded by hosts and found to be suspicious based on known signatures or URLs. |
| Malware SMTP | A malware profile would provide information on files downloaded by hosts and found to be suspicious based on known signatures or URLs. |

Table 306: Fields on the Threat Prevention Policies Page (*continued*)

| Field | Description |
|-------------|---|
| Log | All traffic is logged by default. Use the pulldown to narrow the types of traffic to be logged. |
| Description | Enter a description for the threat prevention policy. |

RELATED DOCUMENTATION

[Add a Threat Prevention Policy | 830](#)
[Edit a Threat Prevention Policy | 831](#)
[Delete Threat Prevention Policy | 832](#)

Add a Threat Prevention Policy

You are here: **Security Services > Advanced Threat Prevention.**

To add a threat prevention policy:

1. Click the add icon (+) on the upper right side of the Threat Prevention Policy page.
The Create Threat Prevention Policy page appears.
2. Complete the configuration according to the guidelines provided in [Table 307 on page 830](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 307: Fields on the Create Threat Prevention Policy Page

| Field | Action |
|---|--|
| Name | Displays the threat prevention policy name. |
| Description | Displays the threat prevention policy description. |
| Profiles | |
| Include C&C profile in policy | Select the check box. |
| Include infected host profile in policy | Select the check box. |

Table 307: Fields on the Create Threat Prevention Policy Page (*continued*)

| Field | Action |
|-----------------------------------|--|
| Include malware profile in policy | Select the check box. |
| Log Setting | |
| Log Setting | Select an option from the list. The available options are: <ul style="list-style-type: none"> • Log all traffic • Log only blocked traffic • Do not log any traffic |

RELATED DOCUMENTATION

[About the Advanced Threat Prevention Page | 828](#)
[Edit a Threat Prevention Policy | 831](#)
[Delete Threat Prevention Policy | 832](#)

Edit a Threat Prevention Policy

You are here: **Security Services > Advanced Threat Prevention.**

To edit a threat prevention policy:

1. Select the existing a threat prevention that you want to edit on the Threat Prevention Policies page.
2. Click the pencil icon available on the upper right side of the page.

The Edit a Threat Prevention page appears with editable fields. For more information on the options, see [“Add a Threat Prevention Policy” on page 830](#).

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

RELATED DOCUMENTATION

[About the Advanced Threat Prevention Page | 828](#)
[Add a Threat Prevention Policy | 830](#)

Delete Threat Prevention Policy

You are here: **Security Services** > **Advanced Threat Prevention**.

To delete a threat prevention policy:

1. Select a threat prevention policy that you want to delete on the Threat Prevention Policies page.
2. Click the delete icon available on the upper right side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the Advanced Threat Prevention Page | 828](#)

[Add a Threat Prevention Policy | 830](#)

[Edit a Threat Prevention Policy | 831](#)

SSL Initiation Profiles

IN THIS CHAPTER

- [About the SSL Initiation Profile Page | 833](#)
- [Add an SSL Initiation Profile | 835](#)
- [Edit an SSL Initiation Profile | 837](#)
- [Delete SSL Initiation Profile | 838](#)

About the SSL Initiation Profile Page

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 835](#).
- Edit an SSL initiation profile. See [“Edit an SSL Initiation Profile” on page 837](#).
- Delete SSL initiation profile. See [“Delete SSL Initiation Profile” on page 838](#).
- Show or hide columns in the SSL Initiation Profile table. To do this, use the Show Hide Columns icon in the top right corner of the page and select the options you want to show or deselect to hide options on the page.
- 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 308 on page 834 describes the fields on the SSL Initiation Profile page.

Table 308: 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. |
| 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 835 |
| Edit an SSL Initiation Profile 837 |
| Delete SSL Initiation Profile 838 |

Add an SSL Initiation Profile

You are here: **Security Services > SSL Profiles > SSL Initiation.**

To add an SSL initiation profile:

1. Click the add icon (+) on the upper right side of the SSL Initiation Profile page.
The Create SSL Initiation Profile page appears.
2. Complete the configuration according to the guidelines provided in [Table 309 on page 835](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 309: Fields on the Create SSL Initiation Profile Page

| Field | Action |
|----------------------------|--|
| General Information | |
| Name | Enter a unique name of the SSL initiation profile. The string must consist of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed; maximum length is 63 characters. |
| Flow Tracing | Select this option to enable flow trace for troubleshooting policy-related issues for this profile. |
| Protocol Version | Specifies the accepted protocol SSL version. Select the protocol from the list: None, All, TLSv1, TLSv1.1, or TLSv1.2. |
| Preferred Cipher | Specify the cipher depending on their key strength. Select a preferred cipher from the list: <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. |

Table 309: Fields on the Create SSL Initiation Profile Page (*continued*)

| Field | Action |
|-------------------------------|---|
| 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 | Select this option to enable SSL session cache. |
| Certificate | |
| 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 309: 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 | 833](#)

[Edit an SSL Initiation Profile | 837](#)

[Delete SSL Initiation Profile | 838](#)

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 side 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 835](#).

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

RELATED DOCUMENTATION

[About the SSL Initiation Profile Page | 833](#)

[Add an SSL Initiation Profile | 835](#)[Delete SSL Initiation Profile | 838](#)

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 side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the SSL Initiation Profile Page | 833](#)[Add an SSL Initiation Profile | 835](#)

[Edit an SSL Initiation Profile | 837](#)

SSL Proxy Profiles

IN THIS CHAPTER

- [About the SSL Proxy Page | 839](#)
- [Add an SSL Proxy Profile | 841](#)
- [Clone an SSL Proxy Profile | 848](#)
- [Edit an SSL Proxy Profile | 849](#)
- [Delete SSL Proxy Profile | 849](#)

About the SSL Proxy Page

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 of the table and enter the session cache timeout in seconds.
- Add an SSL proxy profile. See [“Add an SSL Proxy Profile” on page 841](#).
- Edit an SSL proxy profile. See [“Edit an SSL Proxy Profile” on page 849](#).
- Delete SSL proxy profile. See [“Delete SSL Proxy Profile” on page 849](#).
- Clone an SSL proxy profile. See [“Clone an SSL Proxy Profile” on page 848](#).
- 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 top 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 310 on page 840 describes the fields on the SSL Proxy page.

Table 310: 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. |

Table 310: Fields on the SSL Proxy Page (*continued*)

| Field | Description |
|---------------------|--|
| 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 allowlists 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](#) | 841

Add an SSL Proxy Profile

You are here: **Security Services** > **SSL Profiles** > **SSL Proxy**.

To add an SSL proxy profile:

1. Click the add icon (+) on the upper right side of the SSL Proxy Profile page.
The Create SSL Proxy Profile page appears.
2. Complete the configuration according to the guidelines provided in [Table 311 on page 842](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 311: 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 311: Fields on the Create SSL Proxy Profile Page *(continued)*

| Field | Action |
|----------------|--------|
| Custom Ciphers | |

Table 311: Fields on the Create SSL Proxy Profile Page (*continued*)

| Field | Action |
|-------|--|
| | <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. rsa-with-RC4-128-md5—RSA, 128-bit RC4, MD5 hash 2. rsa-with-RC4-128-sha—RSA, 128-bit RC4, SHA hash 3. rsa-with-des-cbc-sha—RSA, DES/CBC, SHA hash 4. rsa-with-3DES-edc-cbc-sha—RSA, 3DES EDE/CBC, SHA hash 5. rsa-with-aes-128-cbc-sha—RSA, 128-bit AES/CBC, SHA hash 6. rsa-with-aes-256-cbc-sha—RSA, 256-bit AES/CBC, SHA hash 7. rsa-export-with-rc4-40-md5—RSA-export, 40-bit RC4, MD5 hash 8. rsa-export-with-des40-cbc-sha—RSA-export, 40-bit DES/CBC, SHA hash 9. rsa-with-aes-256-gcm-sha384—RSA, 256-bit AES/GCM, SHA384 hash 10. rsa-with-aes-256-cbc-sha256—RSA, 256-bit AES/CBC, SHA256 hash 11. rsa-with-aes-128-gcm-sha256—RSA, 128-bit AES/GCM, SHA256 hash 12. rsa-with-aes-128-cbc-sha256—RSA, 256-bit AES/CBC, SHA256 hash 13. ecdhe-rsa-with-aes-256-gcm-sha384—ECDHE, RSA, 256-bit AES/GCM, SHA384 hash 14. ecdhe-rsa-with-aes-256-cbc-sha—ECDHE, RSA, 256-bit AES/CBC, SHA hash 15. ecdhe-rsa-with-aes-256-cbc-sha384—ECDHE, RSA, 256-bit AES/CBC, SHA384 hash 16. ecdhe-rsa-with-aes-3des-edc-cbc-sha—ECDHE, RSA, 3DES, EDE/CBC, SHA hash 17. ecdhe-rsa-with-aes-128-gcm-sha256—ECDHE, RSA, 128-bit AES/GCM, SHA256 hash 18. ecdhe-rsa-with-aes-128-cbc-sha—ECDHE, RSA, |

Table 311: Fields on the Create SSL Proxy Profile Page (*continued*)

| Field | Action |
|---------------------------------|---|
| | <p>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 Device 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> |
| 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> |

Table 311: Fields on the Create SSL Proxy Profile Page (*continued*)

| Field | Action |
|-------------------------|---|
| Exempted Addresses | <p>Specifies addresses to create allowlists 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 allowlists.</p> |
| Exempted URL Categories | <p>Specifies URL categories to create allowlists 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 | |
| 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> |

Table 311: Fields on the Create SSL Proxy Profile Page (*continued*)

| Field | Action |
|-------------------------|---|
| 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 (allowlisted, Allowed, Dropped, or Ignored).</p> |
| 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 | <p>Select the check box if you want to revoke the certificate.</p> |
| 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> |

Table 311: Fields on the Create SSL Proxy Profile Page (*continued*)

| Field | Action |
|--|--|
| Hold Instruction Code | Select Ignore if you want to keep the instruction code on hold. |
| Mirror Decrypt Traffic | |
| Interface | Select an SSL decryption port mirroring interface from the list. This is an Ethernet interface on SRX Series device 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 | 839](#)
[Edit an SSL Proxy Profile | 849](#)
[Delete SSL Proxy Profile | 849](#)
[Clone an SSL Proxy Profile | 848](#)

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 841](#).

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

RELATED DOCUMENTATION

[About the SSL Proxy Page | 839](#)

[Edit an SSL Proxy Profile | 849](#)

[Delete SSL Proxy Profile | 849](#)

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 side 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 841](#).

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

RELATED DOCUMENTATION

[About the SSL Proxy Page | 839](#)

[Delete SSL Proxy Profile | 849](#)

[Clone an SSL Proxy Profile | 848](#)

Delete SSL Proxy Profile

You are here: **Security Services > SSL Profiles > SSL Proxy**.

To delete SSL proxy profile:

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 side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

| |
|--|
| About the SSL Proxy Page 839 |
| Add an SSL Proxy Profile 841 |
| Edit an SSL Proxy Profile 849 |
| Clone an SSL Proxy Profile 848 |

Firewall Authentication—Access Profile

IN THIS CHAPTER

- [About the Access Profile Page | 851](#)
- [Add an Access Profile | 853](#)
- [Edit an Access Profile | 858](#)
- [Delete an Access Profile | 858](#)

About the Access Profile Page

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 853](#).
- Edit an access profile. See [“Edit an Access Profile” on page 858](#).
- Delete an access profile. See [“Delete an Access Profile” on page 858](#).
- 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 top 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 312 on page 852 describes the fields on the Access Profile page.

Table 312: Fields on the Access Profile Page

| Field | Description |
|--------------|--|
| Profile Name | Displays the name of an access profile. |
| 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. |

Table 312: Fields on the Access Profile Page (*continued*)

| Field | Description |
|----------------|---|
| RADIUS Servers | Displays the RADIUS server configuration. |

RELATED DOCUMENTATION

[Add an Access Profile | 853](#)
[Edit an Access Profile | 858](#)
[Delete an Access Profile | 858](#)

Add an Access Profile

You are here: **Security Services > Firewall Authentication > Access Profile.**

To add an access profile:

1. Click the add icon (+) on the upper right-side of the Access Profile page.
The Create Access Profile page appears.
2. Complete the configuration according to the guidelines provided in [Table 313 on page 853](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 313: Fields on the Access Profile Page

| Field | Description |
|-----------------------|---|
| Access Profile 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 | Select an address pool from the list that can be used by different client applications. 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 861 . |
| Authentication | |

Table 313: Fields on the Access Profile Page *(continued)*

| Field | Description |
|-------|---|
| 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 +. <p>The Create Local Authentication User page appears.</p> <ol style="list-style-type: none">Enter the following details:<ul style="list-style-type: none">User Name—Enter the username 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 313: 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. • Retry—Enter the number of retries that a device can attempt to contact a RADIUS server. Range is 1 through 100 seconds. • Routing Instance—Select the routing instance from the list for managing the routing instance. • Source Address—Enter a source IP address configured on one of the device's interfaces. • 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. 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 313: 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"> Click +. The Create LDAP Server page appears. 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. Retry—Enter the number of retries that a device can attempt to contact an LDAP server. Range is 1 through 10 seconds. Routing Instance—Select the routing instance from the list for managing the routing instance. Source Address—Enter a source IP address configured on one of the device's interfaces. 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. Click OK to save changes. <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> |

Table 313: Fields on the Access Profile Page (*continued*)

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

Authentication Order

| | |
|---------|---|
| 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 device 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 | 851](#)[Edit an Access Profile | 858](#)[Delete an Access Profile | 858](#)

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-side 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 853](#).

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

RELATED DOCUMENTATION

[About the Access Profile Page | 851](#)[Add an Access Profile | 853](#)[Delete an Access Profile | 858](#)

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-side of the page.
3. Click **Yes** to delete access profiles or click **No** to retain access profiles.

RELATED DOCUMENTATION

[About the Access Profile Page | 851](#)

[Add an Access Profile | 853](#)

[Edit an Access Profile | 858](#)

Firewall Authentication—Address Pools

IN THIS CHAPTER

- [About the Address Pools Page | 860](#)
- [Add an Address Pool | 861](#)
- [Edit an Address Pool | 863](#)
- [Delete Address Pool | 863](#)
- [Search for Text in an Address Pools Table | 864](#)

About the Address Pools Page

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 861.](#)
- Edit Address Pool. See [“Edit an Address Pool” on page 863.](#)
- Delete Address Pool. See [“Delete Address Pool” on page 863.](#)
- Search for Text in an Address Pools table. See [“Search for Text in an Address Pools Table” on page 864.](#)
- 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 **Action_Detail_View**.

- Filter the address pool based on select criteria. To do this, select the filter icon at the top right-hand 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 top right corner of the page and select the options you want to show or deselect to hide options on the page.

Field Descriptions

Table 314 on page 861 describes the fields on the Address Pools page.

Table 314: Fields on the Address Pools Page

| Field | Description |
|-----------------|---|
| Name | Specifies the name of the address pool. |
| Network Address | Specifies the network address used by the address pool. |
| 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. |
| Address Range | Specifies the name of the address range. |

RELATED DOCUMENTATION

| |
|---|
| Add an Address Pool 861 |
| Edit an Address Pool 863 |
| Delete Address Pool 863 |
| Search for Text in an Address Pools Table 864 |

Add an Address Pool

You are here: Security Services > Firewall Authentication > Address Pools.

To add an address pool:

1. Click the add icon (+) on the upper right side of the Address Pools page.
The Create Address Pool page appears.
2. Complete the configuration according to the guidelines provided in [Table 315 on page 862](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 315: Fields on the Create Address Pool Page

| Field | Description |
|-------------------------|---|
| General | |
| Pool Name | Enter the address pool name. |
| Network Address | Enter an IPv4 address for the address pool. |
| XAUTH Attributes | |
| Primary DNS Server | Enter the primary-dns IPv4 address. |
| Secondary DNS Server | Enter the secondary-dns IPv4 address. |
| Primary WINS Server | Enter the primary-wins IPv4 address. |
| Secondary WINS Server | Enter the secondary-wins IPv4 address. |
| Address Ranges | |
| Add | Click + to add a new address range for the address pool. |
| Name | Enter a name for the IP address range. |
| Lower Limit | Enter the lower limit of the address range. |
| High Limit | Enter the upper limit of the address range. |
| Delete | Click the delete icon to delete the address range for the address pool. |

RELATED DOCUMENTATION

[About the Address Pools Page | 860](#)

[Edit an Address Pool | 863](#)

[Delete Address Pool | 863](#)

[Search for Text in an Address Pools Table | 864](#)

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 side 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 861](#).

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

RELATED DOCUMENTATION

[About the Address Pools Page | 860](#)

[Add an Address Pool | 861](#)

[Delete Address Pool | 863](#)

[Search for Text in an Address Pools Table | 864](#)

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 side of the page.

3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

| |
|---|
| About the Address Pools Page 860 |
| Add an Address Pool 861 |
| Edit an Address Pool 863 |
| Search for Text in an Address Pools Table 864 |

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 top 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 860 |
| Add an Address Pool 861 |
| Edit an Address Pool 863 |
| Delete Address Pool 863 |

Firewall Authentication Settings

IN THIS CHAPTER

- About the Authentication Settings Page | 865

About the Authentication Settings Page

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:

- Complete the configuration according to the guidelines provided in [Table 316 on page 865](#).
- Click **Save** to save the changes.

[Table 316 on page 865](#) describes the fields on the Firewall Authentication page.

Table 316: 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 | |

Table 316: Fields on the Firewall Authentication Page (*continued*)

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

Table 316: Fields on the Firewall Authentication Page *(continued)*

| Field | Description |
|-----------|---|
| 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](#) | 868

Firewall Authentication—UAC Settings

IN THIS CHAPTER

- About the UAC Settings Page | 868

About the UAC Settings Page

You are here: **Security Services > Firewall Authentication > UAC Settings.**

Use this page to configure UAC Settings.

Field Description

To configure UAC settings:

- Complete the configuration according to the guidelines provided in [Table 317 on page 868](#).
- Click **Save** to save the changes.

[Table 317 on page 868](#) describes the fields on the UAC Setting page.

Table 317: Fields on the UAC Setting Page

| Field | Description |
|-----------------|-------------|
| Global Settings | |

Table 317: 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 | |
| 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. |

Table 317: Fields on the UAC Setting Page (*continued*)

| Field | Description |
|----------------------------|---|
| 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> |
| 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](#) | 720

Firewall Authentication—Active Directory

IN THIS CHAPTER

- About the Active Directory Page | 871

About the Active Directory Page

You are here: **Security Services > Firewall Authentication > Active Directory.**

You can configure Active directory.

[Table 318 on page 871](#) describes the fields on the Active Directory page.

Table 318: 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 device to retrieve address-to-user mapping information. |
| Timeout | |
| Authentication Entry Timeout | <p>Set the timeout to 0 to avoid having the user's entry being removed from the authentication table after the timeout.</p> <p>NOTE: When a user is no longer active, a timer is started for that user's entry in the Active Directory authentication table. When the time is up, the user's entry is removed from the table. Entries in the table remain active as long as there are sessions associated with the entry.</p> <p>The default authentication entry timeout is 30 minutes. Starting in Junos OS Release 19.2R1, the default value is 60 minutes.</p> <p>To disable timeout, set the interval to zero. The range is 10 through 1440 minutes.</p> |

Table 318: Fields on the Active Directory Page *(continued)*

| Field | Description |
|--|---|
| WMI Timeout | <p>Enter the number of seconds that the domain PC has to respond to the SRX Series device's query through Windows Management Instrumentation (WMI) or Distributed Component Object Module (DCOM).</p> <p>If no response is received from the domain PC within the wmi-timeoutinterval, the probe fails and the system either creates an invalid authentication entry or updates the existing authentication entry as invalid. If an authentication table entry already exists for the probed IP address, and no response is received from the domain PC within the wmi-timeout interval, the probe fails and that entry is deleted from the table.</p> <p>The range is 3 through 120 seconds.</p> |
| Invalid Authentication Entry Timeout | <p>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 | |
| Include | <p>Enable to include IP addresses from the Available column.</p> <p>Click the Add icon (+) to create a new IP address and add it as either include or exclude from monitoring.</p> <p>Click the Delete icon to delete a new IP address and add it as either include or exclude from monitoring.</p> |
| Exclude | <p>Enable to exclude IP addresses from the Available column.</p> <p>Click the Add icon (+) to create a new IP address and add it as either include or exclude from monitoring.</p> <p>Click the Delete icon to delete a new IP address and add it as either include or exclude from monitoring.</p> |
| Domain Settings | |

Table 318: Fields on the Active Directory Page (*continued*)

| Field | Description |
|----------------------------------|--|
| Test | Click Test to check the Domain Connection status. test:Status page appears and displays the status. |
| + | Click + to add a domain. The Add Domain page appears. NOTE: <ul style="list-style-type: none"> Starting in Junos OS Release 19.2R1, for SRX4200, SRX1500, SRX550M, and vSRX 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 devices, you can create only one domain. <p>You can select the pencil icon to edit the domain or select delete icon to delete the domain.</p> |
| General | |
| Domain Name | Enter the name of the domain. The range for the domain name is 1 through 64 characters. |
| User Name | Enter the password for the Active Directory account password. The range for the username is 1 through 64 characters. Example: admin |
| Password | Enter the username for the Active Directory account name. The range for the password is 1 through 128 characters. Example: A\$BC123 |
| Domain Controller(s) | |
| Domain Controller(s) | Click the add icon (+) to add domain controller settings. <ul style="list-style-type: none"> Domain Controller Name—Enter the domain controller name. Name can range from 1 through 64 characters. You can configure up to maximum of 10 domain controllers. IP Address—Enter the IP address of the domain controller. |
| User Group Mapping (LDAP) | |

Table 318: Fields on the Active Directory Page *(continued)*

| Field | Description |
|-----------------------------|---|
| User Group Mapping (LDAP) | <p>Click the add icon (+):</p> <ul style="list-style-type: none"> • IP Address—Enter the IP address of the LDAP server. If no address is specified, the system uses one of the configured Active Directory domain controllers. • Port—Enter the port number of the LDAP server. If no port number is specified, the system uses port 389 for plaintext or port 636 for encrypted text. Default value is port 443. |
| Base Distinguish Name | <p>Enter the LDAP base distinguished name (DN).</p> <p>Example: DC=example,DC=net</p> |
| User Name | Enter the username of the LDAP account. If no username is specified, the system will use the configured domain controller's username. |
| Password | Enter the password for the account. If no password is specified, the system uses the configured domain controller's password. |
| Use SSL | Enable Secure Sockets Layer (SSL) to ensure secure transmission with the LDAP server. Disabled by default, then the password is sent in plaintext. |
| Authentication Algorithm | Enable this option to specify the algorithm used while the SRX Series device communicates with the LDAP server. By default simple is selected to configure simple(plaintext) authentication mode. |
| IP User Mapping | |
| Discovery Method (WMI) | <p>Enable the method of discovering IP address-to-user mappings.</p> <p>WMI—Windows Management Instrumentation (WMI) is the discovery method used to access the domain controller. This option should be enabled only for internal hosts or trusted hosts.</p> |
| Event Log Scanning Interval | <p>Enter the scanning interval at which the SRX Series device scans the event log on the domain controller. The range is 5 through 60 seconds.</p> <p>Default value is 60 seconds.</p> |
| Initial Event Log TimeSpan | <p>Enter the time of the earliest event log on the domain controller that the SRX Series device will initially scan. This scan applies to the initial deployment only. After WMIC and the user identification start working, the SRX Series device scans only the latest event log.</p> <p>The range is 1 through 168 hours. Default value is 1 hour.</p> |

Release History Table

| 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 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 devices, you can create only one domain. |

RELATED DOCUMENTATION

| [About the Authentication Priority Page](#) | **879**

Firewall Authentication—Local Authentication

IN THIS CHAPTER

- [About the Local Authentication Page | 876](#)
- [Add a Local Auth Entry | 877](#)
- [Delete a Local Auth Entry | 878](#)

About the Local Authentication Page

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 Auth Entry” on page 877](#).
- Delete a local auth entry. See [“Delete a Local Auth Entry” on page 878](#).
- Clear all the local auth entry. To do this, select the local auth entries you want to clear and click **Clear All** at the top right of the table.

Field Descriptions

[Table 319 on page 876](#) describes the fields on the Local Auth page.

Table 319: 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. |

Table 319: Fields on the Local Auth Page (*continued*)

| Field | Description |
|-----------|---|
| 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 Auth Entry | 877](#)
[Delete a Local Auth Entry | 878](#)

Add a Local Auth Entry

You are here: **Security Services > Firewall Authentication > Local Authentication.**

To add a local auth entry:

1. Click the add icon (+) on the upper right side of the Local Auth page.
The Add Local Auth Entry page appears.
2. Complete the configuration according to the guidelines provided in [Table 320 on page 877](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 320: Fields on the Add Local Auth Page

| Field | Action |
|------------|---|
| IP Address | Enter an IP address for the local authentication. |
| User Name | Enter a username for the local authentication. |

Table 320: Fields on the Add Local Auth Page (continued)

| Field | Action |
|-----------|---|
| 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 | 876
- Delete a Local Auth Entry | 878

Delete a Local Auth Entry

You are here: **Security Services > Firewall Authentication > Local Authentication.**

To delete a local auth entry:

1. Select a local auth entry that you want to delete on the Local Auth Entry page.
2. Click the delete icon available on the upper right side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

- About the Local Authentication Page | 876
- Add a Local Auth Entry | 877

Firewall Authentication—Authentication Priority

IN THIS CHAPTER

- About the Authentication Priority Page | 879

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 321 on page 879](#) describes the fields on the Auth Priority page.

Table 321: Fields on the Auth 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. |
| 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. |

Table 321: Fields on the Auth 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 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 | 876](#)

Firewall Authentication—Identity Management

IN THIS CHAPTER

- [About the Identity Management Page | 881](#)
- [Add an Identity Management Profile | 881](#)
- [Edit an Identity Management Profile | 885](#)
- [Delete Identity Management Profile | 886](#)

About the Identity Management Page

You are here: **Security Services > Firewall Authentication > Identity Management.**

You can add, edit or delete the identity management profiles. You can also view the connection status of this SRX device with the Juniper Identity Management Services (JIMS).

Tasks You Can Perform

You can perform the following tasks from this page:

- Add an identity management profile. See [“Add an Identity Management Profile” on page 881.](#)
- Edit an identity management profile. See [“Edit an Identity Management Profile” on page 885.](#)
- Delete an identity management profile. See [“Delete Identity Management Profile” on page 886.](#)

RELATED DOCUMENTATION

| [Add an Identity Management Profile | 881](#)

Add an Identity Management Profile

You are here: **Security Services > Firewall Authentication > Identity Management.**

To add an identity management profile:

1. Click **Configure** on the identity management page.
The Configure Identity Management Profile page appears.
2. Complete the configuration according to the guidelines provided in [Table 322 on page 882](#).
3. Click **Finish** to save the changes. If you want to discard your changes, click **Cancel**.

Table 322: Fields on the Configure Identity Management Profile Page

| Field | Action |
|------------------------------------|--|
| General Information | |
| General Information | Connection for Primary and Secondary Identity. |
| 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. |
| Primary CA Certificate | Specifies the primary certificate of the JIMS. SRX device will use it to verify JIMS's certificate for SSL connection. Select Upload CA certificate to device or specify the path of the file on device . |
| Primary CA Certificate file upload | Enables you to locate and upload the CA certificate. Click Browse to locate the CA certificate on your device and click Upload the selected CA certificate. |
| Primary CA Certificate file path | Enter a file path of the primary CA certificate. |
| Primary Client ID | Enter a primary client ID of the SRX device to obtain access token. It must be consistent with the configuration of the API client created on JIMS. |

Table 322: Fields on the Configure Identity Management Profile Page (*continued*)

| Field | Action |
|--------------------------------------|--|
| 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 device to obtain access token. It must be consistent with the configuration of the API client created on JIMS.</p> |
| Secondary Identity Management 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> |
| 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> |

Table 322: Fields on the Configure Identity Management Profile Page (*continued*)

| Field | Action |
|---|--|
| 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 | Select the check box if you want to disable the IP query function that is enabled by default. |
| 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 | Select an IP address book from the predefined address book in which an address set must be selected as IP filter. |
| 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> |

Table 322: Fields on the Configure Identity Management Profile Page (*continued*)

| Field | Action |
|-------------------------|---|
| Exclude IP Address Book | Select an IP address book that you want identity management profile to exclude. |
| 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 device. You can specify up to twenty domain names for the filter. |

RELATED DOCUMENTATION

[About the Identity Management Page | 881](#)

[Edit an Identity Management Profile | 885](#)

[Delete Identity Management Profile | 886](#)

Edit an Identity Management Profile

You are here: **Security Services > Firewall Authentication > Identity Management.**

To edit an identity management profile:

1. Select the existing identity management profile that you want to edit on the Identity Management page.
2. Click the pencil icon available on the upper right side of the page.

The Edit an Identity Management Profile page appears with editable fields. For more information on the options, see [“Add an Identity Management Profile” on page 881.](#)

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

RELATED DOCUMENTATION

[About the Identity Management Page | 881](#)

[Add an Identity Management Profile | 881](#)[Delete Identity Management Profile | 886](#)

Delete Identity Management Profile

You are here: **Security Services > Firewall Authentication > Identity Management.**

To delete identity management profile:

1. Select an identity management profile that you want to delete on the Identity Management page.
2. Click the delete icon available on the upper right side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the Identity Management Page | 881](#)[Add an Identity Management Profile | 881](#)[Edit an Identity Management Profile | 885](#)

ICAP Redirect

IN THIS CHAPTER

- [About the ICAP Redirect Profile Page | 887](#)
- [Add an ICAP Redirect Profile | 889](#)
- [Edit an ICAP Redirect Profile | 891](#)
- [Delete ICAP Redirect Profile | 891](#)

About the ICAP Redirect Profile Page

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 889](#).
- Edit an ICAP redirect profile. See [“Edit an ICAP Redirect Profile” on page 891](#).
- Delete an ICAP redirect profile. See [“Delete ICAP Redirect Profile” on page 891](#).
- Filter the ICAP redirect profiles based on select criteria. To do this, select the filter icon at the top right-hand 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 top 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 323 on page 888 describes the fields on the ICAP Redirect Profile page.

Table 323: 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. |
| 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 | 889](#)
- [Edit an ICAP Redirect Profile | 891](#)
- [Delete ICAP Redirect Profile | 891](#)

Add an ICAP Redirect Profile

You are here: **Security Services > ICAP Redirect.**

To add an ICAP redirect profile:

1. Click the add icon (+) on the upper right side of the ICAP Redirect Profiles page.
The Create ICAP Redirect Profile page appears.
2. Complete the configuration according to the guidelines provided in [Table 324 on page 889](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 324: 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. |

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 325 on page 890](#).

Edit—Edit an ICAP Redirect server configuration. Enter information as specified in [Table 325 on page 890](#).

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. |

Table 324: Fields on the Create ICAP Redirect Profile Page (*continued*)

| Field | Action |
|----------------|---|
| Default Action | Select a default action from the list to be taken when there are scenarios other than the above two mentioned ones. |

Table 325: Fields on the Create ICAP Redirect Server Page

| Field | Action |
|-----------------------|---|
| Name | <p>Enter an ICAP Redirect server name.</p> <p>The string must contain alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed; maximum length is 63 characters.</p> |
| Host Type* | Select Name or IP address. |
| Host | Enter the host name or host IP address depending on what host type you choose. |
| Port | <p>Specifies the port in the server. This is the server listening post and the default port will be reached according to protocol defined.</p> <p>Enter the port number. The range is 1025 through 65534.</p> |
| Sockets | <p>Specifies the number of connections to be created.</p> <p>Enter the number of connections. The range is 1 through 64.</p> |
| Authentication | |
| Authorization Type | Specifies the type of authentication. |
| Credentials Type | <p>Select the credential type as ASCII or Base64.</p> <p>Based on the Credential Type that you choose, enter the ASCII string or Base64 string.</p> |
| 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 | <p>Specifies the virtual router that is used for launching.</p> <p>Select a routing instance from the list.</p> |

Table 325: Fields on the Create ICAP Redirect Server Page (continued)

| Field | Action |
|------------------------|---|
| SSL Initiation Profile | Select an SSL initiation profile from the list. |

RELATED DOCUMENTATION

| |
|--|
| About the ICAP Redirect Profile Page 887 |
| Edit an ICAP Redirect Profile 891 |
| Delete ICAP Redirect Profile 891 |

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 side 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 889](#).

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

RELATED DOCUMENTATION

| |
|--|
| About the ICAP Redirect Profile Page 887 |
| Delete ICAP Redirect Profile 891 |

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 side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

| | |
|--|--|
| | About the ICAP Redirect Profile Page 887 |
| | Add an ICAP Redirect Profile 889 |
| | Edit an ICAP Redirect Profile 891 |

8

PART

VPN

[IPsec VPN | 894](#)

[Manual Key VPN | 942](#)

[Dynamic VPN | 947](#)

IPsec VPN

IN THIS CHAPTER

- [About the IPsec VPN Page | 894](#)
- [IPsec VPN Global Settings | 896](#)
- [Create a Site-to-Site VPN | 899](#)
- [Create a Remote Access VPN—Juniper Secure Connect | 914](#)
- [Create a Remote Access VPN—NCP Exclusive Client | 929](#)
- [Edit an IPsec VPN | 939](#)
- [Delete an IPsec VPN | 940](#)

About the IPsec VPN Page

You are here: **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 896](#).
- Edit an IPsec VPN configuration. See [“Edit an IPsec VPN” on page 939](#).
- Delete an IPsec VPN configuration. See [“Delete an IPsec VPN” on page 940](#).
- Show or hide columns in the IPsec VPN table. To do this, click the Show Hide Columns icon in the top 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 326 on page 895 describes the fields on the IPsec VPN page.

Table 326: Fields on the IPsec VPN Page

| Field | Description |
|------------|--|
| Name | Displays the name of the IPsec VPN. |
| IKE Status | Displays the Phase I Internet Key Exchange (IKE) status. |

Table 326: Fields on the IPsec VPN Page (*continued*)

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

RELATED DOCUMENTATION

[Create a Site-to-Site VPN | 899](#)

[Edit an IPsec VPN | 939](#)

[Delete an IPsec VPN | 940](#)

IPsec VPN Global Settings

You are here: **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 327 on page 897](#) describes the fields on the Global Settings page.

Table 327: 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. |
| IPsec VPN Monitor Options | Enable this option if you want the device to monitor VPN liveliness. |
| Interval (seconds) | Enter a value from 2 through 3600 seconds after which Internet Control Message Protocol (ICMP) requests are sent to the peer. |
| Threshold | Enter a value from 1 through 65,536 to specify the number of consecutive unsuccessful pings before the peer is declared unreachable. |
| Remote Access VPN | |
| Default Profile Name | Select a default profile name from the list. NOTE: This option is available when at least one Juniper Secure Connect VPN is created. |
| SSL VPNTunnel tracking | Enable this option to track Encapsulated Security Payload (ESP) tunnels. |

Table 327: 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"> Click +. The Add SSL VPN Profile page appears. 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. To add a new SSL termination profile: <ol style="list-style-type: none"> Click Add. The Create SSL Termination Profile page appears. 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. To add a certificate, click Add. For more information on adding a device certificate, see “Add a Device Certificate” on page 294. To import a certificate, click Import. For more information on importing a device certificate, see “Import a Device Certificate” on page 291. Click OK. Click OK. Click OK. <p>To edit a SSL termination profile, select the profile you want to edit and click on the pencil icon.</p> <p>To delete a SSL termination profile, select the profile you want to delete and click on the delete icon.</p> |
| Internal SA | |

Table 327: Fields on the Global Settings Page (*continued*)

| Field | Description |
|------------------|--|
| Internal SA Keys | <p>Enter the encryption key. You must ensure that the manual encryption key is in ASCII text and 24 characters long; otherwise, the configuration will result in a commit failure.</p> <p>NOTE: This option is available only for SRX5000 line of devices, SRX4100, SRX4200, SRX4600 devices, and vSRX.</p> |

RELATED DOCUMENTATION

[About the IPsec VPN Page | 894](#)
[Edit an IPsec VPN | 939](#)
[Delete an IPsec VPN | 940](#)

Create a Site-to-Site VPN

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

To create a site-to-site VPN:

1. Click **Create VPN** and select **Site to Site** on the upper right side of the IPsec VPN page.

The Create Site to Site VPN page appears.

2. Complete the configuration according to the guidelines provided in [Table 328 on page 899](#) through [Table 333 on page 909](#).

The VPN connectivity will change from gray 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 328: Fields on the Create IPsec VPN Page

| Field | Action |
|-------|---------------------------|
| Name | Enter a name for the VPN. |

Table 328: Fields on the Create IPsec VPN Page (*continued*)

| Field | Action |
|--------------|--|
| 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 | <p>Select the routing mode to which this VPN will be associated:</p> <ul style="list-style-type: none">• Traffic Selector (Auto Route Insertion)• Static Routing• Dynamic Routing – OSPF• Dynamic Routing – BGP <p>For each topology, J-Web auto generates the relevant CLIs. Traffic Selector is the default mode.</p> |

Table 328: 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. The following are the authentication methods for a certificate based: <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. NOTE: ecdsa-signatures-521 supports only SRX5000 line of devices with SPC3 card and junos-ike package installed. • 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 328: 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 329 on page 903.</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 331 on page 905.</p> |

Table 328: 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 333 on page 909.</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 329: 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. |
| 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> |

Table 329: Fields on the Remote Gateway Page (*continued*)

| Field | Action |
|--------------------|---|
| 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 330 on page 904 for fields information.</p> |

Table 330: Fields on the Create Global Address Page

| Field | Action |
|---------|---|
| Name | Enter 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 | <p>IPv4 Address—Enter a valid IPv4 address.</p> <p>Subnet—Enter the subnet for IPv4 address.</p> |
| IPv6 | <p>IPv6 Address—Enter a valid IPv6 address.</p> <p>Subnet Prefix—Enter a subnet mask for the network range. Once entered, the value is validated.</p> |

Table 331: 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. |
| External Interface | Select an outgoing interface from the list for IKE negotiations. 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. |
| Tunnel Interface | Select an interface from the list to bind it to the tunnel interface (route-based VPN). Click Add to add a new interface. The Create Tunnel Interface page appears. See Table 332 on page 908 . |

Table 331: Fields on the Local Gateway Page (continued)

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

Table 331: Fields on the Local Gateway Page (continued)

| Field | Action |
|-------------------|---|
| 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 policies.</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 policies.</p> <p>NOTE: This option is available if the routing mode is Dynamic Routing - BGP.</p> |
| 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 <i>Manage Device Certificates</i>.</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 <i>Manage Trusted Certificate Authority</i>.</p> |

Table 331: Fields on the Local Gateway Page (*continued*)

| Field | Action |
|----------------------------------|---|
| 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"> • ascii-text—ASCII text key. • hexadecimal—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. |
| Add | <p>Click Add.</p> <p>The Create Global Address page appears. See Table 330 on page 904.</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 332: Fields on the Create Tunnel Interface Page

| Field | Action |
|----------------|--|
| Interface Unit | Enter the logical unit number. |
| Description | Enter a description for the logical interface. |

Table 332: Fields on the Create Tunnel Interface Page (*continued*)

| Field | Action |
|---|---|
| Zone | Select a zone for the logical interface from the list to use as a source zone in the firewall policy. |
| 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. | |
| 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 333: IKE and IPsec Settings

| Field | Action |
|---------------------|--|
| IKE Settings | |
| IKE Version | <p>Select the required IKE version, either v1 or v2 to negotiate dynamic security associations (SAs) for IPsec.</p> <p>Default value is v2.</p> |
| IKE Mode | <p>Select the IKE policy mode from the list:</p> <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. |

Table 333: IKE and IPsec Settings (*continued*)

| Field | Action |
|---|---|
| Encryption Algorithm | <p>Select the appropriate encryption mechanism from the list.</p> <p>Default value is aes-256-gcm.</p> |
| 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> |
| 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> |
| 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> |
| Advance Configuration (Optional) | |
| General IKE ID | <p>Enable this option to accept peer IKE ID.</p> |
| IKEv2 Re-authentication | <p>Configure the reauthentication frequency to trigger a new IKEv2 reauthentication.</p> |
| IKEv2 Re-fragmentation | <p>This option is enabled by default.</p> |

Table 333: IKE and IPsec Settings (*continued*)

| Field | Action |
|--------------------------|--|
| IKEv2 Re-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 both IPv4 and IPv6 messages. Range: 570 to 1320 bytes.</p> <p>Default values are:</p> <ul style="list-style-type: none"> • IPv4 messages—576 bytes. • IPv6 messages—1280 bytes. |
| NAT-T | <p>Enable this option for IPsec traffic to pass through a NAT device.</p> <p>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 devices.</p> |
| NAT Keep Alive | <p>Select appropriate keepalive interval in seconds. Range: 1 to 300.</p> <p>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.</p> |
| IPsec Settings | |
| Protocol | Select either Encapsulation Security Protocol (ESP) or Authentication Header (AH) protocol from the list to establish VPN. Default value is ESP. |
| Encryption Algorithm | <p>Select the encryption method. Default value is aes-256-gcm.</p> <p>NOTE: This option is available only for the ESP protocol.</p> |
| Authentication Algorithm | <p>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.</p> <p>NOTE: This option is available when the encryption algorithm is not gcm.</p> |
| 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> |

Table 333: IKE and IPsec Settings (*continued*)

| Field | Action |
|-------------------------------|---|
| 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 | <p>Enable this option to use it in a destination IP address.</p> <p>NOTE: This option is not available for Traffic Selectors routing mode.</p> |
| 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 device 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 device 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> |

Table 333: IKE and IPsec Settings (*continued*)

| Field | Action |
|------------------|---|
| 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> |
| 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 | 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. |
| Idle Time | 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. |
| 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 | 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. |

RELATED DOCUMENTATION

[About the IPsec VPN Page](#) | 894

Create a Remote Access VPN—Juniper Secure Connect

You are here: **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.

2. Complete the configuration according to the guidelines provided in [Table 334 on page 914](#) through [Table 339 on page 925](#).

The VPN connectivity will change from gray 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 334: 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. |

Table 334: Fields on the Create Remote Access (Juniper Secure Connect) Page (*continued*)

| Field | Action |
|-----------------------------|---|
| Description | <p>Enter a description. This description will be used for the IKE and IPsec proposals, policies, remote access profile, client configuration, and NAT rule set.</p> <p>During edit the IPsec policy description will be displayed. IPsec policy and remote access profile descriptions will be updated.</p> |
| Routing Mode | <p>This option is disabled for the remote access.</p> <p>Default mode is Traffic Selector (Auto Route Insertion).</p> |
| 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"> • 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 with each other. The same key must be configured for each peer. This is the default method. • Certificate Based—Specifies the type of digital signatures, which are certificates that confirm the identity of the certificate holder. <p>The supported signature is rsa-signatures. rsa-signatures specifies that a public key algorithm, which supports encryption and digital signatures, is used.</p> |
| 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> |

Table 334: Fields on the Create Remote Access (Juniper Secure Connect) Page (*continued*)

| Field | Action |
|------------------------|---|
| 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 335 on page 917.</p> <p>NOTE: The J-Web UI displays the remote user's URL once local gateway is configured.</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 336 on page 920.</p> |
| 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 339 on page 925.</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 335: 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"> • This option is not available if the default profile is configured. • You must enable the default profile. If not enabled, configure the default profile under VPN > IPsec VPN > Global Settings > Remote Access VPN. |
| 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 device.</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 335: 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 device is reachable.</p> <p>Disable this option to allow the Juniper Secure Connect client to detect till the SRX Series device 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 Certificate Based 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> |
| 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> |

Table 335: Fields on the Remote User Page (*continued*)

| Field | Action |
|------------------------|--|
| 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> |
| EAP-TLS | <p>Enable this option for the authentication process. IKEv2 requires EAP for user authentication. SRX Series device cannot act as an EAP server. An external RADIUS server must be used for IKEv2 EAP to do the EAP authentication. SRX will act as a pass-through authenticator relaying EAP messages between the Juniper Secure Connect client and the RADIUS server.</p> <p>This option is enabled by default.</p> <p>NOTE: This option is available only if you select the Certificate Based authentication method.</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> |
| 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> |

Table 335: Fields on the Remote User Page (*continued*)

| Field | Action |
|----------------------------|--|
| Flush Credential at Logoff | Enable this option to delete username and password from the cache. You must reenter the username and password. |
| 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> |
| 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> |

Table 336: 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 device.</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 336: 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 337 on page 925.</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"> • ascii-text—ASCII text key. • hexadecimal—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 “Add a Device Certificate” on page 294.</p> <p>To import a certificate, click Import. For more information on importing a device certificate, see “Import a Device Certificate” on page 291.</p> <p>NOTE: This option is available if the authentication method is Certificated Based.</p> |

Table 336: 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 “Add a Certificate Authority Profile” on page 306.</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 853.</p> |

Table 336: 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 “Add a Device Certificate” on page 294.</p> <p>To import a certificate, click Import. For more information on importing a device certificate, see “Import a Device Certificate” on page 291.</p> <ul style="list-style-type: none"> • Click OK. c. Click OK. 3. Click OK. |

Table 336: 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 devices 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 338 on page 925.</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> |
| 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 337: 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 | Select a zone from the list to add it to the tunnel interface. This zone is used in the auto-creation of the firewall policy. |
| Routing Instance | Select a routing instance from the list. NOTE: The default routing instance, primary, refers to the main inet.0 routing table in the logical system. |

Table 338: 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. |
| IP Type | Select IPv4 . |
| IPv4 | |
| IPv4 Address | Enter a valid IPv4 address. |
| Subnet | Enter the subnet for IPv4 address. |

Table 339: 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.

Table 339: IKE and IPsec Settings (*continued*)

| Field | Action |
|---|---|
| Encryption Algorithm | <p>Select the appropriate encryption mechanism from the list.</p> <p>Default value is AES-CBC 256-bit.</p> |
| Authentication Algorithm | Select the authentication algorithm from the list. For example, SHA 256-bit. |
| 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. |
| Lifetime Seconds | <p>Select a lifetime duration (in seconds) of an IKE security association (SA).</p> <p>Default value is 28,800 seconds. Range: 180 through 86,400 seconds.</p> |
| 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 | <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 | 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 | <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> |
| Advance Configuration (Optional) | |
| NAT-T | <p>Enable this option for IPsec traffic to pass through a NAT device.</p> <p>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 devices.</p> |

Table 339: IKE and IPsec Settings (*continued*)

| Field | Action |
|--|--|
| NAT Keep Alive | <p>Select appropriate keepalive interval in seconds. Range: 1 to 300.</p> <p>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.</p> |
| 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 | |
| NOTE: The authentication method is Pre-Shared Key or Certificate Based, it automatically generates protocol as ESP. | |
| 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> |

Table 339: 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> |
| 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 256kb. Range: 64 through 4294967294. |
| 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 | 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. |
| Idle Time | 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. |
| 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 | 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. |

RELATED DOCUMENTATION

| |
|---|
| About the IPsec VPN Page 894 |
| IPsec VPN Global Settings 896 |
| Edit an IPsec VPN 939 |
| Delete an IPsec VPN 940 |

Create a Remote Access VPN—NCP Exclusive Client

You are here: **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 340 on page 929](#) through [Table 344 on page 936](#).

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 340: 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. |

Table 340: Fields on the Create Remote Access (NCP Exclusive Client) Page (*continued*)

| Field | Action |
|-----------------------------|--|
| Description | <p>Enter a description. This description will be used for the IKE and IPsec proposals, policies, remote access profile, client configuration, and NAT rule set.</p> <p>During edit the IPsec policy description will be displayed. IPsec policy and remote access profile descriptions will be updated.</p> |
| Routing Mode | <p>This option is disabled for the remote access.</p> <p>Default mode is Traffic Selector (Auto Route Insertion).</p> |
| 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"> • 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 with each other. The same key must be configured for each peer. This is the default method. • Certificate Based—Types of digital signatures, which are certificates that confirm the identity of the certificate holder. <p>The supported signature is rsa-signatures. rsa-signatures specifies that a public key algorithm, which supports encryption and digital signatures, is used.</p> |
| 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> |

Table 340: Fields on the Create Remote Access (NCP Exclusive Client) Page (*continued*)

| Field | Action |
|------------------------|---|
| Remote User | Displays the remote user icon in the topology. This option is disabled. |
| Local Gateway | Displays the local gateway icon in the topology. Click the icon to configure the local gateway. For more information on the fields, see Table 341 on page 931 . |
| IKE and IPsec Settings | Configure the custom IKE or IPsec proposal and the custom IPsec proposal with recommended algorithms or values. For more information on the fields, see Table 344 on page 936 . NOTE: <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 341: 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 | Enter the public (NAT) IP address of the SRX Series device. NOTE: This option is available only when Gateway is behind NAT is enabled. You can configure an IPv4 address to reference the NAT device. |
| IKE ID | This field is mandatory. Enter the IKE ID in the format user@example.com. |

Table 341: 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 342 on page 935.</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"> • ascii-text—ASCII text key. • hexadecimal—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 “Add a Device Certificate” on page 294.</p> <p>To import a certificate, click Import. For more information on importing a device certificate, see “Import a Device Certificate” on page 291.</p> <p>NOTE: This option is available if the authentication method is Certificated Based.</p> |

Table 341: 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 “Add a Certificate Authority Profile” on page 306.</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 853.</p> |

Table 341: 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 “Add a Device Certificate” on page 294.</p> <p>To import a certificate, click Import. For more information on importing a device certificate, see “Import a Device Certificate” on page 291.</p> <ul style="list-style-type: none"> • Click OK. c. Click OK. 3. Click OK. |
| 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 devices for handling the return traffic correctly.</p> |

Table 341: Fields on the Local Gateway Page (*continued*)

| Field | Action |
|----------------------------------|---|
| 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 343 on page 936.</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> |
| 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 342: 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> |

Table 342: Fields on the Create Tunnel Interface Page (*continued*)

| Field | Action |
|------------------|---|
| 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 343: 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. |
| IP Type | Select IPv4 . |
| IPv4 | |
| IPv4 Address | Enter a valid IPv4 address. |
| Subnet | Enter the subnet for IPv4 address. |

Table 344: IKE and IPsec Settings

| Field | Action |
|---|--|
| IKE Settings | |
| <p>NOTE:</p> <p>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 | Select the authentication algorithm from the list. For example, SHA 256-bit. |
| 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. |

Table 344: IKE and IPsec Settings (*continued*)

| Field | Action |
|---|---|
| Lifetime Seconds | <p>Select a lifetime duration (in seconds) of an IKE security association (SA).</p> <p>Default value is 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> |
| Advance Configuration (Optional) | |
| NAT-T | <p>Enable this option for IPsec traffic to pass through a NAT device.</p> <p>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 devices.</p> |
| NAT Keep Alive | <p>Select appropriate keepalive interval in seconds. Range: 1 to 300.</p> <p>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.</p> |
| 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> |

Table 344: IKE and IPsec Settings (*continued*)

| Field | Action |
|-------------------------------|--|
| 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> |
| 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> |
| 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 256kb. Range: 64 through 4294967294. |
| Advanced Configuration | |

Table 344: 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 | 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. |
| Idle Time | 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. |
| 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 | 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. |

RELATED DOCUMENTATION

[About the IPsec VPN Page | 894](#)
[IPsec VPN Global Settings | 896](#)
[Edit an IPsec VPN | 939](#)
[Delete an IPsec VPN | 940](#)

Edit an IPsec VPN

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

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 IPsec VPN page appears with editable fields. You can modify any previous changes done.

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.
- 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 | 899](#)

[Delete an IPsec VPN | 940](#)

Delete an IPsec VPN

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

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-side 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.

3. Click **Yes** to delete or click **No** to retain the configuration.

RELATED DOCUMENTATION

[About the IPsec VPN Page | 894](#)

[IPsec VPN Global Settings | 896](#)

[Create a Site-to-Site VPN | 899](#)

[Edit an IPsec VPN | 939](#)

Manual Key VPN

IN THIS CHAPTER

- [About the Manual Key VPN Page | 942](#)
- [Add a Manual Key VPN | 943](#)
- [Edit a Manual Key VPN | 945](#)
- [Delete Manual Key VPN | 946](#)

About the Manual Key VPN Page

You are here: **VPN > Manual Key VPN**.

Use this page to configure manual key VPN.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a manual key VPN. See [“Add a Manual Key VPN” on page 943](#).
- Edit a manual key VPN. See [“Edit a Manual Key VPN” on page 945](#).
- Delete a manual key VPN. See [“Delete Manual Key VPN” on page 946](#).

Field Descriptions

[Table 345 on page 942](#) describes the fields on the Manual Key VPN page.

Table 345: Fields on the Manual Key VPN Page

| Field | Description |
|---------|---|
| Name | Displays the name of the manual tunnel. |
| Gateway | Displays the selected gateway. |

Table 345: Fields on the Manual Key VPN Page (*continued*)

| Field | Description |
|----------------|--|
| Bind Interface | Displays the tunnel interface to which the route-based VPN is bound. |
| Df Bit | Displays the DF bit in the outer header. |

RELATED DOCUMENTATION

[Add a Manual Key VPN | 943](#)
[Edit a Manual Key VPN | 945](#)
[Delete Manual Key VPN | 946](#)

Add a Manual Key VPN

You are here: **VPN > Manual Key VPN**.

To add a manual key VPN:

1. Click the add icon (+) on the upper right side of the Manual Key VPN page.
The Add Manual Key VPN page appears.
2. Complete the configuration according to the guidelines provided in [Table 346 on page 943](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 346: Fields on the Manual Key VPN Configuration Page

| Field | Action |
|-----------------------|--|
| VPN Manual Key | |
| VPN Name | Enter the VPN name for the IPsec tunnel. |
| Remote Gateway | Enter the name for the remote gateway. |
| External Interface | Select an interface from the list. |

Table 346: Fields on the Manual Key VPN Configuration Page (*continued*)

| Field | Action |
|--------------------------|---|
| Protocol | <p>Select an option from the list to specify the types of protocols available for configuration:</p> <ul style="list-style-type: none"> • ESP • AH |
| SPI | <p>Enter a SPI value.</p> <p>Range: 256 through 16639.</p> |
| Bind to tunnel interface | Select an interface from the list to which the route-based VPN is bound. |
| Do not fragment bit | <p>Select an option from the list to specify how the device handles the 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. • Set—Set the DF bit to the outer header. • copy—Copy the DF bit to the outer header. |
| Enable VPN Monitor | Select this option to configure VPN monitoring. |
| Destination IP | Enter an IP address for the destination peer. |
| Optimized | Select the check box to enable optimization for the device to use traffic patterns as evidence of peer liveliness. If enabled, ICMP requests are suppressed. This feature is disabled by default. |
| Source Interface | Enter a source interface for ICMP requests (VPN monitoring “hellos”). If no source interface is specified, the device automatically uses the local tunnel endpoint interface. |
| Key Values | |
| Authentication | |
| Algorithm | <p>Specifies the hash algorithm that authenticates packet data. Select a hash algorithm from the list:</p> <ul style="list-style-type: none"> • hmac-md5-96—Produces a 128-bit digest. • hmac-sha1-96—Produces a 160-bit digest. • hmac-sha-256-128 |
| ASCII Text | Select the ASCII Text option, and enter the key in the appropriate format. |
| Hexadecimal | Select the Hexadecimal option, and enter the key in the appropriate format. |

Table 346: Fields on the Manual Key VPN Configuration Page (*continued*)

| Field | Action |
|-------------------|--|
| Encryption | |
| Encryption | <p>Specifies the supported Internet Key Exchange (IKE) proposals. Select an option from the list:</p> <ul style="list-style-type: none"> • 3des-cbc—3DES-CBC encryption algorithm. • aes-128-cbc—AES-CBC 128-bit encryption algorithm. • aes-192-cbc—AES-CBC 192-bit encryption algorithm. • aes-256-cbc—AES-CBC 256-bit encryption algorithm. • des-cbc—DES-CBC encryption algorithm. |
| ASCII Text | Enable this option and enter the key in the appropriate format. |
| Hexadecimal | Enable this option and enter the key in the appropriate format. |

RELATED DOCUMENTATION

[About the Manual Key VPN Page | 942](#)
[Edit a Manual Key VPN | 945](#)
[Delete Manual Key VPN | 946](#)

Edit a Manual Key VPN

You are here: **VPN > Manual Key VPN.**

To edit a manual key VPN:

1. Select the existing manual key VPN that you want to edit on the Manual Key VPN page.
2. Click the pencil icon available on the upper right side of the page.

The Edit a Manual Key VPN page appears with editable fields. For more information on the options, see [“Add a Manual Key VPN” on page 943.](#)

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

RELATED DOCUMENTATION

[About the Manual Key VPN Page | 942](#)[Add a Manual Key VPN | 943](#)[Delete Manual Key VPN | 946](#)

Delete Manual Key VPN

You are here: **VPN > Manual Key VPN.**

To delete a manual key VPN:

1. Select a manual key VPN that you want to delete on the Manual Key VPN page.
2. Click the delete icon available on the upper right side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

[About the Manual Key VPN Page | 942](#)[Add a Manual Key VPN | 943](#)[Edit a Manual Key VPN | 945](#)

Dynamic VPN

IN THIS CHAPTER

- [About the Dynamic VPN Page | 947](#)
- [Global Settings | 948](#)
- [IPsec Template | 950](#)
- [Add a Dynamic VPN | 951](#)
- [Edit a Dynamic VPN | 953](#)
- [Delete Dynamic VPN | 953](#)

About the Dynamic VPN Page

You are here: **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 948](#).
- Add DVPN IPsec template. See [“IPsec Template” on page 950](#).
- Add a dynamic VPN. See [“Add a Dynamic VPN” on page 951](#).
- Edit a dynamic VPN. See [“Edit a Dynamic VPN” on page 953](#).
- Delete dynamic VPN. See [“Delete Dynamic VPN” on page 953](#).
- 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 347 on page 948 describes the fields on the Dynamic VPN page.

Table 347: 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 <i>Add a Gateway</i> and <i>Add a VPN</i>.</p> |
| Client VPNs | Create a client configuration for the dynamic VPN feature. |
| Name | Enter a name for dynamic VPN. |
| User | Enter an user name. 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. |
| 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 | 948](#)

[Edit a Dynamic VPN | 953](#)

[Delete Dynamic VPN | 953](#)

Global Settings

You are here: **VPN > Dynamic VPN.**

To add global settings:

1. Click **Global Settings** on the upper right side of the Resource Profiles page.
The DVPN - Global Settings page appears.
2. Complete the configuration according to the guidelines provided in [Table 348 on page 949](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 348: 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 |
| + | 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. |

Table 348: Fields on the Global Settings page (continued)

| Field | Action |
|----------------------|--------------------------------------|
| 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 947 |
| IPsec Template 950 |
| Add a Dynamic VPN 951 |

IPsec Template

You are here: **VPN > Dynamic VPN.**

To add a dynamic VPN IPsec template:

1. Click **IPsec Template** on the upper right side of the Dynamic VPN page.
The DVPN IPsec Template page appears.
2. Complete the configuration according to the guidelines provided in [Table 349 on page 950](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 349: 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. |

Table 349: Fields on the DVPN IPsec Template Page (*continued*)

| Field | Action |
|--------------------|--|
| External Interface | Select the external interface from the list. |

RELATED DOCUMENTATION

[About the Dynamic VPN Page | 947](#)
[Global Settings | 948](#)
[Add a Dynamic VPN | 951](#)

Add a Dynamic VPN

You are here: **VPN > Dynamic VPN.**

To add a dynamic VPN:

1. Click the add icon (+) on the upper right side of the Dynamic VPN page.
The Add DVPN page appears.
2. Complete the configuration according to the guidelines provided in [Table 350 on page 951](#).
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel**.

Table 350: 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 | |

Table 350: Fields on the DVPN Page (*continued*)

| Field | Action |
|----------------------------|---|
| 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. |
| User Name | Enter a user name. |
| Password | Enter a password for the user name. |
| 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 | <p>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.</p> <p>NOTE: The device does not validate that the IP/net mask combination that you enter here matches up with your security policies.</p> |
| 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 | 947](#)

[Edit a Dynamic VPN | 953](#)[Delete Dynamic VPN | 953](#)

Edit a Dynamic VPN

You are here: **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 side of the page.

The Edit DVPN page appears with editable fields. For more information on the options, see [“Add a Dynamic VPN” on page 951.](#)

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

RELATED DOCUMENTATION

[About the Dynamic VPN Page | 947](#)[Global Settings | 948](#)[IPsec Template | 950](#)[Add a Dynamic VPN | 951](#)

Delete Dynamic VPN

You are here: **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 side of the page.
3. Click **Yes** to delete or click **No** to retain the profile.

RELATED DOCUMENTATION

| |
|----------------------------------|
| About the Dynamic VPN Page 947 |
| Global Settings 948 |
| IPsec Template 950 |
| Add a Dynamic VPN 951 |
| Edit a Dynamic VPN 953 |

9

PART

Reports

Reports | **956**

Reports

IN THIS CHAPTER

- [About Reports Page | 956](#)

About Reports Page

IN THIS SECTION

- [Overview | 957](#)
- [Threat Assessment Report | 961](#)
- [Application and User Usage | 961](#)
- [Top Talkers | 961](#)
- [IPS Threat Environment | 962](#)
- [Viruses Blocked | 962](#)
- [URL Report | 962](#)
- [Virus: Top Blocked | 963](#)
- [Top Firewall Events | 963](#)
- [Top Firewall Deny Destinations | 963](#)
- [Top Firewall Service Deny | 963](#)
- [Top Firewall Denies | 963](#)
- [Top IPS Events | 963](#)
- [Top Anti-spam Detected | 964](#)
- [Top Screen Attackers | 964](#)
- [Top Screen Victims | 964](#)
- [Top Screen Hits | 964](#)
- [Top Firewall Rules | 964](#)
- [Top Firewall Deny Sources | 964](#)
- [Top IPS Attack Sources | 964](#)

- [Top IPS Attack Destinations | 964](#)
- [Top IPS Rules | 965](#)
- [Top Web Apps | 965](#)
- [Top Roles | 965](#)
- [Top Applications Blocked | 965](#)
- [Top URLs by User | 965](#)
- [Top Source Zone by Volume | 966](#)
- [Top Applications by User | 966](#)
- [Top Botnet Threats By Source Address via IDP Logs | 966](#)
- [Top Botnet Threats by Destination Address via IDP Logs | 966](#)
- [Top Botnet Threats by Threat Severity via IDP Logs | 966](#)
- [Top Malware Threats by Source Address via IDP Logs | 967](#)
- [Top Malware Threats by Destination Address via IDP Logs | 967](#)
- [Top Malware Threats by Threat Severity via IDP Logs | 967](#)
- [Top Blocked Applications via Webfilter Logs | 967](#)
- [Top Permitted Application Subcategories by Volume via Webfilter Logs | 967](#)
- [Top Permitted Application Subcategories by Count via Webfilter Logs | 968](#)

Overview

Use the Reports menu to generate reports on demand. There are several predefined reports listed in this page, see [Table 351 on page 957](#). The generated report is displayed in HTML format. You can group multiple reports and generate a consolidated report.

Logical system and tenant support the reports listed in [Table 351 on page 957](#) only for SRX1500, SRX4100, SRX4200, and SRX4600.

Table 351: 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 |

Table 351: Predefined Group Reports and Supported Users (continued)

| Report Name | Root | Logical System Users | Tenant Users Support |
|--------------------------------|------|----------------------|----------------------|
| 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 Service Deny | Yes | Yes | Yes |
| Top Firewall Denies | Yes | Yes | Yes |
| Top IPS Events | Yes | Yes | No |
| Top Anti-spam Detected | Yes | Yes | No |
| 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 Roles | Yes | Yes | No |

Table 351: Predefined Group Reports and Supported Users (continued)

| Report Name | Root | Logical System Users | Tenant Users Support |
|--|------|----------------------|----------------------|
| 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 |
| 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 352 on page 960](#).
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 352: 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 | Select an option from the list: <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. NOTE: It may take a while to generate reports, depending on the device data size. |
| Time Span | Select a predefined time span from the list for the report. |
| From | 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. |
| To | 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. |
| Sorting Options | |

Table 352: 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

Starting in Junos OS Release 19.4R1, 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 Service Deny

Top Firewall Service Deny report contains Top Firewall Service Deny.

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.

TopWeb Apps


Top Web Apps report contains Top Web Apps.



NOTE: TopWeb Apps is not supported for tenant users.

Top Roles


Top Roles report contains Top Roles.



NOTE: Top Roles 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.

Release History Table

| Release | Description |
|------------------------|---|
| 19.4R1 | Starting in Junos OS Release 19.4R1, the Threat Assessment report displays a new Filename column in the Malware downloaded by User table. This column helps to identify the malware filename. |