

Juniper Security Director Cloud

User Guide

Published
2024-03-25

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

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

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

Juniper Security Director Cloud User Guide

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

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

About This Guide | xxxi

1

Introduction

Juniper Security Director Cloud Overview | 2

Security Director Cloud Insights Overview | 17

2

Dashboard

About the Dashboard | 20

Tasks You Can Perform | 20

Field Descriptions | 21

3

Monitor

Alerts | 31

Alerts Overview | 31

Search Alerts | 33

Delete an Alert | 33

Using Generated Alerts | 33

Alert Definitions Main Page Fields | 34

Create Alert Definitions | 34

Edit Alert Definitions | 36

Clone Alert Definition | 37

Delete Alert Definitions | 37

Search Alert Definitions | 37

About the Tunnel Status Alerts | 38

Logs | 41

About the Session Page | 41

Monitor CASB Logs | 46

About the Threats Page | 51

About the Web Filtering Events Page | 57

About the IPsec VPNs Events Page | 63

About the All Security Events Page | 68

Monitor End User Authentication Logs | 74

Insights | 77

How to Monitor Incidents | 77

How to Monitor Mitigation | 80

Maps and Charts | 82

Threat Map Overview | 82

About the Application Visibility Page | 85

About the CASB Application Visibility Page | 90

About the User Visibility Page | 93

Tunnel Status | 100

Tunnel Status Overview | 100

About the Tunnel Status Page | 101

Use the Advanced Filter to Monitor Specific Tunnels | 102

About the Site Tunnel Status Page | 103

Service Locations | 106

About the Service Locations Monitor Page | 106

Advanced Threat Prevention | 108

Hosts Overview | 108

Host Details | 111

Threat Sources Overview | 113

Threat Source Details | 115

HTTP File Download Overview | 118

HTTP File Download Details	120
Signature Details	124
Manual Scanning Overview	125
SMB File Download Overview	126
SMB File Download Details	128
Email Attachments Scanning Overview	132
Email Attachments Scanning Details	134
DNS DGA Detection Overview	136
DNS Tunnel Detection Overview	137
DNS DGA and Tunneling Detection Details	139
Encrypted Traffic Insights Overview	143
Encrypted Traffic Insights Details	145
SMTP Quarantine Overview	149
IMAP Block Overview	150
Telemetry Overview	152
Reports 	155
Reports Overview	155
Managing Reports	155
Report Definitions 	159
Report Definitions Main Page Fields	159
Create Threat Analysis Report Definitions	160
Create Application User Usage Report Definitions	162
Create IPS Report Definitions	164
Create Rule Analysis Report Definitions	166
Create Security Events Report Definitions	168
Create Top Talkers Report Definitions	171

Create Network Operations Report Definitions | 173

Create URLs Visited Per User Report Definitions | 174

Create Log Streaming Report Definitions | 176

Using Report Definitions | 178

Editing Report Definitions | 180

Deleting Report Definitions | 180

Generated Reports | 181

Using Reports | 181

ATP Report Definitions | 183

About the ATP Report Definition Page | 183

Create ATP Report Definition | 185

Edit and Delete ATP Report Definition | 187

 | Edit an ATP Report Definition | 187

 | Delete an ATP Report Definition | 188

Send ATP Report | 188

ATP Generated Reports | 190

About the ATP Generated Reports Page | 190

Secure Edge Reports | 197

About the Secure Edge Reports Page | 197

4

SRX

Device Management-Devices | 201

About the Devices Page | 202

Add Devices to Juniper Security Director Cloud | 222

 | Before You Begin | 223

 | Add Devices to Juniper Security Director Cloud | 224

 | Add Devices or Device Clusters Using Commands | 224

 | Add Devices Using Zero Touch Provisioning | 225

 | Add Device by Scanning QR Code | 227

Manage Device Subscriptions | 228

Device Subscriptions Overview | 228

Associate Your Devices with Subscriptions | 228

Create a Device Group | 229

Edit a Device Group | 230

Create a Preprovision Profile | 231

Edit a Preprovision Profile | 232

Delete Devices From Juniper Security Director Cloud | 233

Add a License to a Device | 233

Import a Device Certificate | 235

Resynchronize a Device with Juniper Security Director Cloud | 237

Out-of-Band Changes Overview | 237

Resolve Out-of-Band Changes | 238

Manage Configuration Versions | 239

View Configuration Versions | 240

Edit Configuration Version Description | 241

Pin a Configuration Version | 241

Rollback to a Configuration Version | 242

Compare Configuration Versions | 243

Reboot a Device | 244

Enroll SRX Series Firewalls from ATP Cloud to Juniper Security Director Cloud | 245

Disenroll SRX Series Firewall from ATP Cloud | 246

Upgrade a Device | 247

Security Logs Configuration | 248

Device Management-Configuration Templates | 250

Configuration Templates Overview | 250

Configuration Templates Workflow | 252

About the Configuration Templates Page | 252

Add a Configuration Template | 255

Preview and Render a Configuration Template | 261

Deploy a Configuration Template on to a Device | 262

Edit, Clone, and Delete a Configuration Template | 263

 Edit a Configuration Template | 263

 Clone a Configuration Template | 264

 Delete a Configuration Template | 264

Device Management-Images | 266

About the Images Page | 266

Image Upgrade Workflow | 268

Add an Image | 269

Stage an Image | 271

Deploy an Image | 272

Delete Images | 273

Device Management-Security Packages | 274

About the Security Packages Page | 274

Install Security Package | 276

Enable Automatic Update of Security Package | 277

SRX Policy | 279

Security Policy Overview | 280

About the SRX Policy Page | 282

Rule Placement Analysis | 284

About the Security Policy Rules Page | 286

Add a Security Policy | 290

Edit and Delete a Security Policy | 293

 Edit a Security Policy | 293

 Delete a Security Policy | 294

Reorder a Security Policy | 295

- Import Security Policies Overview | **296**
- Import Security Policies | **298**
- About the Manage Policy Versions Page | **299**
- Create a Policy Version | **301**
- View Policy Version Details | **301**
- Compare Policy Versions | **304**
- Roll Back a Policy Version | **306**
- Delete a Policy Version | **307**
- Add a Security Policy Rule | **307**
- Edit, Clone, and Delete a Security Policy Rule | **313**
 - Edit a Security Policy Rule | **313**
 - Clone a Security Policy Rule | **314**
 - Delete a Security Policy Rule | **314**
- Reorder a Security Policy Rule | **315**
- Configure Global Options | **315**
- Configure Default Rule Option | **318**
- Select a Security Policy Rule Source | **318**
- Select a Security Policy Rule Destination | **319**
- Select Applications and Services | **321**
 - Add Applications and Services to Security Policy Rule | **321**
- Common Operations on a Security Policy Rule | **322**
- Deploy Security Policies | **325**
- Add SRX Policy Rules to Secure Edge Policy (From SRX Policy Page) | **325**
- Capture IPS Data Packets of Devices | **329**
 - Configure IPS Rules to Capture IPS Data Packets | **329**
 - Configure the IPS Sensor to Capture IPS Data Packets | **330**
- SRX Policy-Device View | 332**

Devices with Security Policies Main Page Fields | 332

Security Subscriptions-IPS | 334

About the IPS Profiles Page | 334

Create an IPS Profile | 336

Edit, Clone, and Delete an IPS Profile | 337

- Edit an IPS Profile | 337

- Clone an IPS Profile | 338

- Delete IPS Profiles | 338

About the <IPS-Profile-Name> Page | 339

Create an IPS or an Exempt Rule | 340

- Create an IPS Rule | 341

- Create an Exempt Rule | 348

Edit, Clone, and Delete an IPS Rule or an Exempt Rule | 349

- Edit an IPS Rule or an Exempt Rule | 349

- Clone an IPS Rule or an Exempt Rule | 350

- Delete IPS Rules or Exempt Rules | 350

About the IPS Signatures Page | 351

Create an IPS Signature | 358

Create an IPS Signature Static Group | 370

Create an IPS Signature Dynamic Group | 372

Edit, Clone, and Delete an IPS Signature | 380

- Edit an IPS Signature | 380

- Clone an IPS Signature | 381

- Delete IPS Signatures | 381

Edit, Clone, and Delete an IPS Signature Static Group | 382

- Edit an IPS Signature Static Group | 382

- Clone an IPS Signature Static Group | 383

- Delete IPS Signature Static Groups | 383

Edit, Clone, and Delete an IPS Signature Dynamic Group | 384

- Edit an IPS Signature Dynamic Group | 384

Clone IPS Signature Dynamic Groups | 385

Delete IPS Signature Dynamic Groups | 385

Security Subscriptions-Content Security | 386

Content Security Overview | 387

Configure the Content Security Settings | 389

About the Content Security Profiles Page | 391

Create a Content Security Profile | 395

Edit, Clone, and Delete a Content Security Profile | 399

Edit a Content Security Profile | 400

Clone a Content Security Profile | 400

Delete a Content Security Profile | 401

About the Web Filtering Profiles Page | 401

Create a Web Filtering Profile | 405

Edit, Clone, and Delete a Web Filtering Profile | 413

Edit a Web Filtering Profile | 413

Clone a Web Filtering Profile | 414

Delete a Web Filtering Profile | 414

About the Antivirus Profiles Page | 415

Create an Antivirus Profile | 417

Edit, Clone, and Delete an Antivirus Profile | 420

Edit an Antivirus Profile | 420

Clone an Antivirus Profile | 421

Delete an Antivirus Profile | 421

About the Antispam Profiles Page | 422

Create an Antispam Profile | 424

Edit, Clone, and Delete an Antispam Profile | 426

Edit an Antispam Profile | 426

Clone an Antispam Profile | 426

Delete an Antispam Profile | 427

About the Content Filtering Profiles Page | 427

Create a Content Filtering Profile | 430

Edit, Clone, and Delete a Content Filtering Profile | 434

 Edit a Content Filtering Profile | 434

 Clone a Content Filtering Profile | 435

 Delete a Content Filtering Profile | 435

About the Content Filtering Policy (New) Page | 435

Create a Content Filtering Policy | 436

Add Rules in a Content Filtering Policy | 437

Edit a Content Filtering Policy | 438

Clone a Content Filtering Policy | 438

Edit a Content Filtering Policy Rule | 439

Clone a Content Filtering Policy Rule | 439

Security Subscriptions-Decrypt Profiles | 440

Decrypt Profiles Overview | 440

About the Decrypt Profiles Page | 447

Create a Decrypt Profile | 449

Edit, Clone, and Delete a Decrypt Profile | 457

 Edit a Decrypt Profile | 458

 Clone an Decrypt Profile | 458

 Delete a Decrypt Profile | 458

Security Subscriptions-SecIntel | 459

Security Intelligence Overview | 459

SecIntel Profiles Overview | 461

About SecIntel Profiles Page | 462

Create Command and Control Profile | 463

Create DNS Profile | 466

Create Infected Hosts Profile | 468

Edit, Clone, and Delete SecIntel Profile | 470

 Edit a SecIntel Profile | 470

 Clone a SecIntel Profile | 471

 Delete a SecIntel Profile | 471

About SecIntel Profile Groups Page | 472

Create SecIntel Profile Group | 473

Edit, Clone, and Delete SecIntel Profile Group | 475

 Edit a SecIntel Profile Group | 475

 Clone a SecIntel Profile Group | 475

 Delete a SecIntel Profile Group | 476

Associate a SecIntel Profile Group to a Security Policy | 476

Security Subscriptions-Anti-Malware | 477

Anti-Malware Overview | 477

About the Anti-Malware Page | 479

Create an Anti-Malware Profile | 481

Edit, Clone, and Delete an Anti-Malware Profile | 486

Security Subscriptions-Secure Web Proxy | 489

About the Secure Web Proxy Page | 489

Create a Secure Web Proxy Profile | 491

Edit a Secure Web Proxy Profile | 492

Clone a Secure Web Proxy Profile | 492

Delete a Secure Web Proxy Profile | 493

IPsec VPN | 494

IPsec VPN Overview | 494

Understanding IPsec VPN Modes | 497

Understanding IPsec VPN Routing | 498

Understanding IKE Authentication | 498

IPsec VPN Main Page Fields | 499

- IPsec VPN Global Settings | **500**
- Create a Policy-Based Site-to-Site VPN | **502**
- Create a Route-Based Site-to-Site VPN | **511**
- Create a Hub-and-Spoke (Establishment All Peers) VPN | **524**
- Create a Hub-and-Spoke (Establishment by Spokes) VPN | **536**
- Create a Hub-and-Spoke Auto Discovery VPN | **546**
- Create a Remote Access VPN—Juniper Secure Connect | **557**
- Importing IPsec VPNs | **569**
- Deploy an IPsec VPN | **570**
- Modify IPsec VPN Settings | **571**
 - Modify Device Selection | **571**
- Delete an IPsec VPN | **571**
 - Delete an IPsec VPN | **572**
 - Delete Hub-and-Spoke IPsec VPNs from Specific Devices | **573**
- IPsec VPN-VPN Profiles | 575**
- VPN Profiles Overview | **575**
- VPN Profiles Main Page Fields | **576**
- Creating VPN Profiles | **576**
- Edit and Clone IPsec VPN profiles | **584**
 - Edit a VPN Profile | **584**
 - Clone IPsec VPN Profile | **585**
- Assigning Policies and Profiles to Domains | **585**
- IPsec VPN-Extranet Devices | 587**
- Creating Extranet Devices | **587**
- Extranet Devices Main Page Fields | **588**
- Find Usage for Extranet Devices | **589**
- NAT-NAT Policies | 590**

NAT Policies Overview | **590**

About the NAT Policies Page | **594**

Create a NAT Policy | **595**

Edit and Delete a NAT Policy | **596**

 | Edit a NAT Policy | **597**

 | Delete a NAT Policy | **597**

 | Delete a NAT Policy from Unassigned Devices | **598**

About the NAT Policy Rules Page | **599**

Create a NAT Policy Rule | **601**

Edit, Clone, and Delete a NAT Policy Rule | **608**

 | Edit a NAT Policy Rule | **608**

 | Clone a NAT Policy Rule | **609**

 | Delete a NAT Policy Rule | **609**

Common Operations on a NAT Policy Rule | **609**

Deploy a NAT Policy | **611**

NAT-NAT Pools | 612

NAT Pools Overview | **612**

About the NAT Pools Page | **612**

Create a NAT Pool | **613**

Edit, Clone, and Delete a NAT Pool | **617**

 | Edit a NAT Pool | **617**

 | Clone a NAT Pool | **618**

 | Delete a NAT Pool | **618**

Identity-JIMS | 619

Juniper Identity Management Service Overview | **619**

About the Identity Management Profile Page | **621**

Create Identity Management Profiles | **622**

Edit, Clone, and Delete Identity Management Profiles | **625**

 | Edit Identity Management Profiles | **626**

Clone Identity Management Profiles | 626

Delete Identity Management Profiles | 627

Deploy the Identity Management Profile to SRX Series Firewalls | 627

Identity-Active Directory | 628

About the Active Directory Profile Page | 628

Create an Active Directory Profile | 629

Deploy an Active Directory Profile to SRX Series Firewalls | 634

Edit, Clone, and Delete an Active Directory Profile | 635

Edit an Active Directory Profile | 635

Clone an Active Directory Profile | 635

Delete an Active Directory Profile | 636

Identity-Access profile | 637

LDAP Functionality in Integrated User Firewall Overview | 637

About the Access Profile Page | 639

Create Access Profiles | 640

Deploy the Access Profile to SRX Series Firewalls | 645

Edit, Clone, and Delete Access Profiles | 646

Edit Access Profiles | 646

Clone Access Profiles | 646

Delete Access Profiles | 647

Identity-Address Pools | 648

About the Address Pool Page | 648

Create Address Pool | 649

Edit and Delete Address Pool | 650

Edit an Address Pool | 651

Delete an Address Pool | 651

Secure Edge

Service Management | 653

Juniper Secure Edge Overview | 653

About the Service Locations Page | 660

Create a Service Location | 662

Edit and Delete Service Locations | 664

 | Edit a Service Location | 664

 | Delete a Service Location | 664

About the Sites Page | 665

Create a Site | 668

Create Bulk Sites | 674

Edit and Delete Sites | 675

 | Edit a Site | 675

 | Delete a Site | 676

About the IPsec Profiles Page | 676

Create an IPsec Profile | 677

Edit or Delete an IPsec Profile | 681

 | Edit an IPsec Profile | 681

 | Delete an IPsec Profile | 681

About the External Probe Page | 682

Security Policy | 683

About the Secure Edge Policy Page | 683

Add a Secure Edge Policy Rule | 687

Edit, Clone, and Delete a Secure Edge Policy Rule | 693

 | Edit a Secure Edge Policy Rule | 693

 | Clone a Secure Edge Policy Rule | 694

 | Delete a Secure Edge Policy Rule | 694

Reorder a Security Policy Rule | 694

Select a Secure Edge Policy Source | 695

Select a Secure Edge Policy Destination | 696

Select Applications and Services | 697

| [Add Applications and Services to Security Policy](#) | 697

[Common Operations on a Secure Edge Policy](#) | 698

[Deploy Secure Edge Policies](#) | 699

[Add SRX Policy Rules to Secure Edge Policy \(From Secure Edge Policy Page\)](#) | 700

Security Subscriptions | 704

[IPS Policies Overview](#) | 705

[About IPS Policies](#) | 705

[Create IPS Rule](#) | 707

[Edit, Clone, and Delete IPS Rules](#) | 710

| [Edit an IPS Rule](#) | 710

| [Clone an IPS Rule](#) | 711

| [Delete IPS Rules](#) | 711

[Create Exempt Rule](#) | 711

[Edit, Clone, and Delete Exempt Rule](#) | 713

| [Edit an Exempt Rule](#) | 713

| [Clone an Exempt Rule](#) | 714

| [Delete Exempt Rules](#) | 714

[Web Filtering Profiles Overview](#) | 715

[About the Web Filtering Profiles Page](#) | 715

[Create a Web Filtering Profile](#) | 718

[Edit, Clone, and Delete a Web Filtering Profile](#) | 721

| [Edit a Web Filtering Profile](#) | 721

| [Clone a Web Filtering Profile](#) | 721

| [Delete a Web Filtering Profile](#) | 722

[CASB Overview](#) | 722

[About the CASB Profiles Page](#) | 724

[Create a CASB Profile](#) | 726

[Edit and Delete a CASB Profile](#) | 731

About the CASB Rules Page	732
Add Rules to a CASB Profile	735
Edit and Delete a CASB Rule	739
About the Application Instances Page	740
Create an Application Instance	742
Edit and Delete an Application Instance	745
About the Application Tagging Page	746
Content Filtering Policies Overview	747
About the Content Filtering Policies Page	748
Create a Content Filtering Policy	749
Add Rules in a Content Filtering Policy	750
Edit and Delete a Content Filtering Policy	751
Edit a Content Filtering Policy	751
Delete a Content Filtering Policy	752
Edit, Clone, and Delete a Content Filtering Policy Rule	752
Edit a Content Filtering Policy Rule	753
Clone a Secure Edge Policy Rule	753
Delete a Secure Edge Policy Rule	753
SecIntel Profiles Overview	753
About SecIntel Profiles	754
Create Command and Control Profile	755
Create DNS Profile	757
Create Infected Hosts Profile	759
Edit, Clone, and Delete SecIntel Profile	761
Edit a SecIntel Profile	761
Clone a SecIntel Profile	762
Delete a SecIntel Profile	762
About SecIntel Profile Groups	762

Create SecIntel Profile Group | **764**

Edit, Clone, and Delete SecIntel Profile Group | **765**

 | Edit a SecIntel Profile Group | **765**

 | Clone a SecIntel Profile Group | **766**

 | Delete a SecIntel Profile Group | **766**

Anti-malware Profiles Overview | **766**

About Anti-malware Profiles | **767**

Create Anti-malware Profile | **768**

Edit, Clone, and Delete Anti-malware Profile | **771**

 | Edit an Anti-malware Profile | **771**

 | Clone an Anti-malware Profile | **771**

 | Delete an Anti-malware Profile | **772**

Create a DNS Security Profile | **772**

Create an Encrypted Traffic Insights Profile | **774**

Service Administration | 775

Certificate Management Overview | **776**

About the Certificate Management Page | **776**

Generate a Certificate | **778**

Upload and Download a Certificate | **780**

 | Upload a Certificate | **780**

 | Download a Certificate | **781**

Regenerate and Delete a Certificate | **781**

 | Regenerate a Certificate | **781**

 | Delete a Certificate | **782**

Add Juniper Clouds Root CA Certificate on Microsoft Windows | **782**

Add Juniper Clouds Root CA Certificate on MacOS | **783**

Add Juniper Clouds Root CA Certificate in Google Chrome | **783**

Add Juniper Clouds Root CA Certificate in Mozilla Firefox | **784**

[Proxy Auto Configuration Files Overview | 784](#)

[About the PAC Files Page | 786](#)

[Edit, Clone, and Delete a Proxy Auto Configuration File | 788](#)

[Edit a Proxy Auto Configuration File | 789](#)

[Clone a Proxy Auto Configuration File | 790](#)

[Delete Proxy Auto Configuration Files | 790](#)

[Distribute a Proxy Auto Configuration File URL to Web Browsers | 791](#)

[Create a Group Policy Object | 791](#)

[Distribute the Proxy Auto Configuration File URL | 792](#)

[Update Organization Group Policy | 792](#)

[Verify the Proxy Auto Configuration File URL Distribution | 792](#)

[Manually Add a Proxy Auto Configuration File URL to a Web Browser | 793](#)

[Add a Proxy Auto Configuration File URL to Google Chrome in Microsoft Windows | 793](#)

[Add a Proxy Auto Configuration File URL to Mozilla Firefox in Microsoft Windows | 794](#)

[Add a Proxy Auto Configuration File URL to Microsoft Edge on Microsoft Windows | 794](#)

[Add a Proxy Auto Configuration File URL to Safari on MacOS | 794](#)

[Configure an Explicit Proxy Profile | 795](#)

[Create a URL Category | 795](#)

[Create a URL Pattern | 796](#)

[About the Addresses Page | 798](#)

[Create Addresses or Address Groups | 800](#)

[Edit, Clone, and Delete Addresses and Address Groups | 804](#)

[Edit Addresses and Address Groups | 805](#)

[Clone Addresses and Address Groups | 805](#)

[Delete Addresses and Address Groups | 805](#)

[Decrypt Profiles Overview | 806](#)

[About the Decrypt Profiles Page | 810](#)

[Create a Decrypt Profile | 812](#)

[Edit, Clone, and Delete a Decrypt Profile | 814](#)

[Edit a Decrypt Profile | 814](#)

- Clone a Decrypt Profile | 814
- Delete a Decrypt Profile | 814

Identity | 816

End User Authentication Overview | 816

About the End User Authentication Page | 817

Add an End User Profile | 829

Edit and Delete an End User Profile | 830

- Edit an End User Profile | 830
- Delete an End User Profile | 831

Add a Group | 831

Edit and Delete a Group | 832

- Edit a Group | 832
- Delete a Group | 833

Juniper Identity Management Service Overview | 833

About the JIMS Page | 835

JIMS Collector Onboarding Overview | 837

Onboard JIMS Collector | 837

Create JIMS Collector Service Accounts | 838

- Configuring Limited Permission User Accounts | 839
- Configuring Properties for Limited Permission User Accounts | 839
- Adding Limited Permission User Accounts to Active Directory Groups | 839
- Defining Group Policies for Limited Permission User Accounts | 839

Install JIMS Collector | 840

Configure JIMS Collector to Get Information from the Directory Service | 841

Configure JIMS Collector to Get Microsoft Event Logs | 842

Configure JIMS Collector to Probe Unknown IP Addresses | 844

Delete JIMS Collector | 844

CASB and DLP | 846

About CASB and DLP | 846

Shared Services

Firewall Profiles-Rule Options | 848

About Rule Options Page | 848

Create Rule Options | 849

Edit, Clone, and Delete Rule Options | 853

Edit Rule Options | 853

Clone Rule Options | 853

Delete Rule Options | 854

Firewall Profiles-Redirect Profiles | 855

About the Redirect Profiles Page | 855

Create a Redirect Profile | 856

Edit, Clone, and Delete a Redirect Profile | 857

Edit a Redirect Profile | 857

Clone a Redirect Profile | 858

Delete a Redirect Profile | 858

Objects-Addresses | 859

About the Addresses Page | 859

Variable Address Overview | 862

Create Addresses or Address Groups | 863

Import and Export Addresses | 868

Import Addresses from a CSV File | 869

Export Addresses to a CSV File | 870

Merge Duplicate Addresses | 870

Replace Addresses in Bulk | 872

Edit, Clone, and Delete Addresses and Address Groups | 872

Edit Addresses and Address Groups | 873

Clone Addresses and Address Groups | 873

Delete Addresses and Address Groups | 874

Objects-GeolP | 875

About the GeolP Page | 875

Create a GeolP Feed | 876

Edit, Clone, and Delete GeolP Feeds | 878

 Edit a GeolP Feed | 878

 Clone a GeolP Feed | 879

 Delete a GeolP Feed | 879

Objects-Services | 881

About the Services Page | 881

Create Services and Service Groups | 883

Import and Export Services | 886

 Import Services from a CSV File | 887

 Export services to a CSV File | 888

Merge Duplicate Services | 888

Replace Services in Bulk | 889

Edit, Clone, and Delete Services and Service Groups | 890

 Edit Services and Service Groups | 891

 Clone Services or Service Groups | 891

 Delete Services and Service Groups | 891

Create Protocols | 892

Edit and Delete Protocols | 896

 Edit Protocols | 896

 Delete Protocols | 896

Objects-Applications | 898

About the Application Signatures Page | 898

Add Application Signatures | 901

Edit, Clone, and Delete Application Signatures | 908

 Edit Custom Application Signatures | 909

 Clone Application Signatures | 909

 Delete Application Signatures | 910

Add Custom Application Signature Groups | 910

Edit, Clone, and Delete Application Signature Groups | 911

 Edit Custom Application Signature Groups | 912

 Clone Application Signature Groups | 912

 Delete Custom Application Signature Groups | 912

Objects-Schedules | 914

Schedules Overview | 914

About the Schedules Page | 915

Create a Schedule | 916

Edit, Clone, and Delete a Schedule | 918

 Edit a Schedule | 918

 Clone a Schedule | 919

 Delete a Schedule | 919

Objects-URL Patterns | 920

About the URL Patterns Page | 920

Create a URL Pattern | 921

Import URL Patterns from a CSV File | 923

Edit, Clone, and Delete a URL Pattern | 924

 Edit a URL Pattern | 925

 Clone a URL Pattern | 925

 Delete a URL Pattern | 925

Objects-URL Categories | 927

About the URL Categories Page | 927

Create a URL Category | 928

Edit, Clone, and Delete a URL Category | 930

 Edit a URL Category | 930

 Clone a URL Category | 930

 Delete a URL Category | 931

Advanced Threat Prevention | 932

Enroll an SRX Series Firewall using Juniper ATP Cloud Web Portal | 932

Remove an SRX Series Firewall From Juniper Advanced Threat Prevention Cloud	936
Search for SRX Series Firewalls Within Juniper Advanced Threat Prevention Cloud	937
Device Information	937
File Inspection Profiles Overview	939
Create File Inspection Profiles	941
Email Management Overview	942
Configure SMTP Email Management	944
Configure IMAP Email Management	948
Adaptive Threat Profiling Overview	951
Create an Adaptive Threat Profiling Feed	954
Allowlist and Blocklist Overview	956
Create Allowlists and Blocklists	957
SecIntel Feeds Overview	963
Juniper Threat Feeds Overview	969
Global Configuration for Infected Hosts	969
Enable Logging	972
Configure Threat Intelligence Sharing	973
Configure Trusted Proxy Servers	975
Configure DAG Filter	976
Configure Webhook	977
Insights-On-prem Collectors 	978
About the Collectors Page	978
About the Log Parsers Page	979
Create a Log Parser	980
Edit and Delete a Log Parser	985
Edit a Log Parser	985

Delete a Log Parser	985
About the Log Sources Page	986
Create a Log Source	987
Edit and Delete a Log Source	987
Edit a Log Source	988
Delete a Log Source	988
About the Identity Settings Page	988
Add JIMS Configuration	989
Edit and Delete an Identity Setting	991
Edit a JIMS Configuration	991
Delete a JIMS Configuration	991
Insights-Cloud Collector 	992
About the Cloud Collector Page	992
Insights-Rules 	993
About the Event Scoring Rules Page	993
Create an Event Scoring Rule	994
Edit and Delete Event Scoring Rules	995
Edit an Event Scoring Rule	995
Delete an Event Scoring Rule	996
About the Incident Scoring Rules Page	996
Create an Incident Scoring Rule	998
Edit and Delete Incident Scoring Rules	999
Edit an Incident Scoring Rule	999
Delete an Incident Scoring Rule	999
Insights-Settings 	1000
About the Threat Intelligence Page	1000
Configure Threat Intelligence Source	1001
Edit and Delete Threat Intelligence Source	1002

- Edit a Threat Intelligence Source | 1003
- Delete a Threat Intelligence Source | 1003

About the Service Now Configuration | 1003

About the Correlation Time Page | 1004

Administration

Subscriptions | 1007

Subscriptions Overview | 1007

Subscription Notifications | 1008

About the Subscriptions Page | 1009

Add a Subscription | 1011

Delete a Subscription | 1012

Users & Roles | 1013

Users Overview | 1013

About the Users Page | 1014

Add a User | 1015

Edit and Delete a User | 1017

- Edit a User | 1017
- Delete a User | 1019

Roles Overview | 1019

About the Roles Page | 1020

Add a Role | 1021

Edit, Clone, and Delete a Role | 1023

- Edit a Role | 1024
- Clone a Role | 1024
- Delete a Role | 1024

Single Sign-On Configuration | 1026

Single Sign-On Configuration Overview | 1026

Configure Single Sign-On Settings | 1027

Audit Logs | 1028

Audit Logs Overview | 1028

About the Audit Logs Page | 1029

Export Audit Logs | 1031

Service Updates | 1032

About the Service Updates Page | 1032

Jobs | 1034

Jobs Management in Juniper Security Director Cloud | 1034

Jobs Main Page Fields | 1035

Using Jobs in Juniper Security Director Cloud | 1037

Viewing the Details of a Job in Juniper Security Director Cloud | 1037

Canceling Scheduled Jobs in Juniper Security Director Cloud | 1039

Data Management | 1040

About the Data Management Page | 1040

Export Log Data | 1042

Delete Device Logs | 1042

Log Streaming | 1043

About the Log Streaming Page | 1043

Add a Log Stream | 1045

Edit and Delete a Log Stream | 1045

 | Edit a Log Stream | 1045

 | Delete a Log Stream | 1046

URL Recategorization | 1047

About the URL Recategorization Page | 1047

Request URL Recategorization | 1049

Organization | 1051

About the Organization Page | 1051

Create an Organization | **1054**

Edit and Delete an Organization | **1056**

 Edit an Organization | **1056**

 Delete an Organization | **1058**

ATP Mapping | 1059

About the ATP Mapping Page | **1059**

Map an Existing ATP Realm to Juniper Security Director Cloud | **1060**

Map an Auto-generated Realm to Secure Edge | **1061**

ATP Audit Logs | 1062

About the ATP Audit Logs Page | **1062**

Export Audit Logs | **1063**

About This Guide

Use this guide to create and manage your organization accounts on Juniper® Security Director Cloud. Juniper Security Director Cloud is a cloud-based portal that manages on-premise security, cloud-based security, and cloud-delivered security.

1

PART

Introduction

[Juniper Security Director Cloud Overview](#) | 2

[Security Director Cloud Insights Overview](#) | 17

Juniper Security Director Cloud Overview

IN THIS SECTION

- [Benefits of Juniper Security Director Cloud | 11](#)
- [Access Juniper Security Director Cloud | 11](#)
- [Using Navigational Elements | 14](#)

Juniper Security Director Cloud is your portal to Secure Access Service Edge (SASE), bridging your current security deployments with your future SASE rollout. Juniper Security Director Cloud helps organizations migrate securely to SASE architecture. Using Juniper Security Director Cloud, organizations can create unified policies once and deploy the policies wherever their users are using the applications. Unified policy management ensures seamless security across all users, applications, or devices wherever they are.

Juniper Security Director Cloud empowers both traditional security roles and network roles by automating tier I and tier II security tasks and by supplementing network visibility with security insights. Additionally, Juniper Security Director Cloud provides value for enterprise and service providers by shifting from monolithic centralized data center architectures to SASE-based, decentralized architectures that bring services closer to end users.

Juniper Security Director Cloud provides a user-friendly and security-focused GUI interface that allows an administrator to perform specific tasks. [Table 1 on page 3](#).

When you log in to application, the main menu (left sidebar) that is displayed and the actions that you can perform depend on your access privileges. [Table 1 on page 3](#) lists the main menu that is available in the Juniper Security Director Cloud, a brief description of each menu item, and a link to the relevant topic in the Juniper Security Director Cloud User Guide.

Table 1: GUI Menu and Description

Menu	Description
Dashboard	<p>The dashboard displays information such as top events, top denials, top applications, top source and destination IP addresses, top traffic, and top infected hosts. Graphical security widgets that can be added, removed, and rearranged per user. These widgets offer each user a customized view of network security. See "About the Dashboard" on page 20 .</p>
Monitor	<p>You can view following information from Monitor menu:</p> <ul style="list-style-type: none"> • Alerts—Alerts are used to notify about significant events within the system. You can define alert criteria based on a set of predefined filters. See "Alerts Overview" on page 31 • Logs—You can view details of the traffic logs that are generated by managed devices. You can view information about security events based on IPS policies, Web filtering policies, and IPSec VPN policies. You can also view an overall, high-level view of your network environment. You can view abnormal events, attacks, viruses, or worms when log data is correlated and analyzed. See "About the Session Page" on page 41 • Maps and Charts—The threat map provides a visualization of the geographic regions for incoming and outgoing traffic. You can view blocked and allowed threat events based on feeds from IPS, antivirus, and antispam engines. See "Threat Map Overview" on page 82 • Reports—Reports are generated based on a summary of network activity and overall network status. These generated reports can help you to perform a trend analysis of your network's activities to study changes in traffic patterns. You can use the predefined reports, or you can build custom reports that meet specific needs. See "Reports Overview" on page 155

Table 1: GUI Menu and Description (Continued)

Menu	Description
SRX>Device Management	<ul style="list-style-type: none"> <li data-bbox="841 359 1425 422">• Devices—Discover and manage devices. See "About the Devices Page" on page 202 . <li data-bbox="841 464 1425 705">• Configuration Templates—Provision configurations, both during onboarding and throughout the device life cycle, for Juniper Networks and other third-party devices. By using configuration templates, you can deploy customized configurations on devices. See "Configuration Templates Overview" on page 250 . <li data-bbox="841 747 1425 1020">• Software Images—A software image is a software installation package used to upgrade or downgrade the operating system running on a network device. Juniper Security Director Cloud helps you to manage (add, stage, deploy, and delete) the entire lifecycle of software images of all managed network devices. See "About the Images Page" on page 266 . <li data-bbox="841 1062 1425 1377">• Security Packages—Security package consists of IPS Signatures, Application Signatures, and URL Categories. Use the Security Packages page. You can view the list of latest security packages available on Juniper Security Director Cloud, view the list of currently installed security packages on the device, and install the latest security packages on the device. See "About the Security Packages Page" on page 274 .

Table 1: GUI Menu and Description (Continued)

Menu	Description
SRX>Security Policy	<ul style="list-style-type: none"> • SRX Policy— Provides security functionality by enforcing rules on traffic that passes through a device. Traffic is permitted or denied based on the action defined in the security policy rules. You can create, modify, and delete security policy and associate the devices with a security policy. See "Security Policy Overview" on page 280 . • Device View—Provides an overall, high-level view of your security policy device settings. You can also use this page to view detailed information on the number of rules and policies assigned per device. See "Devices with Security Policies Main Page Fields" on page 332 .
SRX>Security Subscriptions	<p>Advanced Security management related to:</p> <ul style="list-style-type: none"> • IPS— The intrusion prevention system (IPS) profile is deployed on a device by associating the profile with a security policy rule, which is deployed on the device. You can associate IPS rules and exempt rules with an IPS profile. See "About the IPS Profiles Page" on page 334 . • Content Security—content security is a term used to describe the consolidation of several security features to protect against multiple threat types. You can enable antispam, antivirus, content filtering, and web filtering. See "About the Content Security Profiles Page" on page 391 . • Decrypt Profiles—You can view and manage SSL proxy profiles. See "About the Decrypt Profiles Page" on page 447 . • VPN—You can view and manage the IPsec VPN profiles that provide a means to securely communicate with remote computers across a public WAN, such as the Internet. See "IPsec VPN Overview" on page 494 .

Table 1: GUI Menu and Description (Continued)

Menu	Description
SRX>IPsec VPN	<p>IPsec VPN—You can view and manage the IPsec VPN profiles that provide a means to securely communicate with remote computers across a public WAN, such as the Internet. See "IPsec VPN Overview" on page 494 .</p>
SRX>NAT	<ul style="list-style-type: none"> • NAT Policies— Create, modify, clone, and delete NAT policies and policy rules. You can filter and sort this information to get a better understanding of what you want to configure. See "About the NAT Policies Page" on page 594 . • NAT Pools—A NAT pool is a set of IP addresses that you can define and use for address translation. NAT policies perform address translation by translating internal IP addresses to the addresses in these pools. See "About the NAT Pools Page" on page 612 .

Table 1: GUI Menu and Description (Continued)

Menu	Description
SRX>Identity	<ul style="list-style-type: none"> <li data-bbox="841 363 1409 569">• JIMS—Use the Identity Management Profile page to obtain advanced user identity from different authentication sources for SRX Series Firewalls. You can create, edit, clone, delete and deploy identity management profiles. See "About the Identity Management Profile Page" on page 621 . <li data-bbox="841 606 1409 812">• Active Directory—Active Directory configuration is used by the SRX Series Firewalls to contact the Active Directory server. You can view, create, modify, clone, and delete Active Directory profile. See "About the Active Directory Profile Page" on page 628 . <li data-bbox="841 850 1409 1094">• Access Profiles—Access profiles enable access configuration on the network—this consists of authentication configuration. Juniper Security Director Cloud supports RADIUS, Lightweight Directory Access Protocol (LDAP), and local authentication as authentication methods. See "About the Access Profile Page" on page 639 . <li data-bbox="841 1131 1409 1375">• Address Pools—An address pool is a set of Internet Protocol (IP) addresses available for allocation to users, such as in host configurations with the DHCP. You can create centralized IPv4 address pools independent of the client applications that use the pools. See "About the Address Pool Page" on page 648 .

Table 1: GUI Menu and Description (Continued)

Menu	Description
Shared Services>Firewall Profiles	<p>Perform security-related management tasks related to:</p> <ul style="list-style-type: none">• Rule Options—You can create an object to specify redirect options, authentication, TCP-options, and action for destination-address translated or untranslated packets. When a rule options is created, the Juniper Security Director Cloud creates an object in the database to represent the rule options. See "About Rule Options Page" on page 848 .• Redirect Profiles—You can create a redirect profile and provide a reason for the policy action or to redirect the user request to an informative webpage. See "About the Redirect Profiles Page" on page 855 .

Table 1: GUI Menu and Description (Continued)

Menu	Description
Shared Services>Objects	<p>Mange the following objects:</p> <ul style="list-style-type: none"> • Addresses—Create, edit, and delete addresses and address groups. Addresses and address groups are used in security and NAT services. See "About the Addresses Page" on page 859 . • GeoIP—Create, modify, or delete the IP-based geolocation (GeoIP) feeds. You can use the GeoIP feeds in security policy to deny or allow traffic based on source or destination IP address. See "About the GeoIP Page" on page 875 . • Services—Manage applications across devices. A service refers to an application on a device, such as Domain Name Service (DNS). See "About the Services Page" on page 881 . • Applications—Create, modify, clone, and delete application signature groups. You can also view the details of predefined application signatures that are already downloaded. See "About the Application Signatures Page" on page 898 . • Schedules—A schedule allows a policy to be active for a specified duration. If you want a policy to be active during a scheduled time, you must first create a schedule for that policy or link the policy to an existing schedule. See "Schedules Overview" on page 914 . • URL Patterns—View, create, edit, clone, and delete URL patterns. A URL pattern contains a list of URLs. See "About the URL Patterns Page" on page 920 . • URL Categories—View, create, edit, clone, and delete URL categories. A URL category is a list of URL patterns grouped under a single title. See "About the URL Categories Page" on page 927 .

Table 1: GUI Menu and Description (Continued)

Menu	Description
Administration	<p>Perform administrative tasks including:</p> <ul style="list-style-type: none"> • Subscriptions—Add and manage your Juniper Security Director Cloud subscriptions. See "Subscriptions Overview" on page 1007 . • Users and Roles—Juniper Security Director Cloud supports authentication and role-based access control (RBAC) to its resources and services. See "About the Users Page" on page 1014 • Jobs—The Jobs page lets you monitor the status of jobs that have run or are scheduled to run in Juniper Security Director Cloud. Jobs can be scheduled to run immediately or in the future. See "Jobs Management in Juniper Security Director Cloud" on page 1034 • Audit logs—An audit log is a record of a sequence of activities that have affected a specific operation or procedure. Audit logs are useful for tracing events and for maintaining historical data. See "About the Audit Logs Page" on page 1029 • Data Management—The Data Management page displays device logs related to security and data traffic. You can export or delete these logs. See "About the Data Management Page" on page 1040 • Organization—An organization account helps you to add devices, subscribe your devices, and start managing the devices. An administrator, operator, or user with read-only access of organization can create multiple organization accounts in Juniper Security Director Cloud. See "About the Organization Page" on page 1051

When you log in to Portal, the main menu (left sidebar) that is displayed and the actions that you can perform depend on your access privileges. [Table 1 on page 3](#) displays the main menu available in the Juniper Security Director Cloud Portal, a brief description of each menu item, and a link to the relevant topic in the Juniper Security Director Cloud User Guide.

Benefits of Juniper Security Director Cloud

- Manages all security deployments—physical, virtual, and containerized SRX for traditional deployments— and helps the smooth transition to a SASE architecture.
- Offers fully integrated security with unified policies at every point of connection. With unified policy management, you can create a policy once and apply it anywhere. You don't need to copy over or recreate rule sets.
- Provides a single centralized management interface that enables administrators to manage all phases of the security policy life cycle by using customizable dashboards and reports.
- Offers protection from attacks against the client and from the server-side exploits, malware, and C2 traffic, regardless of where the users and applications are located.
- Enables easy deployment and configuration for new sites using zero-touch provisioning (ZTP), auto-rule placement, and policy-based routing.
- Enables security for on-premise and cloud-based environments simultaneously and at scale, with validated efficacy against data center threats.

Access Juniper Security Director Cloud

To access Juniper Security Director Cloud portal:

1. If you are logging in to Juniper Security Director Cloud for the first time, click **Create an organization account** link. If you already created an organization account, skip to Step "5" on page 13 .
2. Set your login credentials, contact details, and the organization account details according to the guidelines provided in table [Table 2 on page 11](#) .

Table 2: Fields to Create an Organization Account

Field	Description
Login Credentials	
Email	Enter a valid e-mail ID.

Table 2: Fields to Create an Organization Account (*Continued*)

Field	Description
Password	Enter a password that contains at least one number, one uppercase letter and one special character. The password length should be between 8 to 20 characters.
Contact Details	
Contact Details	<p>Enter the following contact details:</p> <ul style="list-style-type: none"> • Name—Enter your name. Only alphabets with spaces are allowed. The maximum length is 32 characters. • Company name—Enter your company name. Only alphanumeric characters, spaces, ` - ` (hyphen) and ` _ ` (underscore) are allowed. The maximum length is 64 characters. • Country—Select the country from the dropdown list. • Phone number—Enter a valid phone number that can contain numbers and +, -, or () symbols. The total length of phone number must be 7 (including hyphen) through 18 characters. Example phone formats: <ul style="list-style-type: none"> • +91-9590951194 • +918087677876 • 408-111-1111 • 1(234)56789011234 • (+351)282435050 • 90191919908 • 555-89097896
Organization account details	

Table 2: Fields to Create an Organization Account (Continued)

Field	Description
Organization name	Enter a name for the organization account for which you would be managing the security devices and services.
Select Home Pop	<p>Select your home region.</p> <p>The home region is usually the geographical area where your SRX Series Firewalls are located. Technically, you can select any region, but we recommend you select the region that is closest to your geographical location.</p> <p>NOTE: The Juniper Security Director Cloud FQDN of each home region is different. You must configure your network firewall to allow access to the FQDN. Contact your sales representative or account manager for the specific FQDN.</p>

3. Click **Create Organization Account**. You will receive an email to verify your e-mail address and to send a request to the Juniper Security Director Cloud team to activate your organization account.
4. Log in to your e-mail account, open the e-mail, and click the **Activate Organization Account** button to send a request to activate your organization account.

NOTE:

- You must verify your e-mail address and send the account activation request by clicking the **Activate Organization Account** button within 24 hours after receiving the e-mail. Otherwise, your account details will be deleted from Juniper Security Director Cloud, and you'll have to re-create your account and send the activation request.
- You will receive an e-mail about your organization account activation status within 7 working days.

If your account activation request is approved, you will receive an e-mail with login page information.

5. Click **Go to Login Page**, enter your e-mail address, and click **Next**.
 - If you are a local user, enter the password and click **Sign in**.

- If you are assigned to multiple organizations configured with SSO authentication, options to sign in using the corresponding domain accounts are displayed. You can click the corresponding sign in option to be redirected to your organization Identity Provider (IdP) page. On the IdP page, enter your credentials and sign in.
6. Click **Go to Dashboard**. You can access different tasks easily using the menu bar on the left of each page. The top-level menu items are listed in [Table 1 on page 3](#) .

Using Navigational Elements

For a more personal and customizable user experience, Juniper Networks provides some navigational aids within the GUI. [Table 3 on page 14](#) shows the sample of navigation, customization, and help icons.

Table 3: Navigational Elements

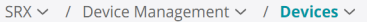



Element	Icon	Location
Breadcrumbs—Trace your location in the UI. The breadcrumbs provide a path back to one of the seven starting tabs: Dashboard, Monitor, Device Management, NAT & Objects, Firewall, Advanced Security, and Administration.		The upper left part of the main screen below the Monitor tab. Not visible on the Dashboard.
Info Tips—Position your mouse over any available question mark icon for quick pop-up guidance.		Various places around the GUI.
Show and Hide Left-Nav—Click the hamburger icon to show or hide the left-navigation section.		Left side of the tab bar.
Show/Hide Columns—In tabular displays, you can choose which columns are visible by clicking the icon, and then selecting the check boxes in the menu.		Upper-right corner of some tabular display windows such as the Monitor tab and the Device Management tab.

Table 3: Navigational Elements *(Continued)*



Element	Icon	Location
<p>Global Search—Search for specific data such as security policies, addresses, zone, service objects, and so on in your network. You can click the result to navigate to the specific page in the UI.</p> <p>You can also refine the search results based on specific criteria such as date range, device type, and policy type. You can also search for objects in your network using full or partial keywords.</p> <p>You can search for:</p> <ul style="list-style-type: none"> • Addresses • Applications • CASB profiles and rules • Configuration templates • Configured schedules • Content Security: <ul style="list-style-type: none"> • Content security profiles • Antivirus profiles • Antispam profiles • Web filtering profiles • Content filtering profiles • Anti-malware • Decrypt profiles 		<p>Navigation aid on the right side of the top bar.</p>

Table 3: Navigational Elements (Continued)

Element	Icon	Location
<ul style="list-style-type: none"> • Devices using the hostname, OS version, and product series as keywords • Extranet devices using the name, description, the IKE identity, and the IKE address as keywords • Firewall rules and rule options • Firewall redirect profiles • Identify management: <ul style="list-style-type: none"> • JIMS • Active Directory • Access profiles • Address pools • IPS profiles and signatures • IPsec VPNs and profiles • NAT policies and pools • SecIntel profiles and groups • Security policies • Secure web proxies • Services • Software images • URL categories • URL patterns • Users and user roles 		

Table 3: Navigational Elements *(Continued)*

Element	Icon	Location
Table Search—In large tabular views, you can search for specific text within any of the visible fields in the display.		Upper-right corner of tabular views. Next to the Show Hide Columns icon.

Security Director Cloud Insights Overview

IN THIS SECTION

- [Benefits | 17](#)
- [Security Director Cloud Insights Architecture | 18](#)

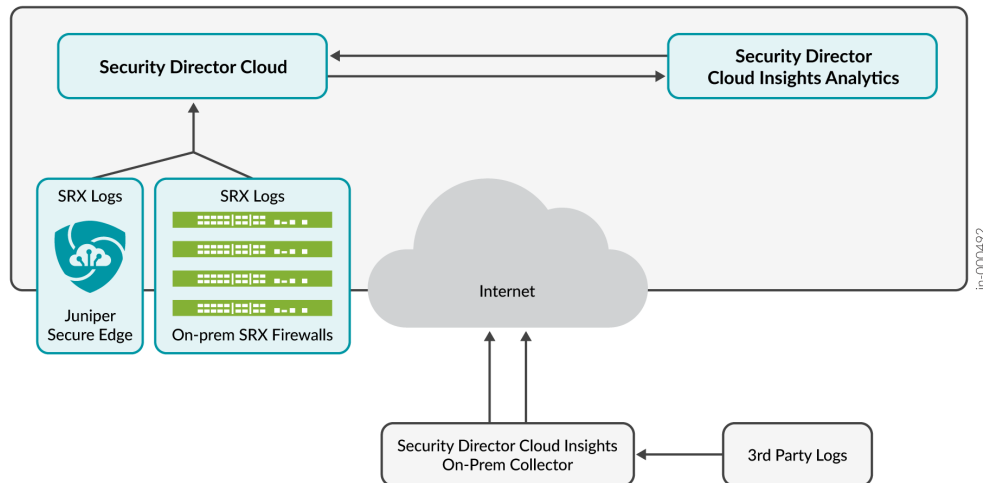
Security Director Cloud Insights facilitates automated security operations. It enables you to take effective actions on security events logged by Juniper Networks security products and third party security products. Security Director Cloud Insights displays events that affect a host or events that are impacted by a particular threat source from different security modules. These events provide instantaneous information about the extent of an attack. The application contains an option to verify the incidents using your trusted threat intelligence provider. After you have verified the incidents, you can take preventive and remedial actions using the rich capabilities of our security products.

Benefits

- Reduce the number of alerts across disparate security solutions.
- Quickly react to active threats with one-click mitigation.
- Improve the security operations center (SOC) teams' ability to focus on the highest priority threats.

Security Director Cloud Insights Architecture

Figure 1: Security Director Cloud Insights Architecture



Security Director Cloud Insights collector collects and aggregates SRX logs and the third party logs. Some of the features in Security Director Cloud uses the SRX logs. You can monitor the incidents and mitigate the events based on your network requirements.

Security Director Cloud Insights receives SRX logs from Juniper Secure Edge or Juniper SRX firewall that are managed by Security Director Cloud. If you have third party security products, then Security Director Cloud Insights receives logs from third party security products. Security Director Cloud Insights correlates the security application logs to tell you what are the most important security incidents in your organization. Security Director Cloud ingests all the security events from different sources and provides unified view to the users.

Security Director Cloud Insights supports the following log collector types:

- Cloud collector—Enable the cloud collector if you receive SRX logs from Juniper Secure Edge or Security Director Cloud managed SRX firewalls. By default, the cloud collector is enabled.
- On-premises collector—If you have a third party log source, such as McAfee, you can deploy Security Director Cloud Insights on-premises collector. You can redirect the output from third party security products to Security Director Cloud Insights on-premises collector. Logs are then filtered and sent to Security Director Cloud.

If you have any third party security product, you'll need to download Security Director Cloud Insights on-premises collector OVA file from the download site and deploy. See [Deploy and Configure Security Director Cloud Insights On-premises Collector](#).

2

PART

Dashboard

[About the Dashboard](#) | 20

About the Dashboard

IN THIS SECTION

- [Tasks You Can Perform | 20](#)
- [Field Descriptions | 21](#)

To access the dashboard, select **Dashboard** from the menu.

Juniper Security Director Cloud provides a user-configurable dashboard that offers you a customized view of network services through widgets. You can drag these widgets from the top of the dashboard to your workspace where you can add, remove, and rearrange the widgets.

The dashboard automatically adjusts the placement of the widgets to dynamically fit on your web browser window without changing the order of the widgets. You can manually reorder the widgets by using the drag and drop option. You can also press and hold the top portion of the widget to move it to a new location.

Tasks You Can Perform

You can perform the following tasks from this page:

- Customize the dashboard by adding, removing, and rearranging the widgets.
- Update the dashboard or an individual widget by clicking the refresh icon.
- Show or hide widget thumbnails in the carousel by selecting the category of widgets to view from the list at the top left of the carousel. The default setting is All Widgets.
- Add a widget to the dashboard by dragging the widget from the palette or thumbnail container into the dashboard.
- Delete a widget from the dashboard page by clicking the delete icon in the title bar of the widget and confirming the delete operation.
- Add a dashboard tab by clicking the plus icon, optionally entering a name, and pressing Enter.

You can then add widgets to the dashboard.

- Rename a dashboard by double-clicking the title bar of the dashboard, entering a name, and pressing Enter.
- Delete a dashboard by clicking the delete icon in the title bar of the dashboard and confirming the delete operation.

Field Descriptions

You can view important data by using the widgets at the top of your dashboard.

[Table 4 on page 21](#) describes the dashboard widgets.

NOTE: All the following widgets are populated from the syslog data.

Table 4: Widgets on the Dashboard

Widget	Description
C&C Server and Malware Source Locations	<p>Displays a world map showing the number of threat event count across countries.</p> <p>You can sort the information based on the time period ranging from 5 minutes to 30 days.</p>
Top Infected File Categories	<p>Displays a graph of the top infected file categories.</p> <p>You can sort the information based on the time period ranging from 5 minutes to 30 days.</p>
Top Scanned File Categories	<p>Displays a graph of the top file types scanned for malware.</p> <p>You can sort the information based on the time period ranging from 5 minutes to 30 days.</p>

Table 4: Widgets on the Dashboard (Continued)

Widget	Description
Top Malware Identified	<p>Displays the top malware found based on the number of times the malware is detected over a period of time.</p> <p>You can sort the information based on the time period ranging from 5 minutes to 30 days.</p>
Top Compromised Hosts	<p>Displays the top compromised hosts based on their associated threat level and blocked status.</p> <p>You can sort the information based on the time period ranging from 5 minutes to 30 days.</p>
VPN Tunnel Status	Displays the status of the VPN tunnels.
Devices Connection Status	<p>Displays the connection status of devices.</p> <p>You can filter the widget by the connection status.</p>
Devices by OS Versions	<p>Displays devices based on the software versions.</p> <p>You can filter the widget by the software version.</p>
Devices by Platforms	<p>Displays devices based on the device platform.</p> <p>You can filter the widget by the platform.</p>
Device Subscriptions Status	<p>Displays the subscription status of devices.</p> <p>You can filter the widget by the subscription status.</p>
Device Management Entitlements	<p>Displays the subscriptions based on devices associated with the subscriptions.</p> <p>You can filter the widget by used or unused subscriptions.</p>
Overall Storage	Displays the storage used by the organization of the user.

Table 4: Widgets on the Dashboard (Continued)

Widget	Description
Threat Map: IPS	<p>Displays a world map showing total IPS event count across countries.</p> <p>You can sort the information based on the source, the destination, and the time period ranging from 5 minutes to 7 days.</p>
Threat Map: Virus	<p>Displays a world map showing the total virus event count across countries.</p> <p>You can sort the information based on the source, the destination, and the time period ranging from 5 minutes to 7 days.</p>
Firewall: Top Events	<p>Displays a bar chart of the top firewall events of the network traffic sorted by count.</p> <p>You can sort the information based on the time period ranging from 5 minutes to 7 days.</p>
Firewall: Top Denials	<p>Displays a column chart of the top requests denied by the firewall based on the source IP addresses sorted by count.</p> <p>You can sort the information based on the time period ranging from 5 minutes to 7 days.</p>
IP: Top Sources	<p>Displays the top IP source addresses of the network traffic sorted by count.</p> <p>You can sort the information based on the time period ranging from 5 minutes to 7 days.</p>
IP: Top Destinations	<p>Displays the top IP destination addresses of the network traffic sorted by count.</p> <p>You can sort the information based on the time period ranging from 5 minutes to 7 days.</p>

Table 4: Widgets on the Dashboard *(Continued)*

Widget	Description
NAT: Top Source Translations	<p>Displays the top source IP addresses that are translated sorted by count.</p> <p>You can sort the information based on the time period ranging from 5 minutes to 7 days.</p>
NAT: Top Destination Translations	<p>Displays the top destination IP addresses that are translated sorted by count.</p> <p>You can sort the information based on the time period ranging from 5 minutes to 7 days.</p>
Top Source IPs by Volume	<p>Displays the top source IP addresses based on the volume of traffic sorted by count.</p> <p>You can sort the information based on time period ranging from 15 minutes to 7 days.</p>
Virus: Top Blocked	<p>Displays viruses with the maximum number of blocks sorted by count.</p> <p>You can sort the information based on the time period ranging from 5 minutes to 7 days.</p>
Web Filtering: Top Blocked	<p>Displays a bar chart of websites with the maximum number of blocks sorted by count.</p> <p>You can sort the information based on the time period ranging from 5 minutes to 7 days.</p>
Applications: Most Sessions	<p>Displays a bar chart of the top applications with a maximum number of sessions sorted by count.</p> <p>You can sort the information based on the time period ranging from 5 minutes to 7 days.</p>

Table 4: Widgets on the Dashboard *(Continued)*

Widget	Description
Top Applications by Volume	<p>Displays the applications based on volume of traffic sorted by count.</p> <p>You can sort the information based on the time period ranging from 5 minutes to 7 days and view the information in a bar chart or a bubble chart.</p>
Top Spams by Source	<p>Displays the number of spams detected by the source IP addresses.</p> <p>You can sort the information based on the time period ranging from 5 minutes to 7 days.</p>
IPS: Top Attacks	<p>Displays the top IPS events of the network traffic sorted by count.</p> <p>You can sort the information based on the time period ranging from 5 minutes to 7 days.</p>
Secure Edge	
Top 5 Users by Bandwidth	<p>Displays the top 5 users by bandwidth usage.</p> <p>You can sort the information based on the time period ranging from 5 minutes to 30 days.</p>
Top 5 Service Locations by Users	<p>Displays the top 5 service locations by number of users.</p> <p>You can sort the information based on the time period ranging from 5 minutes to 30 days.</p>
Top 3 Sites by Bandwidth	<p>Displays the top 3 sites by bandwidth usage.</p> <p>You can sort the information based on the time period ranging from 5 minutes to 30 days.</p>

Table 4: Widgets on the Dashboard *(Continued)*

Widget	Description
Top 3 Service Locations by Bandwidth	<p>Displays the top 3 service locations by number of users.</p> <p>You can sort the information based on the time period ranging from 5 minutes to 30 days.</p>
Top 5 Sites by Users	<p>Displays the top 5 sites by number of users.</p> <p>You can sort the information based on the time period ranging from 5 minutes to 30 days.</p>
Overview	<p>Displays the average bandwidth usage and percentage of users.</p> <p>You can sort the information based on the time period ranging from 5 minutes to 30 days.</p>
Monitored Tunnels Up/Down	Displays all the tunnels with their current status.
Total Service Locations	Displays all the service locations with their current status.
CASB	

Table 4: Widgets on the Dashboard (Continued)

Widget	Description
Sanctioned and Unsanctioned Applications	<p>Displays the sanctioned and unsanctioned applications sorted by count.</p> <p>You can do the following tasks:</p> <ul style="list-style-type: none"> • Hover over the widget to refresh or remove the widget from the dashboard. • Hover over Time Span to sort the information based on the time period ranging from 15 minutes to 30 days. • Hover over the chart to view the number of sanctioned and unsanctioned applications with utilization (%). • Click More Details to view application details in the Monitor > Maps & Charts > CASB Applications > CASB Application Visibility page.
Sanctioned and Unsanctioned Application Instances	<p>Displays the sanctioned and unsanctioned application instances sorted by count.</p> <p>You can do the following tasks:</p> <ul style="list-style-type: none"> • Hover over the widget to refresh or remove the widget from the dashboard. • Hover over Time Span to sort the information based on the time period ranging from 15 minutes to 30 days. • Hover over the chart to view the number of sanctioned and unsanctioned application instances with utilization (%). • Click More Details to view application instance log details in the Monitor > Logs > CASB page.

Table 4: Widgets on the Dashboard (Continued)

Widget	Description
Applications: Most Sessions	<p>Displays a bar chart of the applications with a maximum number of sessions sorted by count.</p> <p>You can do the following tasks:</p> <ul style="list-style-type: none"> • Hover over the widget to refresh or remove the widget from the dashboard. • Hover over View to view the information in bar chart, bubble chart, or donut chart. • Hover over Time Span to sort the information based on the time period ranging from 15 minutes to 30 days. • Click More Details to view application session details in the Monitor > Maps & Charts > CASB Applications > CASB Application Visibility page.
Top Applications by Volume	<p>Displays the applications based on volume of traffic sorted by count.</p> <p>You can do the following tasks:</p> <ul style="list-style-type: none"> • Hover over the widget to refresh or remove the widget from the dashboard. • Hover over View to view the information in bar chart, bubble chart, or donut chart. • Hover over Time Span to sort the information based on the time period ranging from 15 minutes to 30 days. • Click More Details to view application volume details in the Monitor > Maps & Charts > CASB Applications > CASB Application Visibility page.

Table 4: Widgets on the Dashboard (Continued)

Widget	Description
Application Instance Categories	<p>Displays a chart of the application instance categories.</p> <p>You can do the following tasks:</p> <ul style="list-style-type: none"> • Hover over the widget to refresh or remove the widget from the dashboard. • Hover over the chart to view the number of application instance categories with utilization (%). • Hover over Time Span to sort the information based on the time period ranging from 15 minutes to 30 days. • Click More Details to view application instance category log details in the Monitor > Logs > CASB page.
Application Summary	<p>Displays the application summary details of users, volume, and session.</p> <p>You can do the following tasks:</p> <ul style="list-style-type: none"> • Hover over the widget to refresh or remove the widget from the dashboard. • Hover over Time Span to sort the information based on the time period ranging from 15 minutes to 30 days. • Click More Details to view application summary details in the Monitor > Maps & Charts > CASB Applications > CASB Application Visibility page.

3

PART

Monitor

[Alerts | 31](#)

[Logs | 41](#)

[Insights | 77](#)

[Maps and Charts | 82](#)

[Tunnel Status | 100](#)

[Service Locations | 106](#)

[Advanced Threat Prevention | 108](#)

[Reports | 155](#)

[Report Definitions | 159](#)

[Generated Reports | 181](#)

[ATP Report Definitions | 183](#)

[ATP Generated Reports | 190](#)

[Secure Edge Reports | 197](#)

Alerts

IN THIS CHAPTER

- Alerts Overview | 31
- Search Alerts | 33
- Delete an Alert | 33
- Using Generated Alerts | 33
- Alert Definitions Main Page Fields | 34
- Create Alert Definitions | 34
- Edit Alert Definitions | 36
- Clone Alert Definition | 37
- Delete Alert Definitions | 37
- Search Alert Definitions | 37
- About the Tunnel Status Alerts | 38

Alerts Overview

IN THIS SECTION

- Understanding Role-Based Access Control for the Alerts and Alert Definitions | 32

Alerts and notifications notify administrators about significant events within the system. Notifications can also be sent through e-mail. You will be notified when predefined network traffic condition is met. Alert trigger threshold is number of network traffic events crossing a pre-defined threshold within a period of time.

Alerts and notifications provide options for:

- Defining alert criteria based on a set of predefined filters. You can use the filters defined in the Filter Management window on the Event Viewer page to generate alerts.
- Generating an alert message and notifying you when alert criteria are met.
- Searching for specific alerts on the Generated Alerts page based on alert ID, description, alert definition, alert type, or recipient e-mail address.
- Supporting event-based alerts.

For example, an administrator can define a condition such that if the number of firewall-deny events crosses a predefined threshold in a given time range for a specific device, administrators will receive an e-mail alert.

NOTE: If the number of logs matching the alert criteria crosses the defined threshold and remains so for the period set in the alert definition, Juniper Security Director Cloud does not generate new alerts but only updates the time of the last occurrence. It generates new alerts again only when both these conditions are met:

- The number of logs matching the alert criteria drops below the threshold and crosses the threshold again.
- The number of logs crosses the defined threshold again after the time period set in the alert definition elapses. Juniper Security Director Cloud measures this time period from the first time the threshold is crossed in the configured time range.

Understanding Role-Based Access Control for the Alerts and Alert Definitions

NOTE: You must have Security Analyst or Security Architect role or have permissions equivalent to that role to access the alerts and alert definitions.

You must have the following privileges under **Administration > Users & Roles > Roles**:

- **Create Alert Definition** to create an alert definition.
- **Update Alert Definition** to modify alerts.
- **Delete Alert Definition** to delete alerts.
- **User account** under Role Based Access Control to search for user accounts in alert definitions.

Search Alerts

To quickly locate an alert use the search option on the upper right side of the Alerts page:

1. Enter the alert ID, description, or alert name in the search box.
2. Click the search icon.

Delete an Alert

To delete an alert or multiple alerts:

1. Select **Monitor > Alerts > Alerts**.
2. Select an alert or multiple alerts for deletion.
3. On the upper left side of the Alerts page, click the delete icon (X).
The delete alert notification is displayed.
4. Click **OK**.
The alert is deleted.

Using Generated Alerts

Before You Begin

- Read the ["Alerts Overview" on page 31](#) topic.
- Review the Generated Alerts main page for an understanding of existing generated alerts. See ["Alert Definitions Main Page Fields" on page 34](#) for field descriptions.

Use the Generated Alerts page to view the system event-based alerts in response to a configured alert definition. The generated alerts help you to identify problems that appear in your monitored network environment. You can view statistics such as the number of critical and non-critical alerts.

To use the Generated Alerts page:

1. Select **Monitor > Alerts > Alerts**. The Alerts page appears.
2. Select the generated alert and then right-click or click **More > Detail View** to view the detailed information about the generated alert.

Alert Definitions Main Page Fields

Use this page to understand the alert definitions. [Table 5 on page 34](#) describes the fields on this page.

Table 5: Alert Definition Main Page Field

Field	Description
Select	Provides the option to select the available alerts.
Alert Name	Specifies the name of the alert.
Alert Description	Specifies the description of the alert.
Filter	Specifies the filter generating the alerts.
Recipients	Specifies the recipients of the alerts generated from the alert definitions.
Status	Specifies the status of the alert as active or inactive.
Severity	Specifies the severity level of the alert: Info, minor, major, critical.
Alert Type	Specifies the type of alert such as system based.

Create Alert Definitions

Before You Begin

- Read the ["Alerts Overview" on page 31](#) topic.
- Review the Alert Definitions main page for an understanding of your current data set. See ["Alert Definitions Main Page Fields" on page 34](#) for field descriptions.

Use the Alert Definitions page to generate alerts that warn you of problems in your monitored environment. An alert definition consists of data criteria for triggering an alert. An alert is triggered when the event threshold exceeds the data criteria that is defined.

You can create an alert definition to monitor your data in real time. You can identify issues and attacks before they impact your network.

For example, if you are an administrator, you can define a condition such that if the number of firewall deny events crosses a predefined threshold in a given time frame for a specific device, you receive an email alert.

To create an alert definition:

1. Select **Monitor > Alert > Alert Definitions**.
2. Click the + icon.
3. Complete the configuration according to the guidelines provided in [Table 6 on page 35](#).
4. Click **Ok**.

A new alert definition with the configured alert triggering condition is created. You can view the generated alerts from the alert definition to troubleshoot the issues with your system.

Table 6: Alert Definitions Settings

Setting	Guideline
<i>General</i>	
Alert Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 63 characters.
Alert Description	Enter a description for the alerts. The maximum length is 1024 characters.
Alert Type	Displays the type of alert that is system based.
Status	Click the toggle button to view only the active alerts.
Severity	Select the severity level of the alert: Info, minor, major, critical.
<i>Trigger</i>	Displays the data criteria from the list of default and user-created filters that are saved from the Event Viewer.

Table 6: Alert Definitions Settings (Continued)

Setting	Guideline
Data Criteria	<p>Specifies the data criteria from the list of default and user-created filters that are saved from the Event Viewer.</p> <p>To add saved filters:</p> <ul style="list-style-type: none"> • Click the Use data criteria from filters link. The Add Saved Filters page appears. • Select the filters to be added. • Click OK.
Time Span	Specify the time period for triggering an alert.
Number of Events	Enter the event threshold (number of logs for each category). An alert triggers if the number exceeds the specified threshold. Range: between 1-1,000,000,000.
<i>Recipient(s)</i>	
E-mail address(es)	Specify the e-mail addresses for the recipients of the alert notification.
Custom Message	Enter a custom string for identifying the type of alert in the alert notification e-mail.

Edit Alert Definitions

To edit an alert definition:

1. Select **Alerts > Alert Definitions**.
2. Select the alert.
3. On the upper right side of the Alert Definitions page, click the pencil icon.

The edit alert definitions page is displayed showing the same options as when creating a new alert definitions.

4. Click **OK**.

RELATED DOCUMENTATION

| [Create Alert Definitions](#) | 34

Clone Alert Definition

You can clone an existing alert definition.

To clone an alert definition:

1. Select **Monitor > Alerts > Alert Definitions**.
2. Right-click an alert, or select **Clone** from the **More** link.
The Clone window appears with editable fields.
3. Click **OK** to save your changes.

Delete Alert Definitions

To delete an alert definition or multiple alert definitions:

1. Select **Monitor > Alerts > Alert Definitions**.
2. Select an alert definition or multiple alert definitions for deletion.
3. On the upper left side of the Alert Definitions page, click the delete icon.
The delete alert definition notification is displayed.
4. Click **OK**.
The alert definition is deleted.

Search Alert Definitions

To quickly locate an alert definition, use the search option on the upper right side of the **Monitor > Alerts > Alert Definitions** page:

1. Enter the alert definition name, description, or recipient name in the search box.
2. Click the search icon.

About the Tunnel Status Alerts

IN THIS SECTION

- [Tasks You Can Perform | 38](#)

To access this page, click **Monitor > Alerts > Tunnel Status Alerts**.

Use this page to view the tunnel status alerts for the configured tunnels between sites and service locations.

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

Tasks You Can Perform

You can perform the following tasks from this page:

- View a graphical representation of the alerts for a specified time range in the Time Range widget.
- The X-axis represents the defined time while the Y-axis represents the number of alerts.
- Use the slider to decrease or increase the time range of the alerts. You can also select from predefined time ranges such as 5m, 10m, 20m, 30m, 1h, 2h, 4h, 8h, 16h, 24h, or Custom.

If you select **Custom**, you must specify the dates and time range in MM/DD/YYYY and HH:MM:SS 24-hour or AM/PM formats to display the alerts for a specific period.

- View information related to tunnel status. See [No Link Title](#).
- View similar alerts. To do this, select a traffic log and click **Show exact match**.
- Filter on cell data. To do this, select an event row and then click **More > Filter on cell data**.

The search filter string is displayed in the advanced search field. The data in the corresponding column is filtered based on the filter string. Click **X** to clear the advanced search field.

- Exclude the cell data from the table. To do this, select an alert row that you want to exclude and then click **More > Exclude cell data**.

The search filter string is displayed in the advanced search field. The data in the respective column is excluded based on the filter condition. Click **X** to clear the advanced search field.

- Add filters. To do this:
 1. Click the filter icon and then select **Show advanced filter**.

The Add Criteria window opens.

2. Select the values for Field and Condition from the list.
3. Enter the value for the selected field and conditions.
4. Click **Add**.
5. Click **Save**.

The Save Filter page opens.

6. Enter a filter name and description and then click **OK**.

The filter is saved.

NOTE: Click **X** to clear the saved filters.

- Hide filters. To do this, click the filter icon and then select **Hide advanced filter**.
- View or load all the default or saved filters. To do this:
 1. Click the filter icon and then select **All Saved Filters**.
The View/Load Filters page opens.
 2. Select a saved filter and click **OK** to load the data based on filter conditions.
 3. Select a saved filter and click the delete icon on the upper-right corner of the page to delete it.
- Show or hide the columns displayed on the page. To do this, click the three vertical dots on the upper-right corner of the page and then select **Hide/Show Columns**. Select the columns that you want to display in the grid.
- Reset tunnel status alert monitoring preferences. To do this, click the three vertical dots on the upper-right corner of the page and then select **Reset Preference**.

[Table 7 on page 40](#) provides information related to tunnel status alerts.

Table 7: Tunnel Status Alerts

Fields	Description
Time	The time alerts are generated.
Generated By	The service location that generates the alerts.
Site Name	Name of the site.
Status	Status of the tunnel if it is up, down, or unavailable.

Logs

IN THIS CHAPTER

- [About the Session Page | 41](#)
- [Monitor CASB Logs | 46](#)
- [About the Threats Page | 51](#)
- [About the Web Filtering Events Page | 57](#)
- [About the IPsec VPNs Events Page | 63](#)
- [About the All Security Events Page | 68](#)
- [Monitor End User Authentication Logs | 74](#)

About the Session Page

IN THIS SECTION

- [Tasks You Can Perform | 42](#)

To access this page, click **Monitor>Logs>Session**.

You can use the Session page to view the details of the traffic logs that are generated by managed devices.

You can view the traffic logs that are generated in the past 24 hours. These traffic logs are used to debug certain events such as creating creation of sessions, deletion of sessions, and update sessions. You can also view the traffic logs for firewall and other security deployments.

The following examples indicate the types of logs that the Session page displays:

- RT_FLOW_SESSION_CREATE/CLOSE

- APTRACK_SESSION_CREATE/CLOSE and other APTRACK volume update events

NOTE: You must enable policy logging to view the traffic log data, and application tracking at the zone level to view APTRACK logs.

Tasks You Can Perform

You can perform the following tasks from this page:

- View a graphical representation of traffic logs for a specified time range in the Time Range widget.

The X-axis represents the defined time while, while the Y-axis represents the number of traffic logs.

Use the slider to decrease or increase the time range of the traffic logs. You can also select from predefined time ranges such as 5m, 10m, 20m, 30m, 1h, 2h, 4h, 8h, 16h, 24h, or Custom.

If you select Custom, you must specify the dates and time range in MM/DD/YYYY and HH:MM:SS 24-hour or AM/PM formats to display the traffic logs for a specific period.

- View information related to traffic logs. See [Table 8 on page 42](#) .
- View similar traffic logs. Select a traffic log, and click **Show exact match** to view similar logs.
- Group the traffic logs based on the options available in the **Group by** field.
For example, you can group traffic logs based on the destination country and the destination IP address.
- Show or hide the columns displayed on the page—Click the Show Hide Columns icon at the top-right corner of the page, and select the columns to display in the grid.

[Table 8 on page 42](#) provides information related to traffic logs.

Table 8: Columns on the Session Page

Fields	Description
Time	The time when the traffic log was generated.
Generated by	The user who generates the log.
Event Name	Te The event name of the traffic log.

Table 8: Columns on the Session Page (Continued)

Fields	Description
User Name	The username.
Source Country	The name of the country from where the event originated.
Source IP	The source IPv6 or IPv4 IPv4 or IPv6 address from where the event occurred.
Destination Country	The destination country name from where the event occurred.
Destination IP	The destination IPv4 or IPv6 address of the event.
URL	The accessed URL name that triggered the traffic log.
Category	The event category of the traffic log, suchh as, such as firewall or apptrack.
Application	The name of the application associated with the traffic that triggered the event.
Nested Application	The name of the Layer 7 application.
Received Time	The time when the traffic log was received by Juniper Security Director Cloud.
Policy Name	The policy name in the log.
Source Port	The source port of the event.
Destination Port	The destination port of the event.

Table 8: Columns on the Session Page (Continued)

Fields	Description
Description	The description of the log.
Threat Severity	The threat severity of the event.
Name	The name of the event.
Client Hostname	The hostname of the client associated with the traffic that triggered the event. For example, if a specific computer is infected, the name of that computer is displayed.
Event Category	The event category of the traffic log, such as firewall or apptrack.
Argument	The type of the traffic, such as FTP and HTTP.
Service Name	The name of the Layer 4 service used for the traffic that triggered the event, such as FTP, HTTP, SSH, and so on.
Source Zone	The source zone of the site.
Destination zone	The destination zone of the site.
Protocol ID	The protocol ID of the traffic that triggered the event.
Roles	The role names associated with the event.
Reason	The reason for the log generation, such as unrestricted access.
NAT Source Port	The source port of traffic after NAT traversal.

Table 8: Columns on the Session Page (Continued)

Fields	Description
NAT Destination Port	The destination port of traffic after NAT traversal.
NAT Source Rule Name	The source NAT rule name.
NAT Destination Rule Name	The destination NAT rule name.
NAT Source IP	The source IP address after IP address translation.
NAT Destination IP	The destination IP address after IP address translation.
Traffic Session ID	The Session The session ID mapped by the site to an event.
Path Name	The pathname of the log.
Logical System Name	The logical system name.
Rule Name	The rule name.
Profile Name	The name of the event profile that triggered the log.
Malware Info	The information about the malware causing the event.
Source VRF Group Name	The source VRF group name that generated the event.
Destination VRF Group Name	The destination VRF group name that generated the event.

Monitor CASB Logs

IN THIS SECTION

- [Tasks You Can Perform](#) | 46

To access this page, click **Monitor** > **Logs** > **CASB**.

Juniper Secure Edge provides full-stack Security Service Edge (SSE) capabilities to protect web, Software as a service (SaaS), and on-premises applications and provide users with consistent and secure access that follows them wherever they go.

Cloud Access Security Broker (CASB) provides visibility into the security of your cloud applications. You can apply granular controls to ensure authorized access, threat prevention, and compliance to secure your data.

When associated with a Secure Edge policy, a CASB profile collects logs from its configured cloud applications. Use this page to view and monitor these action-based and activity-based application logs.

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

Tasks You Can Perform

You can perform the following tasks from this page:

- View a graphical representation of traffic logs for a specified time range in the Time Range widget.
- The X-axis represents the defined time while the Y-axis represents the number of traffic logs.
- Use the slider to decrease or increase the time range of the traffic logs. You can also select from predefined time ranges such as 5m, 10m, 20m, 30m, 1h, 2h, 4h, 8h, 16h, 24h, or Custom.
- If you select Custom, you must specify the dates and time range in MM/DD/YYYY and HH:MM:SS 24-hour or AM/PM formats to display the traffic logs for a specific period.
- View information related to traffic logs. See [Table 9 on page 48](#) .
- View similar traffic logs. To do this, select a traffic log and click **Show exact match**.
- Group the traffic logs based on the options available in the **Group by** list.

For example, you can group the traffic logs based on the destination country and the destination IP address.

- View the complete details of logs. To do this, select the event row and then click **More > Detail**.
- Filter on cell data. To do this, select an event row and then click **More > Filter on cell data**.

The search filter string is displayed in the advanced search field. The data in the corresponding column is filtered based on the filter string. Click **X** to clear the advanced search field.

- Exclude cell data. To do this, select an event row and then click **More > Exclude cell data**.

The search filter string is displayed in the advanced search field. The data in the respective column is excluded based on the filter condition. Click **X** to clear the advanced search field.

- Add filters. To do this:
 1. Click the filter icon and then select **Show advanced filter**.

The Add Criteria window opens.

2. Select the values for Field and Condition from the list.
3. Enter the value for the selected field and conditions.
4. Click **Add**.
5. Click **Save**.

The Save Filter page opens.

6. Enter a filter name and description and then click **OK**.

The filter is saved.

NOTE: Click **X** to clear the saved filters.

- Hide filters. To do this, click the filter icon and then select **Hide advanced filter**.
- View or load all the default or saved filters. To do this:
 1. Click the filter icon and then select **All Saved Filters**.

The View/Load Filters page opens.
 2. Select a saved filter and click **OK** to load the data based on filter conditions.
 3. Select a saved filter and click the delete icon on the upper-right corner of the page to delete it.

- Show or hide the columns displayed on the page. To do this, click the three vertical dots on the upper-right corner of the page and then select **Hide/Show Columns**. Select the columns that you want to display in the grid.
- Reset CASB profile monitoring preferences. To do this, click the three vertical dots on the upper-right corner of the page and then select **Reset Preference**.

Table 9 on page 48 provides information related to action and activity based application logs.

NOTE: The Action and Activity Logs tabs only display the CASB-related application log information.

Table 9: CASB Page—Action and Activity Logs Tabs

Fields	Description
Action	View the action taken for the event: permit and deny.
Activity	View the activity logging for the CASB profile: Login, Upload, Download, and Share.
Application	View the cloud application name associated with the traffic that triggered the event.
Application Instance	View the application instances of the event.
Authentication Status	View the authentication status of the user.
Authentication Method	View the authentication method used by the user.
Category	View the event category of the traffic log.
Client Hostname	View the client hostname that is associated with the traffic that triggered the event. For example, if a specific computer is infected, the name of that computer is displayed.

Table 9: CASB Page—Action and Activity Logs Tabs (Continued)

Fields	Description
Description	View the description of the log.
Destination Country	View the destination country name from where the event occurred.
Destination IP	View the destination IP address of the event (IPv4 or IPv6).
Destination Port	View the destination port of the event.
Destination Zone	View the destination zone of the site.
Event Category	View the event category of the traffic log.
Event Name	View the event name of the traffic log.
Generated By	The device that generates the log.
Message	View the message received after the login authentication.
Name	View the name of the event.
Nested Application	View the name of the Layer 7 application.
Path Name	View the path name of the log.
Policy Name	View the policy name in the log.
Profile Name	View the name of the CASB profile that triggered the log.

Table 9: CASB Page—Action and Activity Logs Tabs (Continued)

Fields	Description
Protocol ID	Protocol ID of the traffic that triggered the event.
Received Time	View the time when the traffic log was received.
Roles	View the role names associated with the event.
Rule Name	View the rule name.
Service Name	View the name of the Layer 4 service used for the traffic that triggered the event. For example, FTP, HTTP, SSH, and so on.
Session ID	View the Session ID mapped by site to an event.
Site	View the sites for which application visibility data is available.
Source Country	View the source country name from where the event originated.
Source IP	View the source IP address from where the event occurred (IPv4 or IPv6).
Source Port	View the source port of the event.
Source Zone	View the source zone of the site.
Tag	View if the application instance is untagged, sanctioned, or unsanctioned.
Time	View the time when the traffic log was generated.

Table 9: CASB Page—Action and Activity Logs Tabs (Continued)

Fields	Description
Type	View if the cloud application access type is unclassified, work, or personal.
Username	View the username.
URL	View the accessed URL name that triggered the traffic log.

About the Threats Page

IN THIS SECTION

- [Tasks You Can Perform | 52](#)
- [Summary View | 52](#)
- [Detail View | 53](#)

To access this page, click **Monitor > Logs > Threats**.

Use the Threats page to view information about security events based on IPS policies. Analyzing IPS and content security logs yields useful security management information such as abnormal events, attacks, viruses, or worms.

The following examples indicate the types of logs that the Threats page displays:

- AV_VIRUS_DETECETED
- AV_FILE_NOT_SCANNED_DROPPED_MT, IDP_ATTACK_LOG_EVENT
- CONTENT_FILTER_BLOCKED
- ANTISPAM_SPAM_DETECTED_MT
- RT_AAMW - AAMW_HOST_INFECTED_EVENT_LOG

- SMS_MALICIOUS_VERDICT

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

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

NOTE: This information is sourced from IPS and content security features.

Tasks You Can Perform

You can perform the following tasks from this page:

- View a brief summary of all the all the IPS events in your network. See "[Summary View](#)" on page 52 .
- View the comprehensive details of events in a tabular format that includes sortable columns. See "[Detail View](#)" on page 53 .

Summary View

The data presented in the area graph is refreshed automatically based on the selected time range. You can use widgets to view critical information such as IPS severities, top sources, top destinations, top reporting devices, top IPS attacks, top source countries, and top destination countries.

[Table 10 on page 52](#) provides guidelines on using the widgets on the Detail View page.

Table 10: Widgets on the Summary Page

Field	Description
IPS Severities	View the top IPS severities of the events based on the severity level: critical, high, medium.
Top Sources	View the top source IP addresses of the network traffic; sorted by the number of event occurrences.

Table 10: Widgets on the Summary Page (Continued)

Field	Description
Top Destinations	View the top destination IP addresses of the network traffic; sorted by the number of event occurrences.
Top Reporting/Attacked Devices	View the top devices that are attacked by IPS events; sorted by the number of times users are active on the network.
Top IPS Attacks	View the top IPS attacks in the network traffic; sorted by the times devices are attacked.
Top Source Countries	View the top source countries from where the event source originated; sorted by the number of IP addresses.
Top Destination Countries	View the top destination countries from where the event source originated; sorted by the number of IP addresses.
Top Viruses	View viruses with the maximum number of blocks sorted by count.
Top Spam by Source	View the number of spams detected by the source IP addresses.

Detail View

You can sort the events using the Group By option. For example, you can sort the events based on threat severity. The table includes information such as the rule that caused the event, severity for the event, event ID, traffic information, and how and when the event was detected.

[Table 11 on page 54](#) provides guidelines on using the fields on the Detail View page.

Table 11: Fields on the Detail View Page

Fields	Description
Time	View the time when the traffic log was generated.
Generated by	The user who generates the log.
Event Name	View the event name of the traffic log.
Attack Name	View the attack name of the log: Trojan, worm, virus, and so on.
Threat Severity	View the threat severity of the event.
User Name	View the user name.
URL	View the accessed URL name that triggered the traffic log.
Nested Application	View the name of the Layer 7 application.
Action	View the action taken for the event: warning, allow, and block.
Source IP	View the source IP address from where the event occurred (IPv4 or IPv6).
Destination IP	View the destination IP address of the event (IPv4 or IPv6).
Destination Port	View the destination port of the event.
Received Time	View the time when the traffic log was received by Juniper Security Director Cloud.

Table 11: Fields on the Detail View Page (Continued)

Fields	Description
Policy Name	View the policy name in the log.
Source Country	View the source country name from where the event originated.
Destination Country	View the destination country name from where the event occurred.
Source Port	View the source port of the event.
Description	View the description of the log.
Name	View the name of the event.
Category	View the event category of the threat. Category can be Anti-spam, Anti-virus, Web-filtering, and IPS.
Client Hostname	Host name of the client associated with the traffic that triggered the event. For example, if a specific computer is infected, the name of that computer is displayed.
Event Category	View the event category of the traffic log (For example firewall or apptrack).
Argument	View the type of traffic. For example, FTP and HTTP.
Application	Name of the application associated with the traffic that triggered the event.
Host Name	Host name of the device where the log was generated

Table 11: Fields on the Detail View Page (Continued)

Fields	Description
Service Name	View the name of the Layer 4 service used for the traffic that triggered the event. For example, FTP, HTTP, SSH, and so on.
Source Zone	View the source zone of the site.
Destination zone	View the destination zone of the site.
Protocol ID	Protocol ID of the traffic that triggered the event.
Roles	View the role names associated with the event.
Reason	View the reason for the log generation. For example, unrestricted access.
NAT Source Port	View the source port of traffic after NAT.
NAT Destination Port	View the destination port of traffic after NAT.
NAT Source Rule Name	View the source NAT rule name.
NAT Destination Rule Name	View the destination NAT rule name.
NAT Source IP	View the source IP address after the IP address translation.
NAT Destination IP	View the destination IP address after the IP address translation.
Traffic Session ID	View the Session ID mapped by site to an event.
Path Name	View the path name of the log.

Table 11: Fields on the Detail View Page (Continued)

Fields	Description
Logical System Name	View the logical system name.
Rule Name	View the rule name.
Profile Name	View the name of the Web filtering profile that triggered the log.
Malware Info	Information about the malware causing the event.
Source VRF Group Name	View the source VRF group name that generated the event.
Destination VRF Group Name	View the destination VRF group name that generated the event.

About the Web Filtering Events Page

IN THIS SECTION

- [Tasks You Can Perform | 58](#)
- [Summary View | 58](#)
- [Detail View | 59](#)

To access this page, click **Monitor > Logs > Web Filtering**.

Use the Web Filtering page to view information about security events based on Web filtering policies. Web filtering allows you to permit or block access to specific websites by URL or by URL category using cloud-based lookups, a local database, or an external Websense server.

NOTE: You can only recategorize the Juniper NextGen URL categories. To recategorize the URL, right-click on the URL or click **More** and select **Request URL Categorization**. The Request URL Categorization page opens. For more information on the URL recategorization, see "[Request URL Recategorization](#)" on page 1049 .

The following examples indicate the types of logs that the Web Filtering Events page displays: WEBFILTER_URL_BLOCKED and all WEB filter related events

Analyzing Web filtering logs yields useful security management information such as users detected accessing restricted URLs and actions taken by the system. Using the time-range slider, you can quickly focus on the area of activity that you are most interested in. Once the time range is selected, all of the data presented in your view is refreshed automatically. You can also use the Custom button to set a custom time range.

NOTE: This information is sourced from Web filtering in content security.

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

Tasks You Can Perform

You can perform the following tasks from this page:

- View a brief summary of all the Web filtering events in your network. See "[Summary View](#)" on page 58 .
- View the comprehensive details of events in a tabular format that includes sortable columns. See "[Detail View](#)" on page 59 .

Summary View

The top of the page has an area graph of all the Web filtering events against the blocked events. Below the area graph are widgets displaying critical information such as top sources, top destinations, top users, and top reporting devices.

You can use the widgets at the bottom of the page to view critical information such as top URLs blocked, top matched profiles, top sources, and top destinations.

[Table 12 on page 59](#) describes the widgets on the Summary View page.

Table 12: Widgets on the Summary View Page

Widget	Description
Top URLs Blocked	View the URL names that are blocked; sorted by event count.
Top Reporting Devices	View the top devices reporting Web filtering events; sorted by event count.
Top Sources	View the top source IP addresses of the network traffic; sorted by event count.
Top Destinations	View the top destination IP addresses of the network traffic; sorted by event count.

Detail View

You can aggregate 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 address, source country, and so on.

[Table 13 on page 59](#) provides guidelines on using the fields on the Detail View page.

Table 13: Fields on the Detail View Page

Fields	Description
Time	View the time when the traffic log was generated.
Generated by	The user who generates the log.
Event Name	View the event name of the traffic log.
User Name	View the user name.

Table 13: Fields on the Detail View Page (Continued)

Fields	Description
Source Country	View the source country name from where the event originated.
Source IP	View the source IP address from where the event occurred (IPv4 or IPv6).
Destination Country	View the destination country name from where the event occurred.
Destination IP	View the destination IP address of the event (IPv4 or IPv6).
URL	View the accessed URL name that triggered the traffic log.
Category	View the event category of the traffic log (For example firewall or apptrack).
Application	Name of the application associated with the traffic that triggered the event.
Nested Application	View the name of the Layer 7 application.
Received Time	View the time when the traffic log was received by Juniper Security Director Cloud.
Policy Name	View the policy name in the log.
Source Port	View the source port of the event.
Destination Port	View the destination port of the event.

Table 13: Fields on the Detail View Page (Continued)

Fields	Description
Description	View the description of the log.
Attack Name	View the attack name of the log: Trojan, worm, virus, and so on.
Threat Severity	View the threat severity of the event.
Name	View the name of the event.
Client Hostname	Host name of the client associated with the traffic that triggered the event. For example, if a specific computer is infected, the name of that computer is displayed.
Event Category	View the event category of the traffic log (For example firewall or apptrack).
Argument	View the type of traffic. For example, FTP and HTTP.
Action	View the action taken for the event: warning, allow, and block.
Host Name	Host name of the device where the log was generated
Service Name	View the name of the Layer 4 service used for the traffic that triggered the event. For example, FTP, HTTP, SSH, and so on.
Source Zone	View the source zone of the site.
Destination zone	View the destination zone of the site.
Protocol ID	Protocol ID of the traffic that triggered the event.

Table 13: Fields on the Detail View Page (Continued)

Fields	Description
Roles	View the role names associated with the event.
Reason	View the reason for the log generation. For example, unrestricted access.
NAT Source Port	View the source port of traffic after NAT.
NAT Destination Port	View the destination port of traffic after NAT.
NAT Source Rule Name	View the source NAT rule name.
NAT Destination Rule Name	View the destination NAT rule name.
NAT Source IP	View the source IP address after the IP address translation.
NAT Destination IP	View the destination IP address after the IP address translation.
Traffic Session ID	View the Session ID mapped by site to an event.
Path Name	View the path name of the log.
Logical System Name	View the logical system name.
Rule Name	View the rule name.
Profile Name	View the name of the Web filtering profile that triggered the log.
Malware Info	Information about the malware causing the event.

Table 13: Fields on the Detail View Page (Continued)

Fields	Description
Source VRF Group Name	View the source VRF group name that generated the event.
Destination VRF Group Name	View the destination VRF group name that generated the event.

About the IPsec VPNs Events Page

IN THIS SECTION

- [Tasks You Can Perform | 64](#)
- [Summary View | 64](#)
- [Detail View | 64](#)

To access this page, click **Monitor** > **Logs** > **IPsec VPNs**.

Use this page to view information about security events based on IPsec VPN policies. The event viewer provides a view of all IPsec VPN events.

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

NOTE: This information is sourced from system syslog.

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

Tasks You Can Perform

You can perform the following tasks from this page:

- View a brief summary of all the IPsec VPN events in your network. See ["Summary View" on page 64](#).
- View the comprehensive details of events in a tabular format that includes sortable columns. See ["Detail View" on page 64](#).

Summary View

The top of the page has an area graph of all the VPN events. You can use the widgets at the bottom of the page to view critical information such as top sources, top destinations, and top reporting devices.

[Table 14 on page 64](#) describes the widgets on the Summary View page.

Table 14: Widgets on the Summary View Page

Widget	Description
Top Sources	View the top source IP addresses of the network traffic; sorted by event count.
Top Destinations	View the top destination IP addresses of the network traffic; sorted by event count.
Top Reporting Devices	View the top reporting device IP addresses; sorted by event count.

Detail View

You can aggregate 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, log source, host name, source country, and so on.

[Table 15 on page 65](#) provides guidelines on using the fields on the Detail View page.

Table 15: Fields on the Detail View Page

Fields	Description
Log Generated Time	View the time when the traffic log was generated.
Log Received Time	View the time when the traffic log was received by Juniper Security Director Cloud.
Policy Name	View the policy name in the log.
Event Name	View the event name of the traffic log.
Source Country	View the source country name from where the event originated.
Source IP	View the source IP address from where the event occurred (IPv4 or IPv6).
Destination Country	View the destination country name from where the event occurred.
Destination IP	View the destination IP address of the event (IPv4 or IPv6).
Source Port	View the source port of the event.
Destination Port	View the destination port of the event.
Description	View the description of the log.
Attack Name	View the attack name of the log: Trojan, worm, virus, and so on.
Threat Severity	View the threat severity of the event.

Table 15: Fields on the Detail View Page (Continued)

Fields	Description
Name	View the name of the event.
Category	View the event category of the traffic log (For example firewall or apptrack).
URL	View the accessed URL name that triggered the traffic log.
Event Category	View the event category of the traffic log (For example firewall or apptrack).
User Name	View the user name.
Argument	View the type of traffic. For example, FTP and HTTP.
Action	View the action taken for the event: warning, allow, and block.
Application	Name of the application associated with the traffic that triggered the event.
Host Name	Host name of the device where the log was generated
Service Name	View the name of the Layer 4 service used for the traffic that triggered the event. For example, FTP, HTTP, SSH, and so on.
Nested Application	View the name of the Layer 7 application.
Source Zone	View the source zone of the site.
Destination zone	View the destination zone of the site.

Table 15: Fields on the Detail View Page (Continued)

Fields	Description
Protocol ID	Protocol ID of the traffic that triggered the event.
Roles	View the role names associated with the event.
Reason	View the reason for the log generation. For example, unrestricted access.
NAT Source Port	View the source port of traffic after NAT.
NAT Destination Port	View the destination port of traffic after NAT.
NAT Source Rule Name	View the source NAT rule name.
NAT Destination Rule Name	View the destination NAT rule name.
NAT Source IP	View the source IP address after the IP address translation.
NAT Destination IP	View the destination IP address after the IP address translation.
Traffic Session ID	View the Session ID mapped by site to an event.
Path Name	View the path name of the log.
Logical System Name	View the logical system name.
Rule Name	View the rule name.
Profile Name	View the name of the IPsec VPN profile that triggered the log.

Table 15: Fields on the Detail View Page (Continued)

Fields	Description
Client Hostname	Host name of the client associated with the traffic that triggered the event. For example, if a specific computer is infected, the name of that computer is displayed.
Malware Info	Information about the malware causing the event.
Source VRF Group Name	View the source VRF group name that generated the event.
Destination VRF Group Name	View the destination VRF group name that generated the event.

About the All Security Events Page

IN THIS SECTION

- [Tasks You Can Perform | 69](#)
- [Summary View | 69](#)
- [Detail View | 70](#)

To access this page, click **Monitor > Logs > All Security Events**.

Use this page to get an overall, high-level view of your network environment. You can view abnormal events, attacks, viruses, or worms when log data is correlated and analyzed.

The following examples indicate the types of logs that the All Security Events page displays:

- AV_VIRUS_DETECETED
- IDP_ATTACK_LOG_EVENT
- CONTENET_FILETER_BLOCKED

- ANTISPAM_SPAM_DETECTED_MTSECINTEL_ACTION_LOG
- AAMW_ACTION_LOG
- SMS_MALICIOUS_VERDICT
- RT_FLOW_SESSION_DENY
- TUN-STATUS-ALERT
- SECINTEL_ACTION_LOG
- AAMW_SMS_STREAMING_LOG

This page provides administrators with an advanced filtering mechanism and provides visibility into actual events collected by the Log Collector. Using the time-range slider, you can instantly focus on areas of unusual activity by dragging the time slider to the area of interest to you. The slider and the Custom button under Time Range remain at the top of each tab. Users select the time range, and then they can decide how to view the data, using the summary view or detail view tabs.

NOTE: This information is sourced from system syslog for the VPN events, and IPS, content security, firewall deny logs (when logging is enabled on policies) for all other events.

Tasks You Can Perform

You can perform the following tasks from this page:

- View a brief summary of all events in your network. See ["Summary View" on page 69](#) .
- View the comprehensive details of events in a tabular format that includes sortable columns. See ["Detail View" on page 70](#) .

Summary View

You can view a brief summary of all the events in your network. At the center of the page is critical information, including total number of events, viruses found, total number of interfaces that are down, number of attacks, CPU spikes, system reboots, and sessions. This data is refreshed automatically based on the selected time range.

At the bottom of the page is an area view of different events that are happening at a specific time. The events include firewall, Web filtering, VPN, content filtering, antispam, antivirus, screen, IPS, and IPsec VPN. Each event is color-coded, with darker shades representing a higher level of activity. Each tab provides deep information like type, and number of events occurring at that specific time.

[Table 16 on page 70](#) describes the widgets on the All Events Summary View page.

Table 16: Widgets on the All Security Events Summary View Page

Field	Description
Total Events	View the total number of events that includes firewall, web filtering, IPS, IPsec VPNs, content filtering, antispam, antivirus, and screen.
Firewall	View the total number of events blocked by the firewall.
Web Filtering	View the total number of URLs permitted and blocked.
Screen	View the total number of blocked screen events.
IPS	View the data seen by the IDP engine and categorized as Critical, High, Medium.
Content Filtering	View the details of the blocked traffic.
Antispam	View the details of the blocked traffic.
Antivirus	View the details of the blocked traffic.

Detail View

Click **Detail View** for comprehensive details of events in a tabular format that includes sortable columns. You can sort the events using the Group By option. For example, you can sort the events based on threat severity. The table includes information such as the rule that caused the event, severity for the event, event ID, traffic information, and how and when the event was detected.

[Table 17 on page 71](#) describes the fields on the All Events Detail View Page.

Table 17: Fields on the All Events Detail View Page

Fields	Description
Time	View the time when the traffic log was generated.
Generated By	
Traffic Session ID	View the Session ID mapped by site to an event.
User Name	View the user name.
Source IP	View the source IP address from where the event occurred (IPv4 or IPv6).
Destination IP	View the destination IP address of the event (IPv4 or IPv6).
Application	Name of the application associated with the traffic that triggered the event.
Nested Application	View the name of the Layer 7 application.
Threat Severity	View the threat severity of the event.
URL	View the accessed URL name that triggered the traffic log. You can only recategorize the Juniper NextGen URL categories. To recategorize the URL, right-click on the URL or click More and select Request URL Categorization . The Request URL Categorization page opens. For more information on the URL recategorization, see " Request URL Recategorization " on page 1049 .
Name	View the name of the event.

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

Fields	Description
Received Time	View the time when the traffic log was received by Juniper Security Director Cloud.
Policy Name	View the policy name in the log.
Event Name	View the event name of the traffic log.
Source Country	View the source country name from where the event originated.
Destination Country	View the destination country name from where the event occurred.
Source Port	View the source port of the event.
Destination Port	View the destination port of the event.
Description	View the description of the log.
Attack Name	View the attack name of the log: Trojan, worm, virus, and so on.
Category	View the event category of the traffic log (For example firewall or apptrack).
Client Hostname	Host name of the client associated with the traffic that triggered the event. For example, if a specific computer is infected, the name of that computer is displayed.
Event Category	View the event category of the traffic log (For example firewall or apptrack).

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

Fields	Description
Argument	View the type of traffic. For example, FTP and HTTP.
Action	View the action taken for the event: warning, allow, and block.
Service Name	View the name of the Layer 4 service used for the traffic that triggered the event. For example, FTP, HTTP, SSH, and so on.
Source Zone	View the source zone of the site.
Destination zone	View the destination zone of the site.
Protocol ID	Protocol ID of the traffic that triggered the event.
Roles	View the role names associated with the event.
Reason	View the reason for the log generation. For example, unrestricted access.
NAT Source Port	View the source port of traffic after NAT.
NAT Destination Port	View the destination port of traffic after NAT.
NAT Source Rule Name	View the source NAT rule name.
NAT Destination Rule Name	View the destination NAT rule name.
NAT Source IP	View the source IP address after the IP address translation.

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

Fields	Description
NAT Destination IP	View the destination IP address after the IP address translation.
Path Name	View the path name of the log.
Logical System Name	View the logical system name.
Rule Name	View the rule name.
Profile Name	View the name of the event profile that triggered the log.
Malware Info	Information about the malware causing the event.
Source VRF Group Name	View the source VRF group name that generated the event.
Destination VRF Group Name	View the destination VRF group name that generated the event.

Monitor End User Authentication Logs

IN THIS SECTION

- [Tasks You Can Perform | 75](#)
- [Summary View | 75](#)
- [Detail View | 75](#)

To access this page, click **Monitor > Logs > End User Authentication**.

Use this page to get an overall, high-level view of end user authentication status.

Using the time-range slider, you can instantly focus on areas of unusual activity by dragging the time slider to the area of interest to you. The slider and the Custom button under Time Range remain at the top of each tab. Users select the time range, and then they can decide how to view the data, using the summary view or detail view tabs.

Tasks You Can Perform

You can perform the following tasks from this page:

- View a brief summary of all end user authentications. See [Table 18 on page 75](#) .
- View the comprehensive details of end user authentication in a tabular format that includes sortable columns. See [Table 19 on page 76](#) .

Summary View

You can view a brief summary of all the authentications and the top five authentication failures.

[Table 18 on page 75](#) describes the widgets on the All Events Summary View page.

Table 18: Widgets on the End User Authentication Summary View Page

Field	Description
Authentication Count	The total number of authentications.
Top 5 Failed Authentications	The details of top five failed authentication.

Detail View

Click **Detail View** for comprehensive details of end user authentication events in a tabular format that includes sortable columns. The table includes information such as the rule that caused the event, severity for the event, event ID, traffic information, and how and when the event was detected.

[Table 19 on page 76](#) describes the fields on the All Events Detail View Page.

Table 19: Fields on the End User Authentication Detail View Page

Fields	Description
Time	The time when the end user authentication log was generated.
User Name	The name of the user who was authenticated.
Generated By	The administrator who generated the authentication log.
Source IP	The source IP address from where the log occurred (IPv4 or IPv6).
Authentication Status	The status (success or failure) of end user authentication.
Authentication Method	The authentication method used by the user.
Message	The description for the authentication.
Received Time	The time when the authentication log was received by Juniper Secure Edge.
Event Name	The event name of the authentication log.
Source Country	View the source country name from where the authentication log originated.
Event Category	The event category of the authentication log.

Insights

IN THIS CHAPTER

- [How to Monitor Incidents | 77](#)
- [How to Monitor Mitigation | 80](#)

How to Monitor Incidents

IN THIS SECTION

- [Timeline View | 80](#)

Use the Incidents page to view all incidents related to a tenant in the selected time range. To access the Incidents page, select **Juniper Security Director Cloud > Monitor > Insights > Incidents**.

The data is displayed in grid view. In the Timeline section, you can select a log parser from the list to view log data in the timeline graph. You can zoom in, zoom out, show all data, and refresh the data.

You can view the incident ID, status of the incident, progression, and so on. You can click an incident to view more details and create Service Now tickets if required.

Figure 2: Incidents Page

The screenshot displays the 'Incidents' page with a list of incidents and a detailed 'Incident Summary' panel on the right.

Incidents List:

Time	ID	Risk	Status	Action
Dec 15, 2022, 8:05:21...	2e897de7-1b08-4c...	High	IN	New
Dec 15, 2022, 6:37:16...	52434fff-4bff-46cb...	High	IN	New
Dec 15, 2022, 11:22:4...	e766a989-ecc4-4cc...	High	IN	New
Dec 15, 2022, 11:19:2...	97e7b3c6-b5fd-48...	High	IN	New
Dec 15, 2022, 10:22:0...	91a41de0-ee18-44...	High	IN	New
Dec 15, 2022, 9:48:41...	8eadf5b2-fabf-40...	High	IN	New

82 items

Timeline:

- log_parser_test-1900
- Default McAfee ePolicy Orchestrator Parser
- Default Juniper SRX Parser
- cloud_log
- Default Juniper ATP Appliance Parser
- Default CrowdStrike Parser
- IncidentTest
- jatp-1
- Cloud SRX

Incident Summary:

- Incident ID:** 2e897de7-1b08-4c38-bb25-259e54cc35bb
- Progression:**
 - Download: 0
 - Execution: 0
 - Infection: 1
 - Lateral: 0
 - Phishing: 0
 - Exploit: 0
- Status Info:**
 - Hostname:
 - Username: unauthenticated-user
 - IP Address:

After you create a ticket, the status of the incident changes to Acknowledged.

Table 20 on page 78 describes different fields available in the grid. You can view data for 10 mins, 30 mins, 1 hour, 8 hours, 1 day, 4 days, 7 days, and 30 days.

Table 20: Fields on the Incidents Page

Field Name	Description
Status	Specifies the status of the Service Now ticket. After you create a Service Now ticket, the status shows Acknowledged.
Incident ID	Specifies the incident ID.
Risk	Specifies the threat metric and severity rating.
Progression	Specifies the progression of an incident. For example, phishing, infection, and so on.

Table 20: Fields on the Incidents Page (Continued)

Field Name	Description
Threat Target	Specifies the IP address of the target.
Date & Time	Specifies the timestamp of the incident.

In the Status column, click **New** to set the incident status.

Select an incident right-click and select **Detail** to see the incident summary.

[Table 21 on page 79](#) explains the options available for each incident on the Incident Summary page.

Table 21: Options for Each Incident

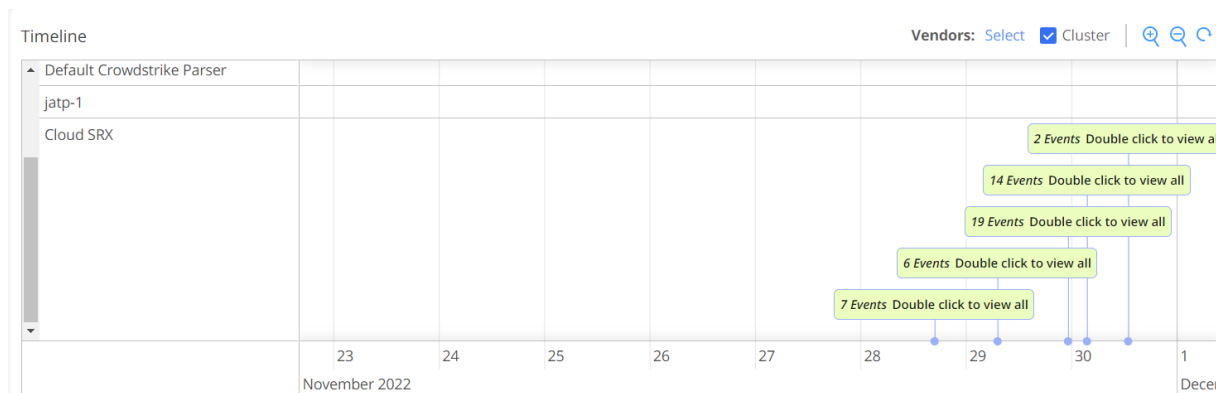
Option	Description
Incident Details	Click Incident Details to see the details of an incident.
Mitigate Incident	<p>Select Mitigate to enable or disable the Source IP Filtering/Endpoint IP Filtering mitigation if it's disabled and vice versa.</p> <p>To mitigate incidents, you must have already configured ATP Cloud. See ATP Mapping.</p>
Create Ticket	<p>Click Create Ticket to create a Service Now ticket for an incident. You must have already configured Service Now settings to create a Service Now ticket. See "About the Service Now Configuration" on page 1003 .</p> <p>To create a ServiceNow ticket:</p> <ol style="list-style-type: none"> 1. Select Create Ticket. The Create Service Now Ticket page is displayed. 2. In the Urgency field, select the priority of the ticket from the list. 3. In the Short Description field, provide a short description about the incident. 4. In the Description field, provide a more detailed description about the incident. 5. Click OK.

Timeline View

You can view all incidents on a timeline graph. Hover over each event to see more details about an incident. In the Vendors list, you can select the required log parser. You can select either one or all the log parsers. By default, the timeline graph shows all of the configured vendors in the log source.

You can enable the **Cluster** option to cluster events belonging to the same time.

Figure 3: Cluster View of Incidents

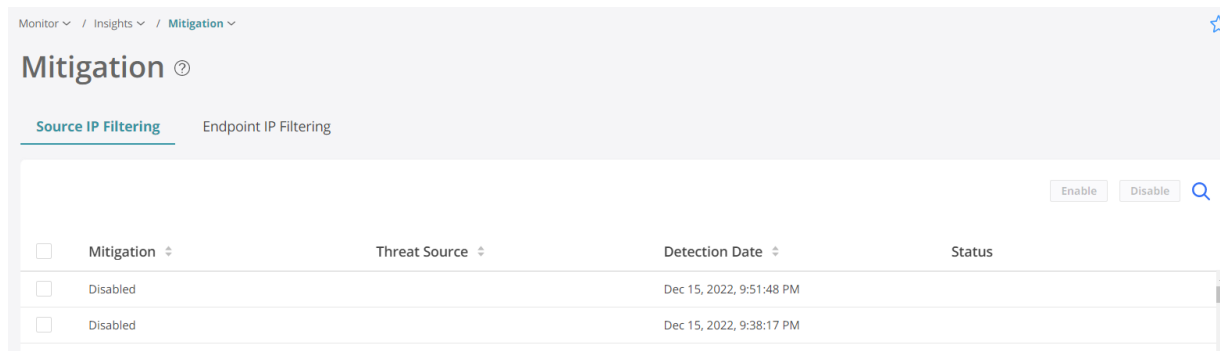


You can also zoom in, zoom out, and reset the data in the timeline graph. The reset option shows events for the corresponding incidents.

How to Monitor Mitigation

Using the Mitigation page, you can view the list of endpoints and threat sources that are mitigated by Security Director Cloud Insights. To access this page, select **Juniper Security Director Cloud > Monitor > Insights > Mitigation**. You can select an event and disable the mitigation, if enabled, and vice versa.

Figure 4: Incident Page



You can mitigate threat source IP addresses through ATP Cloud. You must configure ATP Cloud to enable the mitigation. See [ATP Mapping](#).

You can perform the following actions from the Mitigation page:

- Source IP filtering—Select the **Source IP Filtering** option to view only the threat source IP addresses that are mitigated by Security Director Cloud Insights.
- Endpoint IP filtering—Select the **Endpoint IP Filtering** option to view only the endpoint IP addresses that are mitigated by Security Director Cloud Insights.
- Search—You can search for data based on threat source or target IP addresses.
- Enable mitigation—If mitigation is disabled for an IP address, select an event for which you want to enable mitigation and click **Enable**. The Status column shows whether the enable task is successful.
- Disable mitigation—If you want to disable mitigation for an IP address, select an event for which you want to disable mitigation and click **Disable**. The Status column shows whether the disable task is successful or not.

Maps and Charts

IN THIS CHAPTER

- [Threat Map Overview | 82](#)
- [About the Application Visibility Page | 85](#)
- [About the CASB Application Visibility Page | 90](#)
- [About the User Visibility Page | 93](#)

Threat Map Overview

The threat map provides a visualization of the geographic regions for incoming and outgoing traffic. You can view blocked and allowed threat events based on feeds from IPS, antivirus, antispam engines, and screen attempts.

Clicking a specific geographical location displays an event count for each attack object. This event count view is useful for viewing unusual activity that could indicate a possible attack.

You can view the color-coded threats at the top of the page. You can also get a quick view of:

- The total number of threats blocked and allowed
- The individual count of threats blocked and allowed for each event
- The top targeted devices
- The top destination countries
- The top source countries

Clicking a threat displays the Threats page. The data on the Threats page is filtered based on the threat you clicked. For example, if you click the threat count of the IPS threats, the filtered results display only the IPS threat logs.

You can click any individual source or destination point on the threat map to review information about the threat events. The information includes the number of threat events, the type of threats, the time of

events, the source IP address, and the destination IP address. You can also perform further analysis of the attack by clicking the attack type and viewing the filtered list of events from the Event Viewer.

You can click a country on the threat map to display the respective country page. You can view the total threat events since midnight, followed by inbound and outbound threat events. The threat map displays the highest top five inbound and outbound IP addresses, but you can also view all IP addresses.

Click **View Details** to see more details for the country on the right panel. In addition, you can view the total number of inbound and outbound threats for each event.

NOTE: Threats with unknown geographical IP addresses are displayed as undefined.

Table 22 on page 83 describes different types of threats blocked and allowed.

Table 22: Types of Threats

Attack	Description
IPS Threats	<p>Intrusion detection and prevention (IDP) attacks detected by the IDP module.</p> <p>The information reported about the attack includes:</p> <ul style="list-style-type: none"> • The source of the attack • The destination of the attack • The type of attack • The session information • The severity • The policy information that permitted the traffic • The action taken: traffic permitted or dropped

Table 22: Types of Threats (Continued)

Attack	Description
Virus	<p>Virus attacks detected by the antivirus engine.</p> <p>The information reported about the attack includes:</p> <ul style="list-style-type: none"> • The source of the infected file • The destination • The file name • The URL used for accessing the file
Spam	<p>The e-mail spam that is detected based on the blocklist of spam e-mails.</p> <p>The information reported about the attack includes:</p> <ul style="list-style-type: none"> • The source • The action taken: The e-mail is rejected or allowed • The reason for identifying the e-mail as spam
Screen	<p>A type of threat detected by the SRX Series Firewalls.</p> <p>The information reported about the attack includes:</p> <ul style="list-style-type: none"> • The attack name • The action taken • The source of the attack • The destination of the attack

About the Application Visibility Page

IN THIS SECTION

- [Prerequisites | 85](#)
- [Tasks You Can Perform | 86](#)
- [Card View | 86](#)
- [Grid View | 88](#)

To access this page, select **Monitor > Maps & Charts > Applications**.

Juniper Security Director Cloud supports application visibility, a feature that enables you to protect your network against application-level threats.

The feature provides security management information such as the type, bandwidth consumption, and behavior of applications running on your network. You can use this information to identify application-level threats to your network. For example, you can identify threats posed by applications that consume excess bandwidth and cause data loss due to network bandwidth congestion. You can also control the applications at a granular level by managing the type of traffic allowed to enter or exit the network.

There are two ways in which you can view your application visibility data—**Card View** or **Grid View**. By default, the data is displayed in **Card View**.

Prerequisites

You need to do the following to view application visibility data:

- Ensure that an application signature package is installed on the SRX Series Firewall. For example:

```
show services application-identification version
Application package version: 3387
```

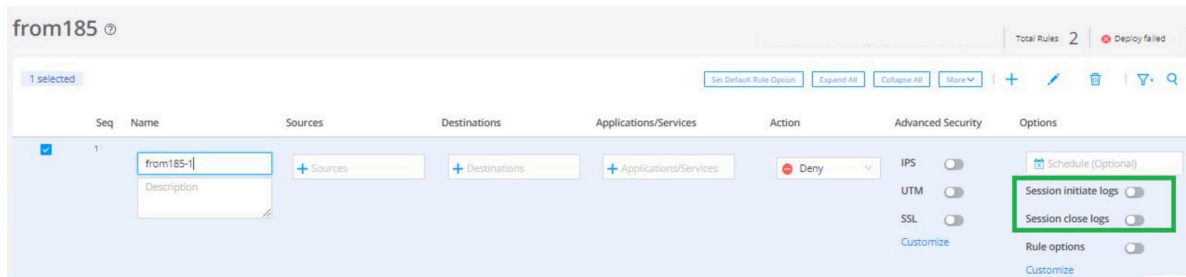
- Ensure that a dynamic application is applied on the firewall rule. For example:

```
set security policies from-zone trust to-zone untrust policy from185-1 match dynamic-
application any
```

You can also match the firewall rule to a specific dynamic application or group. For example:

```
set security policies from-zone trust to-zone untrust policy from185-2 match dynamic-
application junos:ICMP-ECHO
set security policies from-zone trust to-zone untrust policy from185-2 match dynamic-
application junos:ICMP-ECHO-REPLY
```

- Enable Session initiate logs and Session close logs on the firewall rule.



Tasks You Can Perform

You can perform the following tasks from this page:

- View application visibility data in **Card View**. See "[Card View](#)" on page 86 .
- View application visibility data in **Grid View**. See "[Grid View](#)" on page 88 .

Card View

Click the **Card View** link for a brief summary of the top 50 applications consuming the maximum bandwidth in your network. The data can be presented graphically as a bubble graph, heat map, or a zoomable bubble graph. The data is refreshed automatically based on the selected time range. You can also use the **Custom** option in the Time Span field to set a custom time range.

You can hover over your applications to view critical information such as total number of sessions, category, bandwidth consumed, risk levels, and characteristics. You can also view the top five users accessing your application.

[Table 23 on page 87](#) provides guidelines on using the fields on the **Card View** of the **Application Visibility** page.

Table 23: Fields on the Card View

Field	Description
Time Span	<p>Select the required time range to view a user's data.</p> <p>Use the custom option to choose the time range if you want to view data for more than one day.</p>
For	<p>Displays the sites for which application visibility data is displayed. By default, All Sites is selected. To view application visibility data for a specific site group:</p> <ol style="list-style-type: none"> 1. Click Edit to open the Add Site Group page. 2. Select the Selective option. 3. Select the site(s) you want to the site group from the available sites and click > to add the site(s) to the site group. 4. Click OK.
Show By	<p>Select from the following options to view a user's data:</p> <ul style="list-style-type: none"> • Bandwidth—Shows data based on the amount of bandwidth the application has consumed for a particular time range. • Number of Sessions—Shows data based on the number of sessions consumed by the application.
Select Graph	<p>Select from the following graphical representations to view an application's data:</p> <ul style="list-style-type: none"> • Bubble Graph • Heat Map • Zoomable Bubble Graph <p>By default, data is shown in the Bubble Graph format.</p>

Table 23: Fields on the Card View (Continued)

Field	Description
Group By	<p>Select from the following options to view the application's data:</p> <ul style="list-style-type: none"> • Risk-Grouped by critical, high, unsafe, and so on. • Category-Grouped by categories such as web, infrastructure, and so on.

Grid View

Click the **Grid View** link to obtain comprehensive details about applications. You can view top users by volume, top applications by volume, top category by volume, top characteristics by volume, and sessions by risk. You can also view the data in a tabular format that includes sortable columns. You can sort the applications in ascending or descending order based on application name, risk level, and so on. [Table 24 on page 88](#) describes the widgets in this view. Use these widgets to get an overall, high-level view of your applications, users, and the content traversing your network.

[Table 24 on page 88](#) provides guidelines on using the fields on the **Grid View** of the **Application Visibility** page.

Table 24: Widgets on the Grid View

Field	Description
Top Users By Volume	Top users of the application; sorted by bandwidth consumption.
Top Apps By Volume	Top applications using the network traffic, such as Amazon, Facebook, and so on, sorted by bandwidth consumption.
Top Category By Volume	The top category of the application, such as Web, infrastructure, and so on; sorted by bandwidth consumption.

Table 24: Widgets on the Grid View (Continued)

Field	Description
Top Characteristics By Volume	Top behavioral characteristics of the application, such as whether it is highly prone to misuse, the top bandwidth consumer, and so on.
Sessions By Risk	Number of events or sessions received; grouped by risk.

[Table 25 on page 89](#) describes the fields in the table below the widgets. Users are displayed by usernames or IP addresses. When you click a link, the **User Visibility** page appears in a grid view, with the correct filter applied. Sessions are also displayed as links and when you click a link, the **All Events** page appears with all security events.

Table 25: Detailed View of Applications

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

Table 25: Detailed View of Applications (Continued)

Field	Description
Characteristics	Characteristics of the application. For example, prone to misuse, bandwidth consumer, capable of tunneling.

About the CASB Application Visibility Page

IN THIS SECTION

- [Tasks You Can Perform | 90](#)
- [Summary View | 90](#)
- [Grid View | 91](#)

To access this page, click **Monitor** > **Maps & Charts** > **CASB Applications**.

Use the CASB Application Visibility page to view information related to CASB supported cloud applications and categories by its volume and session by risks associated with the applications.

There are two ways in which you can view your CASB application visibility data: **Summary View** or **Grid View**. By default, the data is displayed in Summary View.

Tasks You Can Perform

You can perform the following tasks from this page:

- View a summary of the CASB application visibility data. See "[Summary View](#)" on page 90 .
- View the comprehensive details of CASB application visibility data. See "[Grid View](#)" on page 91 .

Summary View

The data presented in the area graph is refreshed automatically based on the selected time range. You can use widgets to view critical information such as CASB supported cloud applications.

Table 26 on page 91 provides guidelines on using the widgets on the Summary View page

Table 26: Widgets on the Summary View Page

Field	Description
Time span	<p>Select the required time range to view a user's data.</p> <p>Use the custom option to choose the time range if you want to view data for more than one day.</p>
Show by	<p>Select from the following options to view a user's data:</p> <ul style="list-style-type: none"> • Volume—Shows data based on the volume consumed by the cloud application. • Number of Sessions—Shows data based on the number of sessions consumed by the cloud application.
Select graph	<p>Select from the following graphical representations to view a cloud application's data:</p> <ul style="list-style-type: none"> • Bubble Graph • Heat Map • Zoomable Bubble Graph <p>By default, data is shown in the Bubble Graph format.</p>
View by	<p>Select from the following options to view the cloud application's data:</p> <ul style="list-style-type: none"> • Risk-Grouped by critical, high, unsafe, and so on. • Category-Grouped by categories such as web, infrastructure, and so on.

Grid View

Click the Grid View link to obtain comprehensive details about cloud applications. You can view top applications by volume, top category by volume, and sessions by risk. You can also view the data in a

tabular format that includes sortable columns. You can sort the data in ascending or descending order based on the applications name, risk level, and so on.

[Table 27 on page 92](#) provides guidelines on using the fields on the Grid View of the CASB Application Visibility page. Use these widgets to get an overall, high-level view of your applications, users, and the content traversing your network.

Table 27: Widgets on the Grid View

Field	Description
Top Apps by Volume	Top cloud applications using the network traffic, such as Dropbox, Salesforce, and so on, sorted by bandwidth consumption.
Top Category by Volume	The top category of the cloud application, such as Web, infrastructure, and so on; sorted by bandwidth consumption.
Sessions by Risk	Number of events or sessions received; grouped by risk.

[Table 28 on page 92](#) describes the fields in the table below the widgets.

Table 28: Detailed View of Applications

Field	Description
Application Name	Name of the application, such as Dropbox, Salesforce, and so on.
Tag	Displays if the application instance is tagged as untagged, sanctioned, or unsanctioned.
Risk Level	Risk associated with the application: critical, high, unsafe, moderate, low, and unknown.
Users	Total number of users accessing the cloud applications.

Table 28: Detailed View of Applications (Continued)

Field	Description
Volume	Bandwidth used by the cloud application.
Total Sessions	Total number of cloud application sessions.
Category	Category of the cloud application, such as Web, infrastructure, and so on.
Sub Category	Subcategory of cloud application. For example, file sharing, applications, and miscellaneous.
Characteristics	Characteristics of cloud application. For example, prone to misuse, bandwidth consumer, capable of tunneling.

RELATED DOCUMENTATION

[CASB Overview | 722](#)

[About the Dashboard | 20](#)

[Monitor CASB Logs | 46](#)

About the User Visibility Page

IN THIS SECTION

- [Prerequisites | 94](#)
- [Tasks You Can Perform | 95](#)
- [Summary View | 95](#)
- [Grid View | 97](#)

To access this page, select **Monitor > Maps & Charts > Users**.

Use the User Visibility page to view information about users or source IP addresses (such as top 50 users or IP addresses accessing high bandwidth consuming applications or establishing higher number of sessions) on your network. Based on this information, network administrators can choose to rate-limit a device that is accessing applications which consume large bandwidth or create maximum traffic.

Prerequisites

You need to do the following to view user visibility data:

- Ensure that an application signature package is installed on the SRX Series Firewall. For example:

```
show services application-identification version
Application package version: 3387
```

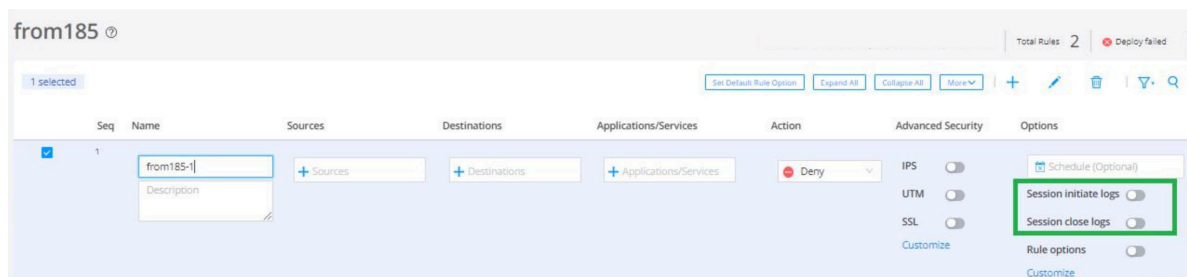
- Ensure that a dynamic application is applied on the firewall rule. For example:

```
set security policies from-zone trust to-zone untrust policy from185-1 match dynamic-
application any
```

You can also match the firewall rule to a specific dynamic application or group. For example:

```
set security policies from-zone trust to-zone untrust policy from185-2 match dynamic-
application junos:ICMP-ECHO
set security policies from-zone trust to-zone untrust policy from185-2 match dynamic-
application junos:ICMP-ECHO-REPLY
```

- Enable Session initiate logs and Session close logs on the firewall rule.



- Configure source identity on the firewall rule. Otherwise, the source IP address of the end host is displayed instead of the user name. See [User Role Firewall Security Policies](#).

Tasks You Can Perform

You can perform the following tasks from this page:

- View user visibility data in **Summary View**. See "[Summary View](#)" on page 95 .
- View user visibility data in **Grid View**. See "[Grid View](#)" on page 97 .

Summary View

Click the **Summary View** tab to view the data graphically as a bubble graph, heat map, or a zoomable bubble graph. The data is refreshed automatically based on the selected time span.

You can hover over the chart to view critical information such as the total number of sessions established and bandwidth consumed about each user.

Users are represented by the IP address or usernames of their devices on the network.

You can also view the top five applications of each user, based on either their bandwidth consumption or number of sessions established.

[Table 29 on page 95](#) provides guidelines on using the fields on the **Summary View** tab of the **User Visibility** page.

Table 29: Fields on the Summary View

Field	Description
Time Span	<p>Select the duration (last 15 minutes, last 30 minutes, last 45 minutes, last 1 hour, last 4 hours, last 8 hours, last 12 hours, last 1 day, or custom) for which you want to view the user visibility data.</p> <p>Select Custom to view data for more than one day.</p> <p>The Custom Time page appears.</p> <p>Specify the From date and To date (in MM/DD/YYYY format).The time span is from 00:00 through 23:59.</p>

Table 29: Fields on the Summary View (Continued)

Field	Description
For	<p>Displays the devices for which application visibility data is displayed. By default, All devices is selected. To view application visibility data for a specific device group:</p> <ol style="list-style-type: none"> 1. Click Edit to open the Add Device Group page. 2. Select the Selective option. 3. Select the devices(s) you want to add to the device group from the available devices and click > to add the devices(s) to the device group. 4. Click OK.
Show By	<p>Select the criterion to display information regarding the bandwidth consumed and number of sessions established by applications in the selected time span:</p> <ul style="list-style-type: none"> • Bandwidth—Displays users based on their bandwidth consumption. Users running applications that consume larger bandwidth are represented by larger bubbles or matrices. • Number of Session—Displays users based on the number of sessions established. Users running applications that have higher number of sessions established are represented by larger bubbles or matrices.
Select Graph	<p>Select one of the following options to view data graphically:</p> <ul style="list-style-type: none"> • Bubble Graph (default) • Heat Map • Zoomable Bubble Graph

Table 29: Fields on the Summary View (Continued)

Field	Description
Group By	<p>Select from the following options to view the application's data:</p> <ul style="list-style-type: none"> • Risk-Grouped by critical, high, unsafe, and so on. • Category-Grouped by categories such as web, infrastructure, and so on.

[Table 30 on page 97](#) describes the parameters that are displayed when you hover your cursor over the chart.

Table 30: Parameters on the Chart

Parameter	Description
User Name	Name of the user or source IP address accessing the application.
Bandwidth	Total Bandwidth consumed by the user (device).
Number of Sessions	Total number of application sessions established by the user (device).

Grid View

Click the **Grid View** tab to view high-level details of the users on your network. You can view widgets that provide information about top users by volume and top applications that create network traffic by volume. The data is also displayed in a tabular format with sortable columns.

[Table 31 on page 98](#) describes the widgets on the **Grid View** of the **User Visibility** page.

Table 31: Widgets on the Grid View

Field	Description
Top Users by Volume	Top users of applications, based on bandwidth consumption, for the selected time span.
Top Apps by Volume	Top applications accessed by users on the network, based on bandwidth consumption, for the selected time span. For example: Amazon

[Table 32 on page 98](#) describes the fields in the table below the widgets.

The table includes sortable columns, with the users (devices) represented by usernames or IP addresses.

Click the Search icon to enter the search text that can include a specific application or user name, or IP address of a device on the network.

Table 32: Detailed View of Users

Field	Description
User Name	IP address or username of the user (device) accessing the applications.
Volume	Bandwidth consumed by a user (who is represented by a user name or IP address).
Total Sessions	Total number of application sessions established by a specific user (device).

Table 32: Detailed View of Users (Continued)

Field	Description
Applications	<p>Name of the application accessed by a specific user (device).</p> <p>For example: Google</p> <p>NOTE: By default, this column lists only one application per user. If a user accesses more than one application, a +<integer>icon (for example: +2) appears to the right of the application name. The integer indicates the number of additional applications accessed by the user. Click the integer to view all applications accessed by a user.</p>

Tunnel Status

IN THIS CHAPTER

- [Tunnel Status Overview | 100](#)
- [About the Tunnel Status Page | 101](#)
- [Use the Advanced Filter to Monitor Specific Tunnels | 102](#)
- [About the Site Tunnel Status Page | 103](#)

Tunnel Status Overview

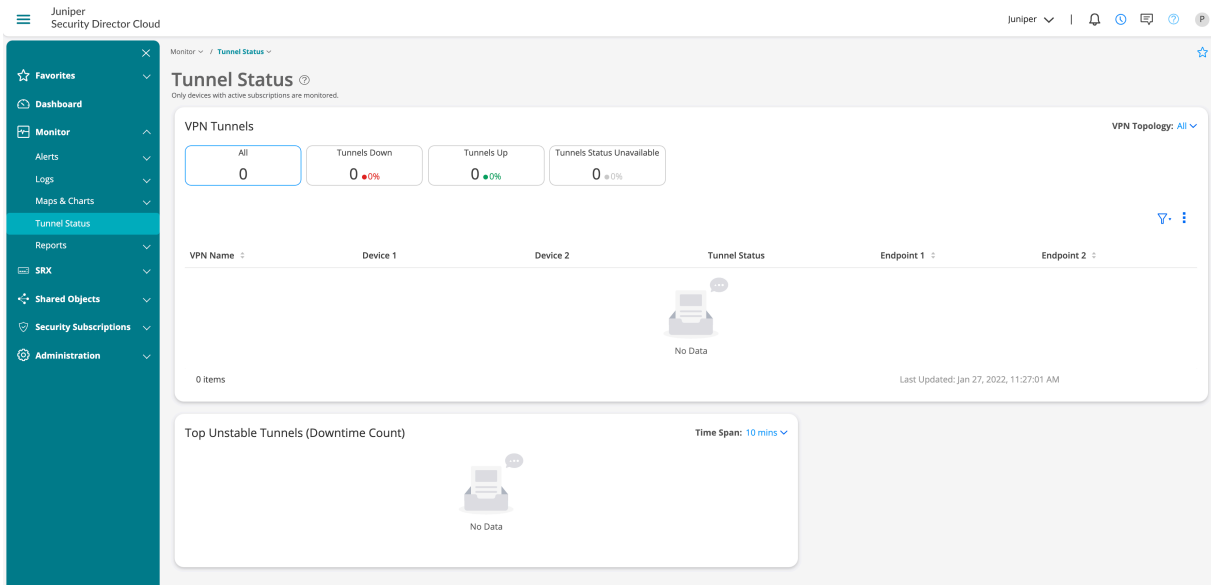
Juniper Security Director Cloud displays the status of IPsec VPN tunnels in a dashboard and tabular format. The number of tunnels for each VPN depends on the type of VPN, such as site-to-site, hub-and-spoke, or remote access VPN. Juniper Security Director Cloud supports a route-based tunnel mode. You can view the tunnel status of IPsec VPNs configured on devices that are managed by Juniper Security Director Cloud. The tunnel status micro-service runs at specified intervals and updates the status of the IPsec VPN tunnels as up or down every 10 minutes.

[Figure 5 on page 101](#) shows the VPN Tunnels dashboard for the VPNs, the VPN tunnels, and the VPN tunnel downtime count.

The VPN Tunnels dashboard contains widgets that display the total number of IPsec VPN tunnels, the number of VPN tunnels that are up, the number of tunnels that are down, and the number of tunnels whose status is unavailable. You can click the widgets to filter the VPN list and display all the tunnels, only tunnels that are up, or only tunnels that are down. You can also filter the VPN list based on the VPN topology—site-to-site and hub-and-spoke. You can also use the filter to specify custom search parameters and display the VPN list based on the VPN name and endpoints connected with the VPN tunnels.

The Top Unstable Tunnels dashboard displays the top five unstable VPN tunnels that were down for a specific period along with the downtime count. You can select a time span from 10 minutes to 30 days. The list of tunnels varies depending on the selected time span. Based on the selected duration, a time range and graph are displayed with the tunnel status data.

Figure 5: Tunnel Status Page



About the Tunnel Status Page

IN THIS SECTION

- [Tasks You Can Perform | 101](#)
- [Field Descriptions | 102](#)

To access this page, select **Monitor > Tunnel Status > Device Tunnel Status**.

Use the Tunnel Status page to view the total number of monitored IPsec VPNs, VPN tunnels, their status as either up or down, and the tunnel downtime count.

Tasks You Can Perform

You can perform the following tasks from this page:

- View the current VPN tunnel details in the VPN Tunnels dashboard.
- Use the advanced filter to display the VPN list filtered by the VPN name or endpoints. See "[Use the Advanced Filter to Monitor Specific Tunnels](#)" on page 102 .

- View the tunnel downtime count ranging from 10 minutes to 30 days in the Top Unstable Tunnels dashboard.

Field Descriptions

Table 33 on page 102 provides guidelines on using the fields on the IPsec VPN Monitoring page.

Table 33: Fields on the Tunnel Status Page

Fields	Description
VPN Name	Specifies the name of the IPsec VPN. Click the name to navigate to the Tunnel Status page.
Device 1	Specifies the IPv4 address of the source device.
Device 2	Specifies the IPv4 address of the destination device.
Tunnel Status	Specifies the status of the tunnel: Tunnels Up, Tunnels Down, or Tunnels Status Unavailable. If the tunnel is down, also displays the reason for the failure.
End Point 1	Specifies the name of endpoint 1.
End Point 2	Specifies the name of endpoint 2.

Use the Advanced Filter to Monitor Specific Tunnels

You can use the advanced filter to filter the list of VPNs that the Tunnel Status page displays based on the VPN name and endpoints.

1. Select **Monitor > Tunnel Status > Device Tunnel Status**.
2. Click the filter icon, then **Add filter**.
The Add Criteria page opens.
3. Complete the configuration of the license according to the guidelines provided

Table 34: Fields on the Add Criteria Page

Field	Description
Field	Decide whether to filter the VPN tunnel list based on VPN name or endpoints, then select one of the following options: <ul style="list-style-type: none"> • VPN Name • Endpoint 1 • Endpoint 2
Condition	Select the condition of the search parameter. You can choose for the query to match the field value or enter a value to search for results containing the value.
Value	Enter the VPN or endpoint name as the search parameter value.

4. Click **Add**.

About the Site Tunnel Status Page

IN THIS SECTION

- [Tasks You Can Perform | 104](#)
- [Field Descriptions | 104](#)

To access this page, select **Monitor > Tunnel Status > Site Tunnel Status**.

Use the Site Tunnel Status page to view the status of the configured tunnels between sites and service locations.

Tasks You Can Perform

You can perform the following tasks from this page:

- View the current tunnel status of the sites. See [Table 35 on page 104](#) .
- Use the advanced filter to display the site list filtered by the site name, service locations, tunnel type, or endpoints. See [Table 36 on page 105](#) .

Field Descriptions

[Table 35 on page 104](#) provides guidelines on using the fields on the Site Tunnel Status Monitoring page.

Table 35: Fields on the Site Tunnel Status Page

Fields	Description
Sites	Name of the site.
Service Locations	Name of the service location of the site.
Tunnel Status	The current status of the tunnel: Tunnels Up, Tunnels Down, or Tunnels Unmonitored.
Tunnel Type	Type of the tunnel: GRE or IPsec
Endpoint 1	Name of endpoint 1.
Endpoint 2	Name of endpoint 2.

You can use the advanced filter to filter tunnel status based on the site, service location, tunnel type, endpoint 1, or endpoint 2. Click the filter icon to add the criteria.

[Table 36 on page 105](#) provides the guidelines on using the fields on the Add Criteria page.

Table 36: Fields on the Add Criteria Page

Field	Description
Field	<p>Filter the site tunnel list based on one of the following options:</p> <ul style="list-style-type: none">• Sites• Service Locations• Tunnel Type• Endpoint 1• Endpoint 2
Condition	Select the condition of the search parameter.
Value	Enter the name of a site, service location, tunnel type, endpoint 1, or endpoint 2 as the search parameter value.

Service Locations

IN THIS CHAPTER

- [About the Service Locations Monitor Page | 106](#)

About the Service Locations Monitor Page

IN THIS SECTION

- [Map View | 106](#)
- [Grid View | 107](#)

To access this page, select **Monitor > Service Locations**.

Use the Service Locations page to view the status of each service location, the number of provisioned users per location, the outbound data transfer per service location, and the available storage.

You can view your data using the Map View or Grid View. By default, the data set is displayed in the Map view for the specified time span. In the Time Span field, you can specify the time range to view the service location's data. Hover over the Time Span field to select the time range.

Map View

Click **Map View** to view all the service locations pinned in a map. You can hover over each pin to view critical information of that particular service location such as:

- Current status of the service location
- Region
- Location

- Number of users
- Bandwidth used by the users

Grid View

Click **Grid View** to obtain comprehensive details about service locations in a tabular format.

[Table 37 on page 107](#) provides guidelines on using the fields on the Grid View.

Table 37: Widgets on the Grid View

Field	Description
Service Location Name	The name of the service location.
Status	The current status of the service location.
Users	The number of active users in the service location
Bandwidth	The total bandwidth used by all the active users.

Advanced Threat Prevention

IN THIS CHAPTER

- [Hosts Overview | 108](#)
- [Host Details | 111](#)
- [Threat Sources Overview | 113](#)
- [Threat Source Details | 115](#)
- [HTTP File Download Overview | 118](#)
- [HTTP File Download Details | 120](#)
- [Signature Details | 124](#)
- [Manual Scanning Overview | 125](#)
- [SMB File Download Overview | 126](#)
- [SMB File Download Details | 128](#)
- [Email Attachments Scanning Overview | 132](#)
- [Email Attachments Scanning Details | 134](#)
- [DNS DGA Detection Overview | 136](#)
- [DNS Tunnel Detection Overview | 137](#)
- [DNS DGA and Tunneling Detection Details | 139](#)
- [Encrypted Traffic Insights Overview | 143](#)
- [Encrypted Traffic Insights Details | 145](#)
- [SMTP Quarantine Overview | 149](#)
- [IMAP Block Overview | 150](#)
- [Telemetry Overview | 152](#)

Hosts Overview

Access this page from the **Monitor > ATP > Hosts** menu.

The hosts page lists compromised hosts and their associated threat levels. From here, you can monitor and mitigate malware detections on a per host basis.

Compromised hosts are systems for which there is a high degree of confidence that attackers have gained unauthorized access. When a host is compromised, the attacker can do several things, such as:

- Send junk or spam e-mail to attack other systems or distribute illegal software.
- Collect personal information, such as passwords and account numbers.

Compromised hosts are listed as security threat intelligence data feeds (also called information sources.) The data feed lists the IP address of the host along with a threat level; for example, 10.130.132.133 and threat level. 5. Once threats are identified, you can create threat prevention policies to take enforcement actions on the inbound and outbound traffic on these infected hosts. See "[Global Configuration for Infected Hosts](#)" on page 969 for more information.

For the Hosts listed on this page, you can perform the following actions on one or multiple hosts at once:

Table 38: Operations for Multiple Infected Hosts

Action	Definition
Export Data	Click the Export button to download compromised host data to a CSV file. You are prompted to narrow the data download to a selected time-frame.
Set Policy Override	Select the check box beside one or multiple hosts and choose one of the following options: <ul style="list-style-type: none"> • Never include host(s) in infected hosts feed • Always include host(s) in infected hosts feed • Use configured policy (not included in infected hosts feed)
Set Investigation Status	Select the check box beside one or multiple hosts and choose one of the following options: In progress, Resolved - false positive, Resolved - fixed, and Resolved - ignored.

NOTE: When you select a **Policy Override** option for hosts, other dependent status fields, such as Infected Host Feed, will also change accordingly. In some cases, you may have to refresh the page to see the updated information.

The following information is available in the Host table.

Table 39: Compromised Host Information

Field	Description
Host Identifier	<p>The Juniper ATP Cloud-assigned name for the host. This name is created by Juniper ATP Cloud using known host information such as IP address, MAC address, user name, and host name. The assigned name will be in the following format: username@server. If the username is not known and MAC address or IP address are used, the name may appear as any of the following formats:</p> <p>user01@2001:db8:cc:dd:ee:ff, user02@10.1.1.1 or 10.1.1.1</p> <p>NOTE: You can edit this name. If you edit the Juniper ATP Cloud-assigned name, Juniper ATP Cloud will recognize the new name and not override it.</p>
Host IP	The IP address of the compromised host.
Threat Level	<p>A number between 0 and 10 indicating the severity of the detected threat, with 10 being the highest.</p> <p>NOTE: Click the three vertical dots at the top of the column to filter the information on the page by threat level.</p>
Infected Host Feed	<p>Displays the current host feed settings:</p> <ul style="list-style-type: none"> • Included: This is the default policy. The host is included in the infected host feed if its threat level meets the set infected host threshold. • Excluded: The host is allowlisted and will be excluded from the infected host feed even if its threat level meets the threshold. • Excluded Manually: The host is allowlisted manually and will be excluded from the infected host feed even if its threat level meets the threshold. <p>Example: If you do not enable Add to Infected Hosts setting while creating a new adaptive threat profiling feed, the feed information will not be sent to the infected host feed.</p> <ul style="list-style-type: none"> • Included Manually: The host is blocklisted and will be included in infected host feed even if its threat level does not meet the threshold.

Table 39: Compromised Host Information (*Continued*)

Field	Description
First Host Activity	Displays the date and time of the first activity of the threat.
Last Host Activity	Displays the date and time of the most recent activity of the threat.
C&C Hits	<p>The number of times a command and control (C&C) server communication threat with this host was detected.</p> <p>NOTE: Click the three vertical dots at the top of the column to filter the information on the page by C&C hits.</p>
Malware	<p>The number of times malware was downloaded by this host.</p> <p>NOTE: Click the three vertical dots at the top of the column to filter the information on the page by malware detections.</p>
Policy	<p>Displays the current policy settings.</p> <ul style="list-style-type: none"> • Use configured policy • Always include host in the Infected Hosts feed • Never include host in the Infected Hosts feed
State of Investigation	Displays either Open, In progress, Resolved-False positive, Resolved-Fixed, Resolved-Ignored
Source	Displays the source of the threat. For example, API, Detection, Adaptive threat profiling feed, and so on.

Host Details

Access this page by clicking the Host Identifier from the **Monitor > ATP > Hosts** page. Double click on the host to view summary details and malicious files that have been downloaded.

Use the host details page to view in-depth information about current threats to a specific host by time frame.

For C&C threat sources, you can change the host identifier, the investigation status, and the blocked status of the host

The information provided on the host details page is as follows:

Table 40: Threat Level Recommendations

Threat Level	Definition
0	Clean; no action is required.
1-3	Low threat level. Recommendation: Disable this host.
4-6	Medium threat level. Recommendation: Disable this host.
7-10	High threat level. Host has been automatically blocked.

- **Host Identifier**—Displays the Juniper ATP Cloud-assigned name of the host. You can edit this name by entering a new name in this field and clicking **Save**. To return to the default assigned name, click **Reset**.
- **Host IP Address**—Displays the IP address of the selected host.
- **MAC Address**—This information is only available when Juniper ATP Cloud is used with Policy Enforcer.
- **Host Status**—Displays the current threat level of the host and recommended actions.
- **Investigation Status**—The following states of investigation are available: Open, In progress, Resolved - false positive, Resolved - fixed, and Resolved - ignored.
- **Policy override for this host**—The following options are available: Use configured policy (not included in infected hosts feed), Always include host in infected hosts feed, Never include host in infected hosts feed.

NOTE: The blocked status changes in relation to the investigation state. For example, when a host changes from an open status (Open or In Progress) to one of the resolved statuses, the blocked status is changed to allowed and the threat level is brought down to 0. Also, when

the investigation status is changed to resolved, an event is added to the log at the bottom of the page.

- **Host threat level graph**—This is a color-coded graphical representation of threats to this host displayed by time frame. You can change the time frame, and you can slide the graph backward or forward to zoom in or out on certain times. When you zoom in, you can view individual days within a month.
- **Expand timeframe to separate events**—Use this check box to stretch a period of time and see the events spread out individually.
- **Past threats**—The date and status of past threats to this host are listed here. The time frame set previously also applies to this list. The description for each event provides details about the threat and the action taken at the time.

Threat Sources Overview

Access this page from the **Monitor > ATP > Threat Sources** menu.

The Threat Sources page lists information of servers that have attempted to contact and compromise hosts on your network. A threat source is a centralized computer that issues commands to botnets (compromised networks of computers) and receives reports back from them.

Benefits

- Using C&C feeds adds another layer of protection to your network, preventing the creation of botnets from within your network. Botnets gather sensitive information, such as account numbers or credit card information, and participate in distributed denial-of-service (DDoS) attacks.
- Using C&C feeds also prevents botnets from communicating with hosts within your network to gather information or launch an attack.

You can allowlist threat sources from the details page. See "[Threat Source Details](#)" on page 115 .

NOTE:

- At this time, C&C URL feeds are not supported with SSL forward proxy.

The following information is available on this page.

Table 41: Threat Source Data Fields

Field	Definition
External Server	The IP address or host name of the suspected threat source.
Blocked Via	Displays the custom feed name.
Highest Threat Level	The threat level of the threat source as determined by an analysis of actions and behaviors.
Count	The number of times hosts on the network have attempted to contact the threat server.
Country	The country where the threat source is located.
Last Seen	The date and time of the most recent threat source hit.
Protocol	The protocol of the threat source.
Action	The action taken on the communication (permitted, sinkhole, or blocked).
Category	Displays the DNS feed category. The available options are custom, global, and whitelist.
DNS Record Type	Displays the query type of the DNS request. The supported DNS query types are A, AAAA, MX, CNAME, SRV, SRV NoErr, TXT, ANY, and so on.
Report False Positive	Displays the status of report false positives.

RELATED DOCUMENTATION

| [Threat Source Details](#) | 115

Threat Source Details

Access this page by clicking on an **External Server** link from the **Threat Sources** page.

Use Threat Source Details page to view analysis information and a threat summary for the threat source. The following information is displayed for each threat source.

- Threat Summary (Location, Category, Host Name, and Time Seen)
- Total Hits
- Protocols and Ports (TCP and UDP)

For threat sources of type C&C, you can add the threat source to the allowlist or report it as a false positive to Juniper Networks from the Threat Source Details page.

For threat source of type DNS , you can only report the threat source as false positive to Juniper Networks.

Table 42: Options on the Threat Source Details Page (Upper Right Side of Page)

Button/Link	Purpose
Select Option > Add to Whitelist	<p>Choose this option to add the threat source to the allowlist.</p> <p>WARNING: Adding a threat source to the allowlist automatically triggers a remediation process to update any affected hosts (in that realm) that have contacted the newly allowlisted threat source.</p> <p>All C&C events related to this allowlisted server will be removed from the affected hosts' events, and a host threat level recalculation will occur.</p> <p>If the host score changes during this recalculation, a new host event appears describing why it was rescored. (For example, "Host threat level updated after threat source 1.2.3.4 was cleared.") Additionally, the threat source will no longer appear in the list of threat source because it has been cleared.</p> <p>NOTE: You can also allowlist threat source from the Configuration > Allowlists page. See "Create Allowlists and Blocklists" on page 957 for details.</p>
Select Option > Report as False Positive	<p>Choose this option to launch a new screen which lets you send a report to Juniper Networks, informing Juniper of a false position or a false negative. Juniper will investigate the report; however, this does not change the verdict.</p>

Under Time Range is a graph displaying the frequency of events over time. An event occurs when a host communicates to the threat source IP address (either sending or receiving data). You can filter this

information by clicking on the time-frame links: 1 day, 1 week, 1 month, Custom (select your own time-frame).

Hosts is a list of hosts that have contacted the server. The information provided in this section is as follows:

Table 43: Threat Source Contacted Host Data

Field	Definition
Client Host	The name of the host in contact with the threat source.
Client IP Address	The IP address of the host in contact with the threat source. (Click through to the Host Details page for this host IP.)
Threat Level at Time	The threat level of the threat source as determined by an analysis of actions and behaviors at the time of the event.
Status	The action taken by the device on the communication (whether it was permitted, sinkhole, or blocked).
Protocol	The protocol (TCP or UDP) the threat source used to attempt communication.
Source Port	The port the threat source used to attempt communication.
Device Name	The name of the device in contact with the threat source.
Date/Time Seen	The date and time of the most recent threat source hit.
Username	The name of the host user in contact with the threat source.

Domains is a list of domains that the IP address previously used at the time of suspicious events. If a threat source IP address is seen changing its DNS/domain name to evade detection, a list of the various names used will be listed along with the dates in which they were seen.

Table 44: Threat Source Associated Domains Data

Field	Definition
C & C Host	This is a list of domains to which the destination IP addresses in the threat source events resolved.
Last Seen	The date and time of the most recent threat source server hit.

Signatures are a list of the threat indicators associated with the IP address. A threat source blocked by the Juniper “Global Threat Feed” will show domains and/or signatures. (The “Blocked Via” column, under the threat source listing, shows whether a threat source IP address was found in the Juniper “Global Threat Feed” or in a different configured custom feed.)

Table 45: Threat Source Signature Data

Field	Definition
Name	The name or type of detected malware.
Category	Description of the malware and way in which it may have compromised a resource or resources.
Date	The date the malware was seen.

Certificates is a list of certificates associated with the threat source.

Table 46: Threat Source Certificate Data

Field	Definition
Certificate Hash	Displays the certificate hash of the threat source.
Date/Time Seen	The date and time when the certificate hash file was last updated.

RELATED DOCUMENTATION

[Threat Sources Overview](#) | 113

HTTP File Download Overview

Access the HTTP File Download page from the **Monitor > ATP > File Scanning > HTTP File Downloads** menu.

The following tabs are available:

- **Full File**—Displays a record of all file metadata sent to the cloud for inspection. These are the files that are sent to cloud for inspection but are not blocked based on the signature match detections and policy configurations on Juniper Secure Edge. From the **Full File** tab, click the file hash link to view more information, such as file details, what other malware scanners say about this file, and a complete list of hosts that downloaded this file.
- **Partial File**—Partial file analysis leverages the Positive Hit Advanced Strike Engine (PHASE) to recognize signatures and determines if there is a potential malware to be blocked before the entire file is downloaded. The **Partial File** tab displays a record for all malware hit events for all blocked signature match detections. From the **Partial File** tab, click the file signature to view more information, such as file details, host that downloaded the file, and so on.

Benefits of viewing HTTP File Downloads

- Allows you to view a compiled list of suspicious downloaded files all in one place, including the signature, threat level, URL, and malware type.
- Allows you to filter the list of downloaded files by individual categories.

Export Data—Click the Export button to download file scanning data to a CSV file. You are prompted to narrow the data download to a selected timeframe.

The following information is available on this page.

Table 47: HTTP Scanning Data Fields

Field	Definition	Applicable To
File Hash	A unique identifier located at the beginning of a file that provides information on the contents of the file. The file hash can also contain information that ensures the original data stored in the file remains intact and has not been modified.	Full File

Table 47: HTTP Scanning Data Fields *(Continued)*

Field	Definition	Applicable To
Phase Sig ID	A unique identifier for each signature that is generated by Juniper ATP Cloud.	Partial File
Threat Level	The threat score. NOTE: Click the three vertical dots at the top of the column to filter the information on the page by threat level.	Full File Partial File
Filename	The name of the file, including the extension. NOTE: Enter text in the space at the top of the column to filter the data.	Full File Partial File
Last Submitted	The time and date of the most recent scan of this file.	Full File Partial File
URL	The URL from which the file originated. NOTE: Enter text in the space at the top of the column to filter the data.	Full File Partial File
Malware Name	The name of file and the type of threat if the verdict is positive for malware. Examples: Trojan, Application, Adware. If the file is not malware, the verdict is "clean." NOTE: Enter text in the space at the top of the column to filter the data.	Full File Partial File
Category	The type of file. Examples: PDF, executable, document. NOTE: Enter text in the space at the top of the column to filter the data.	Full File Partial File

HTTP File Download Details

IN THIS SECTION

- [File Summary | 122](#)
- [Behavior Analysis | 123](#)
- [HTTP Downloads | 123](#)
- [Sample STIX Report | 124](#)

To access this page, navigate to **Monitor > ATP > File Scanning > HTTP File Downloads**. Click on the **File Hash** link in the **Full File** tab to go to the File Download Details page.

Use this page to view analysis information and malware behavior summaries for the downloaded file. This page is divided into several sections:

Table 48: Links on the HTTP File Download Details Page

Button/Link	Purpose
Report False Positive	Click this button to launch a new screen which lets you send a report to Juniper Networks, informing Juniper of a false position or a false negative. Juniper will investigate the report; however, this does not change the verdict. If you want to make a correction (mark system as clean) you must do it manually.

Table 48: Links on the HTTP File Download Details Page (*Continued*)

Button/Link	Purpose
Download STIX Report	<p>When there is a STIX report available, a download link appears on this page. Click the link to view gathered, open-source threat information, such as blocklisted files, addresses and URLs.</p> <p>STIX (Structured Threat Information eXpression) is a language used for reporting and sharing threat information using TAXII (Trusted Automated eXchange of Indicator Information). TAXII is the protocol for communication over HTTPS of threat information between parties.</p> <p>STIX and TAXII are an open community-driven effort of specifications that assist with the automated exchange of threat information. This allows threat information to be represented in a standardized format for sharing and consuming. Juniper ATP Cloud uses this information as well as other sources. This occurs automatically. There is no administrator configuration required for STIX.</p> <p>STIX reports will vary. View a sample report at the bottom of this page.</p> <p>NOTE: Juniper ATP Cloud can also share threat intelligence. You can control what threat information is shared from the Threat Sharing page. See "Configure Threat Intelligence Sharing" on page 973 .</p>
Download Zipped Files	<p>(When available) Click this link to download the quarantined malware for analysis. The link allows you to download a password-protected zipped file containing the malware. The password for the zip file is the SHA256 hash of the malware exe file (64 characters long, alpha numeric string) shown in the General tab for the file in question.</p>
Download PDF Report	<p>Click this link to download a detailed report on the file in question. The report includes file threat level, protocol seen, file category and size, client IP address and username, and much more information, if available. This data is provided in a formatted PDF with a TOC.</p>

The top of the page provides a quick view of the following information (scroll to the right in the UI to see more boxes):

- **Threat Level**—This is the threat level assigned (0-10), This box also provides the file name, and threat category.
- **Top Indicators**—In this box, you will find the malware name, the signature it matches, antivirus state, and the IP address/URL from which the file originated.

- **Prevalence**—This box provides information on how often this malware has been seen, how many individual hosts on the network downloaded the file, and the protocol used.

File Summary

Table 49: General Summary Fields

Field	Definition
Threat Level	This is the assigned threat level 0-10. 10 is the most malicious.
Global Prevalence	How often this file has been seen across different customers.
Last Scanned	The time and date of the last scan to detect the suspicious file.
File Name	The name of the suspicious file. Examples: unzipper-setup.exe, 20160223158005.exe,, wordmui.msi.
Category	The type of file. Examples: PDF, executable, document.
Size	The size of the downloaded file.
Platform	The target operating system of the file. Example. Win32
Malware Name	If possible, Juniper ATP Cloud determines the name of the malware.
Type	If possible, Juniper ATP Cloud determines the type of threat. Example: Trojan, Application, Adware.
Strain	If possible, Juniper ATP Cloud determines the strain of malware detected. Example: Outbrowse.1198, Visicom.E, Flystudio.
sha256 and md5	One way to determine whether a file is malware is to calculate a checksum for the file and then query to see if the file has previously been identified as malware.

Behavior Analysis

Juniper ATP Cloud provides network behavioral analysis and machine learning to determine if an SSL/TLS connection is benign or malicious.

Behavior analysis tab displays the signature information in a radar chart with malware categories or behaviors on each axis. This data helps us better identify the category of a malware and map that category to a severity.

The malware priority is classified into low, medium, and high.

Table 50: Behavior Analysis Fields

Behavior Category	Sample Behavior Definition
Targeting	Checks volume information.
Fine-grained Behavior	Contains code to communicate with device drivers. Contains code to delete services. Memory allocated in system DLL range.
Obfuscation	Utilizes known code obfuscation techniques.
Evasion	Contains code to detect VMs. Contains large amount of unused code (likely obfuscated code). Contains code to determine API calls at runtime.
Persistence	Modifies registry keys to run application during startup.
Networking	Memory or binary contains internet addresses.

HTTP Downloads

This section displays the list of hosts that have downloaded the suspicious file. Click the **IP address** to be taken to the Host Details page for this host. Click the **Device Serial number** to be taken to the Devices page. From there you can view device versions and version numbers for the Juniper ATP Cloud

configuration, including profile, allowlist, and blacklist versions. You can also view the malware detection connection type for the device: telemetry, submission, or C&C event.

In the Network Activity section, you can view information in the following tabs:

- **Contacted Domains**—If available, lists any domains that were contacted while executing the file in the Juniper ATP Cloud sandbox.
- **Contacted IPs**—If available, lists all IPs that were contacted while executing the file, along with the destination IP's country, ASN, and reputation. The reputation field is based on Juniper IP intelligence data destination.
- **DNS Activity**— This tab lists DNS activity while executing the file, including reverse lookup to find the domain name of externally contacted servers. This tab also provides the known reputation of the destination servers.

Sample STIX Report

Figure 6: Sample STIX Report

```
<?xml version="1.0"?>
- <stix:STIX_Package version="1.2" id="example:Package-afbc14e2-b192-4ea0-848f-0a95aaea6cb3" xmlns:WinProcessObj="http://cybox.mitre.org/objects#WinProcessObject-2"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:WinRegistryKeyObj="http://cybox.mitre.org/objects#WinRegistryKeyObject-2" xmlns:stix="http://stix.mitre.org/stix-1"
  xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1" xmlns:WinThreadObj="http://cybox.mitre.org/objects#WinThreadObject-2" xmlns:example="http://example.com"
  xmlns:stixCommon="http://stix.mitre.org/common-1" xmlns:cybox="http://cybox.mitre.org/cybox-2" xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
  xmlns:ttp="http://stix.mitre.org/ttp-1" xmlns:xlink="http://www.w3.org/1999/xlink" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:FileObj="http://cybox.mitre.org/objects#FileObject-2" xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
  xmlns:ProcessObj="http://cybox.mitre.org/objects#ProcessObject-2" xmlns:indicator="http://stix.mitre.org/Indicator-2" xmlns:ids="http://www.w3.org/2000/09/xmldsig#">
  - <stix:STIX_Header>
    - <stix:Description> IOCs for sample id: a9c097d0f6392897ff87764d43ac9ad4b60078f7062325b7798909e484f3f1af</stix:Description>
  </stix:STIX_Header>
  - <stix:Indicators>
    - <stix:Indicator id="example:indicator-92000f82-82b0-45bf-9ac7-bf4566c1c93d" xsi:type="indicator:IndicatorType" timestamp="2017-10-09T20:31:25.918941+00:00">
      <indicator:Title> File Indicator(s) for sample:a9c097d0f6392897ff87764d43ac9ad4b60078f7062325b7798909e484f3f1af</indicator:Title>
      <indicator:Description> An indicator containing File observable(s) </indicator:Description>
      - <indicator:Observable id="example:Observable-987ee5c7-6c56-414c-a696-f3199d5aa0fb">
        - <cybox:Object id="example:File-4f1c86c5-725b-4d44-b19e-e1787dc05c28">
          - <cybox:Properties xsi:type="FileObj:FileObjectType">
            - <FileObj:Hashes>
              - <cyboxCommon:Hash>
                - <cyboxCommon:Type xsi:type="cyboxVocabs:HashNameVocab-1.0"> MD5 </cyboxCommon:Type>
                - <cyboxCommon:Simple_Hash_Value> b941993d05adf34dc9b7d35fe3f0ae61 </cyboxCommon:Simple_Hash_Value>
              </cyboxCommon:Hash>
              - <cyboxCommon:Hash>
                - <cyboxCommon:Type xsi:type="cyboxVocabs:HashNameVocab-1.0"> SHA1 </cyboxCommon:Type>
                - <cyboxCommon:Simple_Hash_Value> e70f1bb911ee60ef6e7aa2c423eaa5a04d17e709 </cyboxCommon:Simple_Hash_Value>
              </cyboxCommon:Hash>
              - <cyboxCommon:Hash>
                - <cyboxCommon:Type xsi:type="cyboxVocabs:HashNameVocab-1.0"> SHA256 </cyboxCommon:Type>
                - <cyboxCommon:Simple_Hash_Value> a9c097d0f6392897ff87764d43ac9ad4b60078f7062325b7798909e484f3f1af </cyboxCommon:Simple_Hash_Value>
              </cyboxCommon:Hash>
              - <cyboxCommon:Hash>
                - <cyboxCommon:Type xsi:type="cyboxVocabs:HashNameVocab-1.0"> SHA512 </cyboxCommon:Type>
                - <cyboxCommon:Simple_Hash_Value> 1afc3d6e068c8e3bb617726a0ecdec428da99c874ef2f1c98538651b6d537bf5e8d00a0e2c49b2d20740146c9ef5f77
              </cyboxCommon:Hash>
            </FileObj:Hashes>
          </cybox:Properties>
        </cybox:Object>
      </indicator:Observable>
    </stix:Indicator>
  </stix:Indicators>
</stix:Package>
```

Signature Details

To access the malware signature details page, go to.

- **Monitor>ATP>File Scanning>HTTP File Download**

- **Monitor > ATP > File Scanning > Email Attachments**
- **Monitor > ATP > File Scanning > SMB File Download**

Click **Partial File** tab and **Phase Sig ID** link to go to the Signature Details page.

Use the Signature Details page to view the malware signature details. The malware signatures are provided by Juniper ATP Cloud to the Juniper Secure Edge as well as SRX Series Firewalls. When Juniper Secure Edge detects a malware file, it can block the file immediately based on these malware signatures and the anti-malware profile. The malware signatures are shared with Juniper Secure Edge whenever there is an update in Juniper ATP Cloud. For each malware signature hit, Juniper Secure Edge provides the malware signature hit report to Juniper ATP Cloud.

This page is divided into several sections:

- **Report False Positive**—Click this button to launch a new screen to send a report to Juniper Networks, informing if the report is a false positive or a false negative. Juniper will investigate the report; however, this does not change the verdict. If you want to make a correction (mark system as clean) you must do it manually.
- **Threat Level**—This is the threat level assigned (0-10). This box also provides the signature file name, threat category and the action taken.
- **Prevalence**—Provides information on how often this malware has been seen, how many individual hosts on the network downloaded the file, and the protocol used.
- **Downloads**—List of hosts that have downloaded the suspicious file. You can view the IP address of the host. You can also view the client IP address, file name of the signature, date/time when the signature was submitted, device serial number, URL, destination IP address and username of the host.

Manual Scanning Overview

Access this page from the **Monitor > ATP > File Scanning > Manual Uploads** menu.

If you suspect a file is suspicious, you can manually upload it to the cloud for scanning and evaluation. Click the **Upload** button to browse to the file you want to upload. The file can be up to 32 MB.

Benefits of Manually Scanning Files

- Allows you to investigate files that were not filtered by existing blocklists.
- Provides all file analysis data that accompanies known suspicious files, such as behavior analysis and network activity.

There is a limit to the number of files administrators can upload for manual scanning. File uploads are limited by realm (across all users in a realm) in a 24-hour period.

Table 51: File Scanning Data Fields

Field	Definition
File Signature	A unique identifier located at the beginning of a file that provides information on the contents of the file. The file signature can also contain information that ensures the original data stored in the file remains intact and has not been modified.
Threat Level	The threat score.
Filename	The name of the file, including the extension.
Last Submitted	The time and date of the most recent scan of this file.
URL	The URL from which the file originated.
Verdict	The name of file and the type of threat if the verdict is positive for malware. Examples: Trojan, Application, Adware. If the file is not malware, the verdict is "clean."
Category	The type of file. Examples: PDF, executable, document.

SMB File Download Overview

Access the SMB File Download page from the **Monitor > ATP > File Scanning > SMB File Downloads** menu.

The Server Message Block (SMB) protocol enables applications or users to access files and other resources on a remote server.

NOTE: SMB protocol is supported only for Security Director Cloud use cases.

The following tabs are available:

- **Full File**—Displays a record of all file metadata sent to the cloud for inspection. These are the files that are sent to cloud for inspection but are not blocked based on the signature match detections and policy configurations on Juniper Secure Edge. From the **Full File** tab, click the file hash link to view more information, such as file details, what other malware scanners say about this file, and a complete list of hosts that downloaded this file.
- **Partial File**—Partial file analysis leverages the Positive Hit Advanced Strike Engine (PHASE) to recognize signatures and determines if there is a potential malware to be blocked before the entire file is downloaded. The **Partial File** tab displays a record for all malware hit event for all blocked signature match detections. From the **Partial File** tab, click the file signature to view more information, such as file details, host that downloaded the file, and so on.

Benefits of viewing SMB File Downloads

- Allows you to view a compiled list of suspicious downloaded files all in one place, including the signature, threat level, URL, and malware type.
- Allows you to filter the list of downloaded files by individual categories.

Export Data—Click the Export button to download file scanning data to a CSV file. You are prompted to narrow the data download to a selected time-frame.

The following information is available on this page.

Table 52: SMB Scanning Data Fields

Field	Definition	Applicable To
File Hash	A unique identifier located at the beginning of a file that provides information on the contents of the file. The file hash can also contain information that ensures the original data stored in the file remains intact and has not been modified. NOTE: Enter text in the space at the top of the column to filter the data.	Full File
Phase Sig ID	A unique identifier for each signature that is generated by Juniper ATP Cloud.	Partial File
Threat Level	The threat score. NOTE: Click the three vertical dots at the top of the column to filter the information on the page by threat level.	Full File Partial File

Table 52: SMB Scanning Data Fields *(Continued)*

Field	Definition	Applicable To
Filename	The name of the file, including the extension.	Full File
	NOTE: Enter text in the space at the top of the column to filter the data.	Partial File
Last Submitted	The time and date of the most recent scan of this file.	Full File
		Partial File
URL	The URL from which the file originated.	Full File
	NOTE: Enter text in the space at the top of the column to filter the data.	Partial File
Malware	The name of file and the type of threat if the verdict is positive for malware. Examples: Trojan, Application, Adware. If the file is not malware, the verdict is "clean."	Full File
	NOTE: Enter text in the space at the top of the column to filter the data.	Partial File
Category	The type of file. Examples: PDF, executable, document.	Full File
	NOTE: Enter text in the space at the top of the column to filter the data.	Partial File

RELATED DOCUMENTATION

[SMB File Download Details](#) | 128

SMB File Download Details

IN THIS SECTION

- [File Summary](#) | 130
- [SMB Downloads](#) | 131

To access this page, navigate to **Monitor > ATP > File Scanning > SMB File Download**. Click on the **File Hash** link in **Full File** tab to go to the SMB File Download Details page.

NOTE: SMB protocol is supported only for Security Director Cloud use cases.

Use this page to view analysis information and malware behavior summaries for the downloaded file. This page is divided into several sections:

Table 53: Links on the SMB File Download Details Page

Button/Link	Purpose
Report False Positive	Click this button to launch a new screen which lets you send a report to Juniper Networks, informing Juniper of a false position or a false negative. Juniper will investigate the report; however, this does not change the verdict.
Download STIX Report	<p>When there is a STIX report available, a download link appears on this page. Click the link to view gathered, open-source threat information, such as blocklisted files, addresses and URLs.</p> <p>STIX (Structured Threat Information eXpression) is a language used for reporting and sharing threat information using TAXII (Trusted Automated eXchange of Indicator Information). TAXII is the protocol for communication over HTTPS of threat information between parties.</p> <p>STIX and TAXII are an open community-driven effort of specifications that assist with the automated exchange of threat information. This allows threat information to be represented in a standardized format for sharing and consuming. Juniper ATP Cloud uses this information as well as other sources. This occurs automatically. There is no administrator configuration required for STIX.</p> <p>STIX reports will vary. View a sample report at the bottom of this page.</p> <p>NOTE: Juniper ATP Cloud can also share threat intelligence. You can control what threat information is shared from the Threat Sharing page. See "Configure Threat Intelligence Sharing" on page 973.</p>

Table 53: Links on the SMB File Download Details Page (Continued)

Button/Link	Purpose
Download Zipped File	(When available) Click this link to download the quarantined malware for analysis. The link allows you to download a password-protected zipped file containing the malware. The password for the zip file is the SHA256 hash of the malware exe file (64 characters long, alpha numeric string) shown in the General tab for the file in question.
Download PDF Report	Click this link to download a detailed report on the file in question. The report includes file threat level, protocol seen, file category and size, client IP address and username, and much more information, if available. This data is provided in a formatted PDF with a TOC.

The top of the page provides a quick view of the following information (scroll to the right in the UI to see more boxes):

- **Threat Level**—This is the threat level assigned (0-10), This box also provides the file name and threat category.
- **Top Indicators**—In this box, you will find the signature match for the file name, and the antivirus details.
- **Prevalence**—This box provides information on how often this malware has been seen, how many individual hosts on the network downloaded the file, and the protocol used.

File Summary

Table 54: General Summary Fields

Field	Definition
General	
Threat Level	This is the assigned threat level 0-10. 10 is the most malicious.
Global Prevalence	How often this file has been seen across different customers.
Last Scanned	The time and date of the last scan to detect the suspicious file.

Table 54: General Summary Fields (Continued)

Field	Definition
File Information	
File Name	The name of the suspicious file. Examples: unzipper-setup.exe, 20160223158005.exe,, wordmui.msi.
Category	The type of file. Examples: PDF, executable, document.
Size	The size of the downloaded file.
Platform	The target operating system of the file. Example. Win32
Malware Name	If possible, Juniper ATP Cloud determines the name of the malware.
Type	If possible, Juniper ATP Cloud determines the type of threat. Example: Trojan, Application, Adware.
Strain	If possible, Juniper ATP Cloud determines the strain of malware detected. Example: Outbrowse.1198, Visicom.E, Flystudio.
Other Details	
sha256 and md5	One way to determine whether a file is malware is to calculate a checksum for the file and then query to see if the file has previously been identified as malware.

SMB Downloads

This is a list of hosts that have downloaded the suspicious file. Click the **Host Identifier** link to be taken to the Host Details page for this host.

RELATED DOCUMENTATION

| [SMB File Download Overview](#) | 126

Email Attachments Scanning Overview

Access the Email Attachments page from the **Monitor > ATP > File Scanning > Email Attachments** menu.

The following tabs are available:

- **Full File**—Displays a record of all file metadata sent to the cloud for inspection. These are the files that are sent to cloud for inspection but are not blocked based on the signature match detections and policy configurations on Juniper Secure Edge. From the **Full File** tab, click the file hash link to view more information, such as file details, what other malware scanners say about this file, and a complete list of hosts that downloaded this file.
- **Partial File**—Partial file analysis leverages the Positive Hit Advanced Strike Engine (PHASE) to recognize signatures and determines if there is a potential malware to be blocked before the entire file is downloaded. The **Partial File** tab displays a record for all malware hit event for all blocked signature match detections. From the **Partial File** tab, click the file signature to view more information, such as file details, host that downloaded the file, and so on.

Benefits of Viewing Scanned Email Attachments

- Allows you to view a compiled list of suspicious email attachments all in one place, including the file hash, threat level, file name, and malware type.
- Allows you to filter the list of email attachments by individual categories.

Export Data—Click the Export button to download file scanning data to a CSV file. You are prompted to narrow the data download to a selected time-frame.

The following information is available on this page.

Table 55: Email Attachments Scanning Data Fields

Field	Definition	Applicable To
File Hash	A unique identifier located at the beginning of a file that provides information on the contents of the file. The file hash can also contain information that ensures the original data stored in the file remains intact and has not been modified.	Full File
Phase Sig ID	A unique identifier for each signature that is generated by Juniper ATP Cloud.	Partial File

Table 55: Email Attachments Scanning Data Fields (Continued)

Field	Definition	Applicable To
Threat Level	The threat score.	Full File Partial File
Date Scanned	The date and time the file was scanned.	Full File Partial File
Filename	The name of the file, including the extension.	Full File Partial File
Recipient	The email address of the intended recipient.	Full File Partial File
Sender	The email address of the sender.	Full File Partial File
Malware Name	The type of malware found.	Full File Partial File
Status	Indicates whether the file was blocked or permitted.	Full File Partial File
Category	The type of file. Examples: PDF, executable, document.	Full File Partial File

Email Attachments Scanning Details

IN THIS SECTION

- [File Summary | 135](#)

To access this page, navigate to **Monitor > ATP > File Scanning > Email Attachments**. Click on the **File Hash** link in **Full File** tab to go to the File Scanning Details page.

Use this page to view analysis information and malware behavior summaries for the downloaded file. This page is divided into several sections:

Report False Positives—Click the **Report False Positive** button to launch a new screen which lets you send a report to Juniper Networks, informing Juniper of a false position or a false negative. Juniper will investigate the report, however, this does not change the verdict. If you want to make a correction (mark system as clean) you must do it manually.

Download STIX Report—

When there is a STIX report available, a download link appears on this page. Click the link to view gathered, open-source threat information, such as blocklisted files, addresses and URLs. STIX (Structured Threat Information eXpression) is a language used for reporting and sharing threat information using TAXII (Trusted Automated eXchange of Indicator Information). TAXII is the protocol for communication over HTTPS of threat information between parties.

STIX and TAXII are an open community-driven effort of specifications that assist with the automated exchange of threat information. This allows threat information to be represented in a standardized format for sharing and consuming. Juniper ATP Cloud uses this information as well as other sources. This occurs automatically. There is no administrator configuration required for STIX.

NOTE: Juniper ATP Cloud can also share threat intelligence. You can control what threat information is shared from the Threat Sharing page. See "[Configure Threat Intelligence Sharing](#)" on page 973 .

Download Zipped Files—(When available) Click this link to download the quarantined malware for analysis. The link allows you to download a password-protected zipped file containing the malware. The password for the zip file is the SHA256 hash of the malware exe file (64 characters long, alpha numeric string) shown in the General tab for the file in question.

The top of the page provides a quick view of the following information (scroll to the right in the UI to see more boxes):

- **Threat Level**—This is the threat level assigned (0-10), This box also provides the threat category and the action taken.
- **Top Indicators**—In this box, you will find the malware name, the signature it matches, and the IP address/URL from which the file originated.
- **Prevalence**—This box provides information on how often this malware has been seen, how many individual hosts on the network downloaded the file, and the protocol used.

File Summary

Table 56: General Summary Fields

Field	Definition
Threat Level	This is the assigned threat level 0-10. 10 is the most malicious.
Action Taken	The action taken based on the threat level and host settings: block or permit.
Global Prevalence	How often this file has been seen across different customers.
Last Scanned	The time and date of the last scan to detect the suspicious file.
File Name	The name of the suspicious file. Examples: unzipper-setup.exe, 20160223158005.exe, wordmui.msi.
Category	The type of file. Examples: PDF, executable, document.
File Size	The size of the downloaded file.
Platform	The target operating system of the file. Example. Win32
Malware Name	If possible, Juniper ATP Cloud determines the name of the malware.

Table 56: General Summary Fields (Continued)

Field	Definition
Type	If possible, Juniper ATP Cloud determines the type of threat. Example: Trojan, Application, Adware.
Strain	If possible, Juniper ATP Cloud determines the strain of malware detected. Example: Outbrowse.1198, Visicom.E, Flystudio.
Other Details	
sha256 and md5	One way to determine whether a file is malware is to calculate a checksum for the file and then query to see if the file has previously been identified as malware.

In the Network Activity section, you can view information in the following tabs:

NOTE: This section will appear blank if there has been no network activity.

- **Contacted Domains**—If available, lists any domains that were contacted while executing the file in the Juniper ATP Cloud sandbox.
- **Contacted IPs**—If available, lists all IPs that were contacted while executing the file, along with the destination IP's country, ASN, and reputation. The reputation field is based on Juniper IP intelligence data destination.
- **DNS Activity**— This tab lists DNS activity while executing the file, including reverse lookup to find the domain name of externally contacted servers. This tab also provides the known reputation of the destination servers.

In the Behavior Details section, you can view the behavior of the file on the system. This includes any processes that were started, files that were dropped, and network activity seen during the execution of the file. Dropped files are any additional files that were downloaded and installed by the original file.

DNS DGA Detection Overview

Domain Name System (DNS) Domain Generation Algorithm (DGA) generates seemingly random domain names that are used as rendezvous points with potential C&C servers. DNS DGA detection uses

machine learning models as well as known pre-computed DGA domain names and provides domain verdicts, which helps in-line blocking and sinkholing of DNS queries on Juniper Secure Edge.

Juniper ATP Cloud provides a machine learning-based DGA detection model. Juniper Secure Edge acts as a collector of security metadata and streams the metadata to Juniper ATP Cloud for DGA analysis. We use both ATP Cloud service and security-metadata-streaming framework to conduct DGA Inspection in the cloud.

DNS DGA detection is available only with a Secure Edge Advanced or higher license.

To view DNS DGA detections, navigate to **Monitor > ATP > DNS**. The DGA detections are displayed as shown in [Figure 7 on page 137](#).

Figure 7: DNS DGA Page

<input type="checkbox"/>	Domain	DNS Record Type	Last Hit Session ID	Last Hit Source IP	Last Hit Destination IP	Total Hits	Verdict	▼ Last Hit Time
<input type="checkbox"/>	www.sina.com	CNAME	13012	12.0.0.1	13.0.0.1	1	Clean	Jun 5, 2021 5:32 AM
<input type="checkbox"/>	juniper1234.net	CNAME	12637	12.0.0.1	13.0.0.1	7	Clean	Jun 5, 2021 5:20 AM
<input type="checkbox"/>	www.yahoo.com	CNAME	12343	12.0.0.1	13.0.0.1	2	Clean	Jun 5, 2021 5:10 AM
<input type="checkbox"/>	alskjfguhiusdfghjsdkfn...	CNAME	4295685486	12.0.0.1	13.0.0.1	1	DGA	May 28, 2021 12:36 AM

RELATED DOCUMENTATION

[security-metadata-streaming](#)

DNS Tunnel Detection Overview

IN THIS SECTION

- [DNS Tunneling Procedure | 138](#)

DNS Tunneling is a cyber-attack method that encodes the data of other programs or protocols in DNS queries and responses. It indicates that DNS traffic is likely to be subverted to transmit data of another protocol or malware beconing.

When a DNS packet is detected as tunneled, Juniper Secure Edge can take permit, deny or sinkhole action.

DNS Tunneling detection is available only with a Secure Edge Advanced or higher license.

Juniper Secure Edge exports the tunneling metadata to Juniper ATP Cloud. To view the DNS tunneling detections, navigate to **Monitor > ATP > DNS**. Click on the **Tunnel** tab to view the DNS tunnel detections as shown in [Figure 8 on page 138](#) . You can click on a domain name to view more details of the hosts that have contacted the domain.

Figure 8: DNS Tunnel Page

Domain	DNS Record Type	Last Hit Session ...	Tunnel Data	Last Hit Source IP	Last Hit Destina...	Total Hits	Last Hit Time
d0040383150000...	—	1154835	d0040383150000...	13.0.0.1	13.0.0.254	1	Apr 13, 2021 12:1...
6a9b0394340000...	SRV	441	6a9b0394340000...	50.0.0.2	60.0.0.2	1	Mar 11, 2021 4:41...
8412035c650000...	SRV	415	8412035c650000...	50.0.0.2	60.0.0.2	1	Mar 11, 2021 4:31...
77c0035a7f00000...	SRV	408	77c0035a7f00000...	50.0.0.2	60.0.0.2	1	Mar 11, 2021 4:30...

DNS Tunneling Procedure

Here is how DNS tunneling works:

1. A cyber attacker registers a malicious domain, for example, “badsite.com”.
2. The domain’s name server points to the attacker’s server, where DNS Tunneling malware program is running.
3. DNS Tunnel client program running on the infected host generates DNS requests to the malicious domain.

4. DNS resolver routes the query to the attacker's command-and-control server.
5. Connection is established between victim and attacker through DNS resolver.
6. This tunnel can be used to exfiltrate data or for other malicious purposes.

DNS DGA and Tunneling Detection Details

IN THIS SECTION

- [DGA | 139](#)
- [Tunnel | 141](#)

To access this page, click **Monitor** > **ATP** > **DNS**.

You can view details about DNS DGA and tunnel detections.

DGA

You can perform the following action in the DGA tab:

- View details about the DGA-based detections. See [Table 57 on page 140](#) .
- View the threat sources if there is a C&C hit for a domain. Click on domain name with DGA verdict to view the threat sources.
- Report false positives. Choose this option to send a report to Juniper Networks, informing a false positive. Juniper will investigate the report; however, this does not change the verdict.
- Export DGA detections as a CSV file to view and analyze the exported DGA detections as needed. You can either export all detections at once or for a specific timespan.
- Select the time span to view the DGA detections for a specific period.

Table 57: Fields on the DGA Tab

Field	Description
Domain	Displays the domain name where DGA hit occurs.
DNS Record Type	<p>Displays the DNS record type.</p> <p>Example: A (Host address), CNAME (Canonical name for an alias), SRV (location of service), and so on.</p> <ul style="list-style-type: none"> • A— DNS record is used to point a domain or subdomain to an IP address. • CNAME—DNS record is used to point a domain or subdomain to another hostname. • SRV—DNS record is used to point a domain or subdomain to a service location.
Last Hit Session ID	Displays the ID of the most recent domain hit.
Last Hit Source IP	Displays the source IP address of the most recent domain hit.
Last Hit Destination IP	Displays the destination IP address of the most recent domain hit.
Total Hits	Displays the total number of hits on the domain.
Verdict	<p>Displays the confirmed DGA verdict provided by ATP Cloud.</p> <ul style="list-style-type: none"> • Clean • DGA
Last Hit Time	Displays the date and time of the most recent domain hit.

Tunnel

Use the Tunnel tab to monitor the DNS tunneling metadata provided by Juniper Secure Edge. [Table 58 on page 141](#) displays the DNS tunneling metadata.

You can perform the following action in the Tunnel tab:

- View details about the DNS tunneling metadata provided by Juniper Secure Edge. [Table 58 on page 141](#) displays the DNS tunneling metadata.
- Export DNS Tunnel detections as a CSV file to view and analyze the exported DNS tunneling detections as needed. You can either export all detections at once or for a specific timespan.
- Select the time span to view the DNS tunneling detections for a specific period.
- View detailed information about a DNS tunnel. Click on a domain name. See [Table 59 on page 142](#)
- Download PCAP from the DNS Tunnel page. Select a client and click **Download PCAP** to download the packet capture details and view more information about the network.

Table 58: Fields on the Tunnel Tab

Field	Description
Domain	Displays the domain name
DNS Record Type	<p>Displays the DNS record type.</p> <p>Example: A (Host address), CNAME (Canonical name for an alias), SRV (location of service), and so on.</p> <ul style="list-style-type: none"> • A— DNS record used to point a domain or subdomain to an IP address. • CNAME—DNS record used to point a domain or subdomain to another hostname. • SRV—DNS record used to point a domain or subdomain to a service location.
Last Hit Session ID	Displays the session ID of the most recent domain hit.
Tunnel Data	Displays the tunnel information shared by Juniper Secure Edge.

Table 58: Fields on the Tunnel Tab (Continued)

Field	Description
Last Hit Source IP	Displays the source IP address of the most recent domain hit.
Last Hit Destination IP	Displays the destination IP address of the most recent domain hit.
Total Hits	Displays the total number of sessions that were hit.
Last Hit Time	Displays the date and time of the most recent domain hit.

Table 59: Fields on the DNS Tunnel page

Field	Description
Client IP Address	Displays the IP address of the host that has contacted the DNS domain.
Device Name	Displays the name of the Juniper Secure Edge device in contact with the DNS domain.
Incoming Bytes	Displays the number of incoming bytes to the DNS tunnel.
Outgoing Bytes	Displays the number of outgoing bytes from the DNS tunnel.
Last Seen	The date and time of the most recent DNS tunnel hit.

Encrypted Traffic Insights Overview

IN THIS SECTION

- [Encrypted Traffic Insights and Detection | 144](#)
- [Workflow | 145](#)

Access this page from the **Monitor > ATP > Encrypted Traffic** menu.

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

Benefits of Encrypted Traffic Insights

- Monitors network traffic for threats without breaking the encryption of the traffic, thereby adhering to data privacy laws.
- Erases the need for additional hardware or network changes to set up and manage the network:
 - Juniper Secure Edge provides the required metadata (such as known malicious certificates and connection details) and connection patterns to ATP Cloud.
 - The ATP Cloud provides behavior analysis and machine learning capabilities.
- Provides greater visibility and policy enforcement over encrypted traffic without requiring resource-intensive SSL decryption:
 - Based on the network behaviors analyzed by ATP Cloud, the network connections are classified as malicious or benign.
- Adds an additional layer of protection beyond traditional information security solutions to help organizations reduce and manage risk.
- Ensures no latency as we do not decrypt the traffic.

[Table 60 on page 144](#) lists the information that is available on the Encrypted Traffic Insights page.

Table 60: Encrypted Traffic Insights

Field	Guideline
External Server IP	The IP address of the external server.
External Server Hostname	The host name of the external server.
Highest Threat Level	The threat level on the external server based on Encrypted Traffic Insights.
Count	The number of times hosts on the network have attempted to contact this server.
Country	The country where the external server is located.
Last Seen	The date and time of the most recent external server hit.
Category	Additional category information known about this server, for example, botnets, malware, etc.

Encrypted Traffic Insights and Detection

Encrypted Traffic Insights combines rapid response and network analysis (both static and dynamic) to detect and remediate malicious activity hidden in encrypted sessions.

A staged approach of Encrypted Traffic Insights for a new TCP session is as follows:

1. **Known Malicious Activity**—Juniper ATP Cloud provides information regarding certificates known to be associated with malware, which Juniper Secure Edge uses to immediately identify malicious traffic.
2. **Unknow Malicious Activity**—Metadata and network connection details are collected and analyzed by Juniper ATP Cloud.
3. **Automated detection and Remediation**—ATP events are correlated with user and device information and added to Infected Host feed.
4. **Host is blocked**

Workflow

This section provides the workflow to perform Encrypted Traffic Insights.

Step	Description
1	A client host requests a file to be downloaded from the Internet.
2	Juniper Secure Edge receives the response from the Internet. Juniper Secure Edge extracts the server certificate from the session and compares its signature with the blocklist certificate signatures. If a match occurs, then connection is blocked. NOTE: The Juniper Networks ATP Cloud feed keeps Juniper Secure Edge up to date with a feed of certificates associated with known malware sites.
3	Juniper Secure Edge collects the metadata and connection statistics and sends it to the ATP Cloud for analysis.
4	The ATP Cloud performs behavioral analysis to classify the traffic as benign or malicious.
5	If a malicious connection is detected, the threat score of the host is recalculated. If the new score is above the threshold, then the client host is added to infected host list, The client host might be blocked based on policy configurations on Juniper Secure Edge devices.

RELATED DOCUMENTATION

[Encrypted Traffic Insights Details](#) | 145

Encrypted Traffic Insights Details

To access this page, navigate to **Monitor > ATP > Encrypted Traffic**. Click on the any of the **External Server IP** address link.

Use Encrypted Traffic Insights Details page to view analysis information and a threat summary for the external server. The following information is displayed for each server:

- Total Hits

- Threat Summary (Location, Category, Time last seen)
- Ports and protocols used

The Encrypted Traffic Insights Details page is divided into several sections:

[Table 61 on page 146](#) lists the actions that you can perform on this page. You can perform these actions using the options that are available on the upper right corner of page.

Table 61: Options on the Encrypted Traffic Insights Details Page

Button/Link	Purpose
Select Option > Add to Allowlist	Choose this option to allowlist the server from Encrypted Traffic Insights based detections. NOTE: You can also allowlist the servers from the Configure > Allowlist > ETA page.
Select Option > Report False Positive	Choose this option to send a report to Juniper Networks, informing Juniper of a false positive. Juniper will investigate the report; however, this does not change the verdict.

Under Time Range is a graph displaying the frequency of events over time. An event occurs when a host communicates to the external server IP address (either sending or receiving data). You can filter this information by clicking on the timeframe links: 1 day, 1 week, 1 month, Custom (select your own timeframe).

Hosts is a list of hosts that have contacted the external server. [Table 62 on page 146](#) lists the information provided in this section.

Table 62: External Server Contacted Host Data

Field	Definition
Client Host	The name of the host in contact with the external server.
Client IP Address	The IP address of the host in contact with the external server. (Click through to the Host Details page for this host IP address.)
Threat Level at Time	The threat level of the external server as determined by an analysis of actions and behaviors at the time of the event.

Table 62: External Server Contacted Host Data (Continued)

Field	Definition
Status	The action taken by the device on the communication (whether it was permitted or blocked). NOTE: At this point of time, Encrypted Traffic Insights only detects malicious threats but does not block it. Actions such as blocking is handled by features such as infected hosts based on the host threat score and customer policies.
Protocol	The protocol (https) the external server used to attempt communication.
Source Port	The port the external server used to attempt communication.
Uploaded	Number of bytes uploaded to the server.
Downloaded	Number of bytes downloaded from the server.
Device Name	The name of the Juniper Secure Edge device in contact with the external server.
Date/Time Seen	The date and time of the most recent external server hit.
Username	The name of the host user in contact with the external server.

Select a client host and click **Download packet** to download the packet capture details and view more information about the network/SSL traffic.

Domains is a list of domains that the IP address has previously used at the time of suspicious events. If an external IP address is seen changing its DNS/domain name to evade detection, a list of the various names used will be listed along with the dates in which they were seen.

Table 63: External Server Associated Domains Data

Field	Definition
C&C Host	This is a list of domains the destination IP addresses in the external server events resolved to.
Last Seen	The date and time of the most recent external server hit.

Signatures is a list of the threat indicators associated with the IP address.

Table 64: ETA Server Signature Data

Field	Definition
Name	The name or type of detected malware.
Category	Description of the malware and way in which it may have compromised a resource or resources.
Date	The date the malware was seen.

Certificates is a list of certificates associated with the external server. Click **View Certificate** and **Download Certificate**

Table 65: ETA Server Certificate Data

Field	Definition
Subject	Specifies the IP address of the external server.
Issuer	Specifies the authority that issued the certificate.
SHA1	SHA1 hash of the server certificate.
Date/Time Seen	The date and time when the SHA1 file was last updated.

RELATED DOCUMENTATION

[Encrypted Traffic Insights Overview](#) | 143

SMTP Quarantine Overview

Access this page from the **Monitor > ATP > Blocked Email** menu.

The SMTP quarantine monitor page lists quarantined emails with their threat score and other details including sender and recipient. You can also act on quarantined emails here, including releasing them and adding them to the blocklist.

NOTE: SMTP is supported only for Security Director Cloud use cases.

The following information is available from the Summary View:

Table 66: Blocked Email Summary View

Field	Description
Time Range	Use the slider to narrow or increase the timeframe within the selected the time parameter in the top right: 12 hrs, 24 hrs, 7 days or custom.
Total Email Scanned	This lists the total number of emails scanned during the chosen timeframe and then categorizes them into blocked, quarantined, released, and permitted emails.
Malicious Email Count	This is a graphical representation of emails, organized by time, with lines for blocked emails, quarantined and not released emails, and quarantined and released emails.
Emails Scanned	This is a graphical representation of emails, organized by time, with lines for total emails, and emails with one or more attachments.
Email Classification	This is another graphical view of classified emails, organized by percentage of blocked emails, quarantined and not released emails, and quarantined and released emails.

The following information is available from the Details View:

Table 67: Blocked Email Details View

Field	Description
Recipient	The email address of the recipient.
Sender	The email address of the sender.
Subject	Click the Read This link and preview the email.
Date	The date the email was received.
Malicious Attachment	Click on the attachment name to go to the Juniper ATP Cloud file scanning page where you can view details about the attachment.
Size	The size of the attachment in kilobytes.
Threat Score	The threat score of the attachment, 0-10, with 10 being the most malicious.
Threat Name	The type of threat found in the attachment, for example, worm or trojan.
Action	The action taken, including the date and the person (recipient or administrator) who took the action.

Using the available buttons on the Details page, you can take the following actions on blocked emails:

- Add domain to blocklist
- Add sender to blocklist
- Release

IMAP Block Overview

Access this page from the **Monitor > ATP > Blocked Email** menu.

The IMAP Block monitor page lists blocked emails with their threat score and other details including sender and recipient. You can also act on blocked emails here, including releasing them and adding them to the blocklist.

NOTE: IMAP is supported only for Security Director Cloud use cases.

The following information is available from the Summary View:

Table 68: Blocked Email Summary View

Field	Description
Time Range	Use the slider to narrow or increase the timeframe within the selected the time parameter in the top right: 12 hrs, 24 hrs, 7 days or custom.
Malicious Email Count	This lists the total number of malicious emails scanned during the chosen timeframe and then categorizes them into blocked, blocked and not allowed, quarantined and allowed.
Emails Scanned	This is a graphical representation of all scanned emails, organized by date.

The following information is available from the Detail View:

Table 69: Blocked Email Detail View

Field	Description
Recipient	The email address of the recipient.
Sender	The email address of the sender.
Subject	Click the Read This link and preview the email.
Date	The date the email was received.

Table 69: Blocked Email Detail View (Continued)

Field	Description
Malicious Attachment	Click on the attachment name to go to the Juniper ATP Cloud file scanning page where you can view details about the attachment.
Size	The size of the attachment in kilobytes.
Threat Score	The threat score of the attachment, 0-10, with 10 being the most malicious.
Threat Name	The type of threat found in the attachment, for example, worm or trojan.
Action	The action taken, including the date and the person (recipient or administrator) who took the action.

Using the available buttons on the Details page, you can take the following actions on blocked emails:

- Unblock Attachment for Selected User(s)
- Unblock Attachment for All Users

Telemetry Overview

Access this page from the **Monitor > ATP > Telemetry > Web Protocols** or **Email Protocols** menu.

The telemetry page provides comprehensive monitoring information of devices for a variety of activities, including the number of web and e-mail files scanned or blocked per protocol. It also offers a counter reset capability.

Benefits of Telemetry

- Exposes monitoring data in the web portal.
- Centralizes valuable monitoring data in one place, facilitating the ability to put events in context against other events for a more comprehensive view of the network.

Reset button—When you select the check box for a device and click Reset, it clears the counter to zero for that device and protocol. This reset applies only to the information displayed on the web portal.

NOTE: In a chassis cluster environment (both active/passive, active/active), each node shares the telemetry data separately. Both the node details are displayed separately in the web portal.

For the Devices listed on this page, you can view the following information for Web Protocols by selecting the HTTP tab and the HTTPS tab.

Table 70: Telemetry Data for Web Protocols

Web Protocols	Available Data
HTTP and HTTPS	Host Name
	Total Scanned
	Blocked
	Permitted
	Quarantined
	Tag and deliver
	Ignored
	Blocklist hits
	Allowlist hits
	Last Reset (This is the time when the device counter was last reset to zero. Note that the reset applies only to the information that is displayed on the web portal.)

For the Devices listed on this page, you can view the following information for Email Protocol by selecting the tabs that correspond to SMTP, SMTPS, IMAP, and IMAPS.

Table 71: Telemetry Data for Email Protocols

Email Protocols	Available Data
SMTP and SMTPS	Host Name
IMAP and IMAPS	Total Scanned
	Blocked
	Permitted
	Quarantined
	Tag and Deliver
	Ignored
	Blocklist hits
	Allowlist hits
	Last Reset (This is the time when the device counter was last reset to zero. Note that the reset applies only to the information that is displayed on the web portal.)

Reports

IN THIS CHAPTER

- [Reports Overview | 155](#)
- [Managing Reports | 155](#)

Reports Overview

Reports are generated based on a summary of network activity and overall network status. These generated reports can help you perform a trend analysis of your network's activities and study changes in traffic patterns.

Using reports, you can:

- Schedule reports based on the defined filters.
- Schedule reports based on the available default reports.

A Juniper Networks branded cover page is the default cover sheet of the reports. It contains the report title, name, and date of report creation. The generated report includes Table of Contents (TOC) with links to each section of the report. When the system generates a report, you and other designated recipients receive the report in PDF format through e-mail.

Managing Reports

You can perform various actions using reports, such as run a report immediately, edit a schedule, edit e-mail recipients, preview a report in the PDF format, send reports, clone reports, and view report definition details.

1. Select **Monitor > Reports > Report Definitions**.
2. Select the report definition, and click one of the following options:

Table 72: More Menu Settings

Setting	Guidelines
Run Now	<p>Select this option to run the report immediately and view the report in the PDF format.</p> <ol style="list-style-type: none"> a. Configure according to the guidelines provided in the Table 73 on page 158 . b. Click OK. The report is generated and a link is displayed to download the report in the PDF format. <p>You can also view the archived reports by clicking the Generated Reports link on the left navigation pane.</p>
Detail	<p>Select this option to view the report name, description, report content type, report definition type, and its contents in the Report Definition Details page.</p> <p>You can also click the icon next to Name in the Report Definitions page to view the Report Definitions Details page.</p>
Preview as PDF	<p>Select this option to preview the generated report in the PDF format.</p> <p>You can also generate the report as needed.</p>

Table 72: More Menu Settings (Continued)

Setting	Guidelines
Send Report	<p>Select this option to send the report through e-mail to the recipient.</p> <ol style="list-style-type: none"> a. Configure according to the guidelines provided in the Table 73 on page 158. b. Click OK. <p>The Edit Recipients page is displayed.</p> <ol style="list-style-type: none"> c. Modify or add the recipients, subject line, or any comments for the e-mail notifications. d. Click OK to send the report to the recipients. <p>A success message is displayed.</p> <p>The user receives a notification once the report is sent. The user can also use the job ID to see more details of the job. You can generate the report as needed.</p>
Edit Recipients	<p>Select this option to edit or add the recipients, e-mail address, subject, and comments.</p> <ol style="list-style-type: none"> a. Modify or add recipients, subject, and comments in the e-mail. b. Click OK.
Edit Schedule	<p>Select this option to edit the schedule such as the start date, end date, and time.</p> <p>Click one of the following:</p> <ul style="list-style-type: none"> • Run Now—To schedule the job immediately. • Schedule at a later time—Select a date and time to schedule the job at a later period of time.

Table 72: More Menu Settings (Continued)

Setting	Guidelines
Clone	<p>Select this option to clone an existing report definition.</p> <ol style="list-style-type: none"> a. Edit the details of the report. b. Click OK.

Table 73: Run Now Settings

Fields	Description
Types	<p>Choose an option from the following types:</p> <ul style="list-style-type: none"> • Run Now—To generate the report immediately, for the default time duration. • Custom Time Range Selection—To generate the report immediately for a selected time range. <p>If you select the type as Custom Time Range Selection, then Show Top and Time Span (Last) fields are displayed.</p> <ul style="list-style-type: none"> • Username—Select the user to run the user-specific URLs Visited Per User Report. This field is displayed only when you select to run the URLs Visited Per User Report.
Show Top	<p>Select the number of top records to be displayed in the generated report.</p> <p>The valid range is 1 to 20.</p>
Time Span (Last)	<p>Select a period in minutes, hours, days, or months, or select Custom to choose the time range to generate reports.</p>
Devices	<p>Select all devices or specific device. By default, data is displayed for all the devices in the network.</p> <p>Choose the Selective option to select specific devices.</p> <p>Select devices from the Available column and click the right arrow to move these devices to the Selected column.</p>

Report Definitions

IN THIS CHAPTER

- Report Definitions Main Page Fields | 159
- Create Threat Analysis Report Definitions | 160
- Create Application User Usage Report Definitions | 162
- Create IPS Report Definitions | 164
- Create Rule Analysis Report Definitions | 166
- Create Security Events Report Definitions | 168
- Create Top Talkers Report Definitions | 171
- Create Network Operations Report Definitions | 173
- Create URLs Visited Per User Report Definitions | 174
- Create Log Streaming Report Definitions | 176
- Using Report Definitions | 178
- Editing Report Definitions | 180
- Deleting Report Definitions | 180

Report Definitions Main Page Fields

Use this page to get an overall, high-level view of your report definition settings. You can filter and sort this information to get a better understanding of what you want to configure.

[Table 74 on page 159](#) describes the fields on the Report Definitions page.

Table 74: Report Definition Main Page Fields

Field	Description
ID	The unique identifier of the report.

Table 74: Report Definition Main Page Fields (Continued)

Field	Description
Name	The name of the report, which can be user-created or predefined.
Description	The description of the report definition.
Type	The type of report definition used, such as log reports, bandwidth report, or policy analysis reports.
Definition Type	The predefined report.
Schedule	The report generation schedule.
Recipients	The recipients of the generated reports.
Last Generated	The time when the last report was generated, along with the status.
Job ID	The unique job ID of the report.

Create Threat Analysis Report Definitions

The threat analysis report provides an assessment of threats that target applications by bypassing traditional network-layer protections. The report also analyzes insider threats from users by allowing them unlimited access to these applications.

Before You Begin

- Read the ["Reports Overview" on page 155](#) topic.
 - Review the Reports main page for an understanding of your current data set. See ["Report Definitions Main Page Fields" on page 159](#) for field descriptions.
1. Select **Monitor > Reports > Report Definitions**.
 2. Click **Create**, and select **Threat Assessment Report**.
 3. Complete the configuration according to the guidelines provided in the [Table 75 on page 161](#) .

Table 75: Threat Analysis Report Definition Settings

Settings	Guidelines
General Information	
Report Name	<p>Enter a unique string for the report name containing maximum 64 alphanumeric characters.</p> <p>The name can contain dashes.</p>
Description	<p>Enter a description containing maximum 900 characters for the report.</p>
Content	
Time Span	<p>Specify the duration for which the report is generated.</p> <p>You can select a time span of the last 3 to 24 hours or a custom time span. When you select the custom option, you must specify the From and To date in the MM/DD/YYYY and HH:MM:SS format.</p>
Number of Top Logs	<p>Enter the number of top events to be displayed.</p> <p>The valid range is 1 to 10, and the default value is 5.</p>
Schedule	
Report Schedule	<p>Click Add Schedule.</p> <p>Select the type of report schedule to use:</p> <ul style="list-style-type: none"> • Run now—Select this option to schedule and publish the configuration at the current time. • Schedule at a later time—Select this option to schedule and publish the configuration at a later time.
Email Section	

Table 75: Threat Analysis Report Definition Settings (Continued)

Settings	Guidelines
Email Recipients	<p>Enable this option to send the report to specific recipients in an email.</p> <ul style="list-style-type: none"> • Recipients—Enter or select the e-mail addresses of the recipients. By default, you can search by first name and select registered users. You can also type in external email addresses. • Subject—Enter a subject line containing maximum 2048 characters for the e-mail. • Comments—Enter the text containing maximum 2048 to include in the body of the e-mail. <p>NOTE: The reports are not sent if a specified recipient does not have permission for a device or domain included in the report configuration when the report is generated.</p>

4. Click **OK** to save the report definition.

A new threat analysis report definition with the defined configurations is created.

Create Application User Usage Report Definitions

The application user usage report provides an overview of the business risks in relation to applications and user behavior, such as abnormalities that can lead to data loss, bandwidth hogging, time-consuming applications, and personal applications that can increase business risks.

Before You Begin

- Read the "[Reports Overview](#)" on [page 155](#) topic.
- Review the Reports main page for an understanding of your current data set. See "[Report Definitions Main Page Fields](#)" on [page 159](#) for field descriptions.

1. Select **Monitor > Reports > Report Definitions**.
2. Click **Create**, and select **Application User Usage Report**.
3. Complete the configuration according to the guidelines provided in the [Table 76 on page 163](#).

Table 76: Application User Usage Report Definition Settings

Settings	Guidelines
General Information	
Report Name	<p>Enter a unique string for the report name containing maximum 64 alphanumeric characters.</p> <p>The name can contain dashes.</p>
Description	<p>Enter a description containing maximum 900 characters for the report.</p>
Content	
Time Span	<p>Specify the duration for which the report is generated.</p> <p>You can select a time span of the last 3 to 24 hours or a custom time span. When you select the custom option, you must specify the From and To date in the MM/DD/YYYY and HH:MM:SS format.</p>
Number of Top Logs	<p>Enter the number of top events to be displayed.</p> <p>The valid range is 1 to 10, and the default value is 5.</p>
Schedule	
Report Schedule	<p>Click Add Schedule.</p> <p>Select the type of report schedule to use:</p> <ul style="list-style-type: none"> • Run now—Select this option to schedule and publish the configuration at the current time. • Schedule at a later time—Select this option to schedule and publish the configuration at a later time.
Email Section	

Table 76: Application User Usage Report Definition Settings (*Continued*)

Settings	Guidelines
Email Recipients	<p>Enable this option to send the report to specific recipients in an email.</p> <ul style="list-style-type: none"> • Recipients—Enter or select the e-mail addresses of the recipients. By default, you can search by first name and select registered users. You can also type in external email addresses. • Subject—Enter the subject for the e-mail notification. • Comments—Enter the comments for the e-mail notification. <p>NOTE: The reports are not sent if a specified recipient does not have permission for a device or domain included in the report configuration when the report is generated.</p>

4. Click **OK** to save the report definition.

A new threat analysis report definition with the defined configurations is created.

Create IPS Report Definitions

The IPS report includes charts and details that show you the IPS activity over time as well as the top attacks, the categories of attacks, and the targeted hosts.

This information in the IPS report helps you determine if new exploits have been discovered or if any network-borne attacks against the client and server system vulnerabilities were detected and blocked which prevented damage to the system.

Before You Begin

- Read the ["Reports Overview" on page 155](#) topic.
 - Review the Reports main page for an understanding of your current data set. See ["Report Definitions Main Page Fields" on page 159](#) for field descriptions.
1. Select **Monitor > Reports > Report Definitions**.
 2. Click **Create**, and select **IPS Report**.
 3. Complete the configuration according to the guidelines provided in [Table 77 on page 165](#).

Table 77: IPS Report Definition Settings

Settings	Guidelines
General	
Report Name	<p>Enter a unique string for the report name containing maximum 64 alphanumeric characters.</p> <p>The name can contain dashes.</p>
Description	<p>Enter a description containing maximum 900 characters for the report.</p>
Content	
Time Span	<p>Specify the duration for which the report is generated.</p> <p>You can select a time span of the last 3 to 24 hours or a custom time span. When you select the Custom option, you must specify the From and To date in the MM/DD/YYYY and HH:MM:SS format.</p>
Number of Top Logs	<p>Enter the number of top events to be displayed.</p> <p>The valid range is 1 to 10, and the default value is 5.</p>
Schedule	
Report Schedule	<p>Click Add Schedule.</p> <p>Select the type of report schedule to use:</p> <ul style="list-style-type: none"> • Run now—Select this option to schedule and publish the configuration at the current time. • Schedule at a later time—Select this option to schedule and publish the configuration at a later time.
Email Section	

Table 77: IPS Report Definition Settings (Continued)

Settings	Guidelines
Email Recipients	<p>Enable this option to send the report to specific recipients in an email.</p> <ul style="list-style-type: none"> • Recipients—Enter or select the e-mail addresses of the recipients. You can search e-mail addresses of users by their first name. You can also enter external email addresses. • Subject—Enter the subject for the e-mail notification. • Comments—Enter the comments for the e-mail notification. <p>NOTE: The reports are not sent if a specified recipient does not have permission for a device or domain included in the report configuration when the report is generated.</p>

4. Click **OK** to save the report definition.

A new IPS report definition with the defined configurations is created.

Create Rule Analysis Report Definitions

The Rule Analysis report contains information about the rules applied to security policies and anomalies detected in the security policies.

Before You Begin

- Read the "[Reports Overview](#)" on page 155 topic.
 - Review the Reports main page to understand your current data set. See "[Report Definitions Main Page Fields](#)" on page 159 for field descriptions.
1. Select **Monitor > Reports > Report Definitions**.
 2. Click **Create**, and select **Rule Analysis Report**.
The Create Rule Analysis Report Definition page opens.
 3. Complete the configuration according to the guidelines provided in [Table 78 on page 167](#).

Table 78: Rule Analysis Report Definition Settings

Settings	Guidelines
General	
Report Name	<p>Enter a unique string for the report name containing maximum 64 alphanumeric characters.</p> <p>The name can contain dashes.</p>
Description	Enter a description containing maximum 900 characters for the report.
Content	
Anomalies	<p>Select the anomalies for Juniper Security Director Cloud to identify while analyzing the rules in a policy.</p> <ul style="list-style-type: none"> • Shadowed • Redundant • Expired scheduler • Logging disabled • Unused rules
Security policies	Select the security policies to perform the rule analysis.
Schedule	
Report Schedule	<p>Click Add Schedule.</p> <p>Select the type of report schedule to use:</p> <ul style="list-style-type: none"> • Run now—Select this option to schedule and to publish the configuration at the current time. • Schedule at a later time—Select this option to schedule and to publish the configuration at a later time.

Table 78: Rule Analysis Report Definition Settings (*Continued*)

Settings	Guidelines
Email Section	
Email Recipients	<p>Enable this option to send the report to specific recipients in an email.</p> <ul style="list-style-type: none"> • Recipients—Enter or select the e-mail addresses of the recipients. You can search e-mail addresses of users by their first name. You can also enter external email addresses. • Subject—Enter the subject for the e-mail notification. • Comments—Enter the comments for the e-mail notification. <p>NOTE: The report is not sent to recipients who do not have permissions to access a device or domain included in the report configuration.</p>

4. Click **OK** to save the report definition.

A new Rule Analysis report definition is created and displayed on the Reports Definitions page.

Create Security Events Report Definitions

The Security Events report is a comprehensive document that outlines all security events that occurs within your network over a specific period through charts and details. The report includes information about security-related incidents such as malware infections, phishing attempts, unauthorized access attempts, and other types of security incidents.

The following information in the report helps you determine if new exploits have been discovered or if any network-borne attacks against the client and server system vulnerabilities were detected and blocked, preventing damage to the system:

- Firewall rules used most often.
- User roles involved in the network traffic most often.
- Source and destination IP addresses involved in the network traffic most often.
- Services allowed access and services denied access most often.
- Source IP addresses and destination IP addresses denied access by the firewall most often.

- Firewall events, including the source and destination countries of the firewall events allowed and denied most often.
- Applications accessed, including the source and destination countries of the websites blocked and the applications that used encryption most often.
- Viruses detected, including the host servers targeted, the countries from where the viruses originated and the countries that the viruses targeted most often.
- Spam detected, including the countries from where the maximum spam originated and content was censored and countries from where IPS-related events originated and were destined most often.
- SecIntel and AAMW events detected, including the hostnames of servers that security-related threats and malware targeted most often.

Before You Begin

- Read the ["Reports Overview" on page 155](#) topic.
- Review the Reports main page to understand your current data set. See ["Report Definitions Main Page Fields" on page 159](#) for field descriptions.

1. Select **Monitor > Reports > Report Definitions**.
2. Click **Create**, and select **Security Events Report**.
The Security Events Report page opens.
3. Complete the configuration according to the guidelines provided in [Table 79 on page 169](#).

Table 79: Security Events Report Definition Settings

Settings	Guidelines
General	
Report Name	Enter a unique string for the report name containing maximum 64 alphanumeric characters. The name can contain dashes.
Description	Enter a description containing maximum 900 characters for the report.
Content	

Table 79: Security Events Report Definition Settings (Continued)

Settings	Guidelines
Time Span	<p>Specify the duration for which the report is generated.</p> <p>You can select a time span of the last 3 to 24 hours or a custom time span. When you select the Custom option, you must specify the From and To date in the MM/DD/YYYY and HH:MM:SS format.</p>
Number of Top Logs	<p>Enter the number of top events to be displayed.</p> <p>The valid range is 1 to 10, and the default value is 5.</p>
Schedule	
Report Schedule	<p>Click Add Schedule.</p> <p>Select the type of report schedule to use:</p> <ul style="list-style-type: none"> • Run now—Select this option to schedule and publish the configuration at the current time. • Schedule at a later time—Select this option to schedule and publish the configuration at a later time.
Email Section	
Email Recipients	<p>Enable this option to send the report to specific recipients in an email.</p> <ul style="list-style-type: none"> • Recipients—Enter or select the e-mail addresses of the recipients. You can search e-mail addresses of users by their first name. You can also enter external email addresses. • Subject—Enter the subject for the e-mail notification. • Comments—Enter the comments for the e-mail notification. <p>NOTE: The report is not sent to recipients who do not have permissions to access a device or domain included in the report configuration.</p>

4. Click **OK** to save the report definition.

A new Security Events report definition is created and displayed on the Reports Definitions page.

Create Top Talkers Report Definitions

The Top Talkers report contains information about the top 10 source IP addresses and top 10 destination IP addresses visited by users. The information about these top 10 IP addresses is categorized based on the bandwidth the sessions consumed and number of sessions. The report also contains information about the top 10 users who consumed the most bandwidth and initiated the most web sessions.

Before You Begin

- Read the ["Reports Overview" on page 155](#) topic.
 - Review the Reports main page to understand your current data set. See ["Report Definitions Main Page Fields" on page 159](#) for field descriptions.
1. Select **Monitor > Reports > Report Definitions**.
 2. Click **Create**, and select **Top Talkers Report**.
The Create Top Talkers Report Definition page opens.
 3. Complete the configuration according to the guidelines provided in [Table 80 on page 171](#).

Table 80: Top Talkers Report Definition Settings

Settings	Guidelines
General	
Report Name	Enter a unique string for the report name containing maximum 64 alphanumeric characters. The name can contain dashes.
Description	Enter a description containing maximum 900 characters for the report.
Content	
Time Span	Specify the duration for which the report is generated. You can select a time span of the last 3 to 24 hours or a custom time span. When you select the Custom option, you must specify the From and To date in the MM/DD/YYYY and HH:MM:SS format.

Table 80: Top Talkers Report Definition Settings (Continued)

Settings	Guidelines
Number of Top Logs	Enter the number of top events to be displayed. The valid range is 1 to 10, and the default value is 5.
Schedule	
Report Schedule	Click Add Schedule . Select the type of report schedule to use: <ul style="list-style-type: none"> • Run now—Select this option to schedule and to publish the configuration at the current time. • Schedule at a later time—Select this option to schedule and to publish the configuration at a later time.
Email Section	
Email Recipients	Enable this option to send the report to specific recipients in an email. <ul style="list-style-type: none"> • Recipients—Enter or select the e-mail addresses of the recipients. You can search e-mail addresses of users by their first name. You can also enter external email addresses. • Subject—Enter the subject for the e-mail notification. • Comments—Enter the comments for the e-mail notification. <p>NOTE: The report is not sent to recipients who do not have permissions to access a device or domain included in the report configuration.</p>

4. Click **OK** to save the report definition.

A new Top Talkers report definition is created and displayed on the Reports Definitions page.

Create Network Operations Report Definitions

The Network Operations report contains information about the top 10 source countries and top 10 destination countries that are allowed and blocked. The information is categorized based on the bandwidth usage and the number of sessions.

Before You Begin

- Read the ["Reports Overview" on page 155](#) topic.
 - Review the Reports main page to understand your current data set. See ["Report Definitions Main Page Fields" on page 159](#) for field descriptions.
1. Select **Monitor > Reports > Report Definitions**.
 2. Click **Create**, and select **Network Operations Report**.
The Create Network Operations Report Definition page opens.
 3. Complete the configuration according to the guidelines provided in [Table 81 on page 173](#).

Table 81: Network Operations Report Definition Settings

Settings	Guidelines
General	
Report Name	Enter a unique string for the report name containing maximum 64 alphanumeric characters. The name can contain dashes.
Description	Enter a description containing maximum 900 characters for the report.
Content	
Time Span	Specify the duration for which the report is generated. You can select a time span of the last 3 to 24 hours or a custom time span. When you select the Custom option, you must specify the From and To date in the MM/DD/YYYY and HH:MM:SS format.
Number of Top Logs	Enter the number of top events to be displayed. The valid range is 1 to 10, and the default value is 5.

Table 81: Network Operations Report Definition Settings (*Continued*)

Settings	Guidelines
Schedule	
Report Schedule	<p>Click Add Schedule.</p> <p>Select the type of report schedule to use:</p> <ul style="list-style-type: none"> • Run now—Select this option to schedule and to publish the configuration at the current time. • Schedule at a later time—Select this option to schedule and to publish the configuration at a later time.
Email Section	
Email Recipients	<p>Enable this option to send the report to specific recipients in an email.</p> <ul style="list-style-type: none"> • Recipients—Enter or select the e-mail addresses of the recipients. You can search e-mail addresses of users by their first name. You can also enter external email addresses. • Subject—Enter the subject for the e-mail notification. • Comments—Enter the comments for the e-mail notification. <p>NOTE: The report is not sent to recipients who do not have permissions to access a device or domain included in the report configuration.</p>

4. Click **OK** to save the report definition.

A new Network Operations report definition is created and displayed on the Reports Definitions page.

Create URLs Visited Per User Report Definitions

The URLs Visited Per User report is specific to a user and contains information about the top 10 URLs that the user visited and the date and time when the user visited the URLs. The report also contains information about the risky URLs visited along with the categories of the URLs an assessment of the bandwidth usage.

Before You Begin

- Read the ["Reports Overview" on page 155](#) topic.
- Review the Reports main page to understand your current data set. See ["Report Definitions Main Page Fields" on page 159](#) for field descriptions.

1. Select **Monitor > Reports > Report Definitions**.
2. Click **Create**, and select **URLs Visited Per User Report**.
The Create URLs Visited Per User Report Definition page opens.
3. Complete the configuration according to the guidelines provided in [Table 82 on page 175](#) .

Table 82: URLs Visited Per User Report Definition Settings

Settings	Guidelines
General	
Report Name	Enter a unique string for the report name containing maximum 64 alphanumeric characters. The name can contain dashes.
Description	Enter a description containing maximum 900 characters for the report.
Content	
Time Span	Specify the duration for which the report is generated. You can select a time span of the last 3 to 24 hours or a custom time span. When you select the Custom option, you must specify the From and To date in the MM/DD/YYYY and HH:MM:SS format.
Number of Top Logs	Enter the number of top events to be displayed. The valid range is 1 to 10, and the default value is 5.
Schedule	

Table 82: URLs Visited Per User Report Definition Settings (*Continued*)

Settings	Guidelines
Report Schedule	<p>Click Add Schedule.</p> <p>Select the type of report schedule to use:</p> <ul style="list-style-type: none"> • Run now—Select this option to schedule and to publish the configuration at the current time. • Schedule at a later time—Select this option to schedule and to publish the configuration at a later time.
Email Section	
Email Recipients	<p>Enable this option to send the report to specific recipients in an email.</p> <ul style="list-style-type: none"> • Recipients—Enter or select the e-mail addresses of the recipients. You can search e-mail addresses of users by their first name. You can also enter external email addresses. • Subject—Enter the subject for the e-mail notification. • Comments—Enter the comments for the e-mail notification. <p>NOTE: The report is not sent to recipients who do not have permissions to access a device or domain included in the report configuration.</p>

4. Click **OK** to save the report definition.

A new URLs Visited Per User report definition is created and displayed on the Reports Definitions page.

Create Log Streaming Report Definitions

You can create a log stream report to view the data (bytes) transferred to the SIEM system, such as Microsoft Sentinel. You can create a report for the current month, previous month, or the entire period of data transfer. The report contains the log stream name, the type of log forwarded (audit log, sessions log, or security events), and the number of bytes forwarded to the external SIEM system.

Before You Begin

- Read the "[Reports Overview](#)" on [page 155](#) topic.

- Review the Reports main page for an understanding of your current data set. See "[Report Definitions Main Page Fields](#)" on page 159 for field descriptions.

To configure a log stream report:

1. Select **Monitor > Reports > Report Definitions**.
2. Click **Create**, and select **Log Streaming Report**.

The Create Log Streaming Report Definition page is displayed.

3. Complete the configuration according to the guidelines provided in [Table 83 on page 177](#) .

Table 83: Log Streaming Report Definition

Settings	Guidelines
General	
Report Name	Enter a unique string for the report name containing maximum 64 alphanumeric characters. The name can contain dashes.
Description	Enter a description containing maximum 900 characters for the report.
Content	
Report Type	<p>Select from the following options:</p> <ul style="list-style-type: none"> • Current Month Usage—Generate the report for current month till date • Last Month Usage—Generate the report for the previous month • Historical Usage—Generate the report about the entire period of data transfer except current month to the SIEM system.
Schedule	

Table 83: Log Streaming Report Definition (Continued)

Settings	Guidelines
Report Schedule	<p>Click Add Schedule.</p> <p>Select the type of report schedule to use:</p> <ul style="list-style-type: none"> • Run now—Schedule and publish the configuration at the current time. • Schedule at a later time—Schedule and publish the configuration at a later time.
Email Section	
Email Recipients	<p>Enable this option to send the report to specific recipients in an email.</p> <ul style="list-style-type: none"> • Recipients—Enter or select the e-mail addresses of the recipients. You can search e-mail addresses of users by their first name. You can also enter external email addresses. • Subject—Enter the subject for the e-mail notification. • Comments—Enter the comments for the e-mail notification.

4. Click **OK** to save the report definition.

A new log streaming report definition with the defined configurations is created.

Using Report Definitions

You can use the Report Definitions page to view a summary of network activity and overall network status.

1. Select **Monitor > Reports > Report Definitions**.

The Report Definitions page opens.

2. Click a column header.

The available options are:

- Sort Ascending—Sorts reports in ascending order, such as from A to Z or 1 to 10.
- Sort Descending—Sorts reports in descending order, such as from Z to A or 10 to 1.
- Show or Hide Columns—Provides a list of columns with check boxes to add or remove columns from the report definitions table. [Table 84 on page 179](#) lists the columns that you can add to the table or remove from the table.
- Check boxes—Each row has a check box. Select the check box to perform operations like, run now, preview as PDF, send report, edit recipients, edit schedule, clone, edit the report definitions, and delete the report definitions.

By default, some predefined reports are available.

Table 84: Report Definitions Columns

Field	Description
ID	The unique identifier of the report.
Name	The name of the report, which can be user-created or predefined.
Description	The description of the report definition.
Type	The type of report definition used, such as log reports, bandwidth report, or policy analysis reports.
Schedule	The report generation schedule.
Recipients	The recipients of the generated reports.
Last Generated	The time when the last report was generated, along with the status.
Job ID	The unique job ID of the report.

- Search for reports by using keywords—Click the search icon, enter the search term in the text box, and press **Enter**. The search results are displayed on the same page.

Editing Report Definitions

1. Select **Monitor > Reports > Report Definitions**.

The Report Definitions page opens.

2. Select a report definition by clicking the appropriate check box.

3. On the upper right side of the Report Definitions page, click **Edit**.

The edit report definition page opens. The options available on the create report definition page are available for editing.

4. Click **OK** to save your changes.

Deleting Report Definitions

You can clear all unwanted report definitions that are not used anywhere in your network.

NOTE: An error message appears if the report definition is used by any object.

1. Select **Monitor > Reports > Report Definitions**.

The report definitions page opens.

2. Select the report definition to delete, and then select the minus sign.

An alert message asking for confirmation to delete your selection is displayed.

3. Click **Yes** to delete your selection.

The delete report notification is displayed.

4. Click **OK**.

Generated Reports

IN THIS CHAPTER

- [Using Reports | 181](#)

Using Reports

IN THIS SECTION

- [Logging | 182](#)

Reports are generated based on a summary of network activity and overall network status. These generated reports can help you to perform a trend analysis of your network's activities to study changes in traffic patterns.

Using reports, you can:

- Schedule reports based on the defined filters.
- Schedule reports based on the available default reports.

A Juniper Networks branded cover page is the default cover sheet reports. It contains the report title, name, and date of report creation. You can provide your company logo on the cover page along with the Juniper Networks logo. You can also provide the text for the footer and the logo for the header. If you do not provide the header and footer, the Juniper Networks branded header and footer are used. The generated report includes Table of Contents (TOC) with links to each section of the report. When the system generates a report, you and other designated recipients receive the report in PDF format through e-mail.

Logging

Logs, also called event logs, provide vital information for managing network security incident investigation and response. Logging provides the following features:

- Receives events from SRX Series Firewalls and application logs.
- Stores events for a defined period of time or a set volume of data.
- Parses and indexes logs to help speed up searching.
- Provides queries and helps in data analysis and historical events investigation.

ATP Report Definitions

IN THIS CHAPTER

- [About the ATP Report Definition Page | 183](#)
- [Create ATP Report Definition | 185](#)
- [Edit and Delete ATP Report Definition | 187](#)
- [Send ATP Report | 188](#)

About the ATP Report Definition Page

IN THIS SECTION

- [Tasks You Can Perform | 183](#)

To access this page, select **Monitor > Reports > ATP Report Definitions**.

You can build custom threat assessment reports which meet your needs for viewing incidents during specific time-frames. Using the available fields, build a report that runs at set intervals and sends data to email addresses you select. You can also use the included, pre-defined, read-only, on-demand reports (Threat Assessment Last Day, Threat Assessment Last Week, and Threat Assessment Last Month). Once a report is run, it is listed in the Generated Reports page for downloading and viewing anytime.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a report—See "[Create ATP Report Definition](#)" on page 185 .
- Edit or delete a report—See "[Edit and Delete ATP Report Definition](#)" on page 187 .

- Send a report—See ["Send ATP Report" on page 188](#).
- Run a report—To run a pre-defined, read-only, on-demand report, select the check box for the report and click the **Run Now** button at the top of the list view page.

NOTE: Once a report is run, it is listed in the Reports> ATP Generated Reports page for viewing anytime.

- Show/Hide Columns—Choose to show or hide a specific column in the table. Hover over the vertical ellipses, select Show/Hide Columns, and select the check box of the columns to display in the table.
- Reset Preference—Reset the displayed columns to the default set of columns for each tab in the table. Hover your mouse cursor over the vertical ellipses, and select **Reset Preference**.

[Table 85 on page 184](#) describes the fields on the ATP Report Definition page.

Table 85: Fields on the ATP Report Definition Page

Field	Description
Name	The name of the ATP report, which can be user-created or predefined.
Description	The description of the report.
Definition Type	The report definition type: recurring or on-demand.
Duration	The duration of report generation: last day, last week, and last month.
Recurrence	The report generation schedule.
Recipients	The recipients of the generated reports.
Last Generated	The time when the last report was generated, along with the status.
Last Modified	The time when the last report was last modified.
Last Modified by	The user who last modified the report.

Table 85: Fields on the ATP Report Definition Page (Continued)

Field	Description
Report Definition ID	The unique identifier of the report.

Create ATP Report Definition

Use the available fields to build a report that runs at set intervals and automatically sends the PDF report to the email addresses you specify.

In addition to creating your own report definition, you can use the included, pre-defined, read-only, on demand reports. The included reports are named as follows:

- Threat Assessment Last Day
- Threat Assessment Last Week
- Threat Assessment Last Month

To create a custom ATP report definition:

1. Navigate to Monitor > Reports>ATP Report Definitions.

The ATP Report Definition Page appears.

2. Click the + (Create) icon on the top right of the page.

The Create Report page appears.

3. Complete the configuration according to the guidelines provided in the

4. Click OK to save the report definition.

A new ATP report definition with the defined configurations is created. The new report is listed as a downloadable PDF file in the Reports>Generated Reports page for viewing anytime.

Table 86: ATP Report Definition Settings

Settings	Guidelines
Report Name	<p>Enter a name for the report.</p> <p>The name must begin with an alphanumeric character and can include dashes, spaces, and underscores; 63-character maximum.</p>
Description	<p>Give the report a detailed description that all administrators can recognize.</p>
Date Range Options	<p>Configure a recurring schedule for running a report. The options are: Last Day (daily), Last Week (once weekly), and Last Month (once monthly).</p> <p>Based on your selection, you will configure a specific time period in the next field.</p>
Generate report every	<p>Use the downward arrow in the entry field for adding multiple days.</p> <p>If you selected Last Day in the previous field, choose multiple days of the week for running a report. For example, every day (add all days manually Sunday through Saturday) or only add Monday, Wednesday, and Friday for an every other day report.</p> <p>If you selected Last Week, choose one day of the week for running a weekly report.</p> <p>If you selected Last Month, choose whether to run a report on the first day of the month or the last day of the month.</p>

Table 86: ATP Report Definition Settings (Continued)

Settings	Guidelines
Email Recipients	<p>Once a report is generated, you can have it sent to one or more email addresses. The email addresses available for receiving reports come from the Administrator > Users list.</p> <p>Note that once the report is created, you can always send it to an email address on-demand by selecting the check box for the report in the list view and clicking the Send button at the top of the page. A new window appears, and you can select an email address there. Again, the available addresses come from the Administrator > Users list.</p>

Edit and Delete ATP Report Definition

IN THIS SECTION

- [Edit an ATP Report Definition | 187](#)
- [Delete an ATP Report Definition | 188](#)

You can edit and delete ATP report definitions from the ATP Report Definitions page. This topic has the following sections:

Edit an ATP Report Definition

1. Select **Monitor > Reports > ATP Report Definitions**.

The ATP Report Definitions page appears.

2. Select a report definition by clicking the appropriate check box.

3. On the upper right side of the ATP Report Definitions page, click **Edit (pencil) icon**.

The edit report definition page opens. The options available on the create report definition page are available for editing.

4. Modify the parameters according to the guidelines provided in [Table 86 on page 186](#).

5. Click **OK** to save your changes.

Delete an ATP Report Definition

You can clear all unwanted report definitions that are not used anywhere in your network.

NOTE: An error message appears if the report definition is used by any object.

1. Select **Monitor > Reports > ATP Report Definitions**.

The ATP Report Definitions page appears.

2. Select the report definition you want to delete, and then click the delete icon (trash can).

An alert message asking for confirmation to delete your selection is displayed.

3. Click **Yes** to delete your selection.

The delete report notification is displayed.

4. Click **OK**.

Send ATP Report

You can send the ATP report through e-mail to the recipients.

To send a report:

1. Select **Monitor > Reports > ATP Report Definitions**.

The ATP Report Definitions page appears.

2. Select a report and click **Send Report**.

The Send Report page appears.

3. Configure according to the guidelines provided in [Table 87 on page 188](#).

4. Click **OK**.

A message is displayed indicating the status of the operation. If the operation is successful, the user receives a notification once the report is sent.

Table 87: Send Report Settings

Setting	Guidelines
Subject	Enter the subject name of the report.
Comments	Enter the description for the report.

Table 87: Send Report Settings (Continued)

Setting	Guidelines
Email Recipients	Enter the e-mail address of the recipient to send the report.

ATP Generated Reports

IN THIS CHAPTER

- [About the ATP Generated Reports Page | 190](#)

About the ATP Generated Reports Page

IN THIS SECTION

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

To access this page, select **Monitor > Reports > ATP Generated Reports**.

You can configure ATP threat assessment reports to be run on-demand or on scheduled intervals. While you cannot determine the information included in the report, you can narrow information to a selected timeframe. When the system generates a report, you and other designated recipients receive the report in PDF format through e-mail.

Tasks You Can Perform

You can perform the following tasks from this page:

- Download the report—Click on a report PDF name to download the report. The content of the generated report is shown in [Table 89 on page 192](#).
- Delete the report—Select a report and click the delete icon (trash can). An alert message asking for confirmation to delete your selection is displayed. Click **Yes** to delete the report.

[Table 88 on page 191](#) displays the fields on ATP Generated Reports page.

Table 88: ATP Generated Reports

Field	Description
Report PDF Name	Name of the generated ATP report. Click on the report name to download the report. The details of the report is described in Table 89 on page 192 .
Generated Time	Date and time of report creation.
Description	Description of the generated report.
Definition	Definition of the generated report.
Generated By	User who generated the report.
Recipients	User with whom the report is shared.

Table 89: ATP Threat Assessment Report Contents

Report Category	Definition
Executive Summary	<p>An overview report data separated into following categories:</p> <ul style="list-style-type: none"> • Malware—Lists newly discovered malware and known malware. • C&C Server Destinations—Lists C&C server destination. <p>NOTE: The criteria to display the C&C server destination in the reports is that the threat level must be equal to or greater than 7.</p> <ul style="list-style-type: none"> • Hosts with Malicious Activities—Lists the following: <ul style="list-style-type: none"> • Infected hosts—Lists the number of potentially infected hosts whose threat level is less than the threshold threat level that is set by the customer. • Blocked hosts—Lists the number of infected hosts that have met the threshold threat level and is blocked by policies configured on Juniper Secure Edge. • Domains and URLs—Lists the domains and URLs that are suspicious or known to be risky. • High-risk User Data—Lists the following: <ul style="list-style-type: none"> • Users' computers infected with malware. • High-risk web sites accessed by users.
Malware	<p>The malware section contains the following information:</p> <ul style="list-style-type: none"> • Top Malware Identified—Lists the names of the top malware by count. • Top Infected File MIME Types—Lists the top infected multi-purpose Internet mail extensions (MIME) by count. • Top Scanned File Categories—Lists the top file categories that are scanned.

Table 89: ATP Threat Assessment Report Contents (*Continued*)

Report Category	Definition
C&C Server and Malware Locations	<p>This section contains the following information:</p> <ul style="list-style-type: none"> • Top C&C Server Location by Count—Lists the top countries for command and control (C&C) servers by number of communication attempts (C&C hits). • Top Malware Threat Locations by Count—Lists the top countries with malware threats.
Hosts	<p>This section contains the following information:</p> <ul style="list-style-type: none"> • Top Compromised Hosts—Lists the top hosts that may have been compromised based on their associated threat level.
Risky Files	<p>This section contains the following information:</p> <ul style="list-style-type: none"> • Top Risky File Categories by Count—Lists the top risky file categories by count for known and newly discovered malicious files. • Top Risky Files Detected by Count—Lists the top risky files detected by count. • Top IPs Detected Attempting to Access Risky Files by Count—Lists the top IP addresses attempting to access risky files. • Top Risky Files Detected by IPs—Lists the top risky files detected per top IP address attempting to access the files.

Table 89: ATP Threat Assessment Report Contents (Continued)

Report Category	Definition
Risky Domains, URLs, AND IPs	<p>This section contains the following information: top risky domains, URLs, and IP addresses detected by the number of times access was attempted. It also includes the top users who have attempted to access these risky domains, URLs, and IP addresses.</p> <ul style="list-style-type: none"> • Top Detected Risky Domains, URLs, and IPs by Count—Lists the top risky domains, URLs, and IP addresses detected by the number of times access was attempted. • Most Active Users for Risky Domains, URLs, and IPs by Count—Lists the top users who are most active in attempting to access the risky domains, URLs, and IP addresses by count. • Top Detected Risky Domains, URLs, and IPs by Threat Level —Lists the top risky domains, URLs, and IP addresses detected by the threat level.

Table 89: ATP Threat Assessment Report Contents (*Continued*)

Report Category	Definition
Email	<p>This section contains the list of actions taken on scanned emails. It also includes email attachments determined to be malware and users who are risky email senders.</p> <ul style="list-style-type: none"> • Actions Taken—Lists the action taken for scanned e-mail. • High-Risk Email Data—Lists the count of e-mail attachments with malware and risky senders. • Malicious SMTP Email by Count—The report breaks scanned e-mail down by protocol and lists SMTP e-mails found to be malicious. • Malicious IMAP Email by Count—The report breaks scanned e-mail down by protocol and lists IMAP e-mails found to be malicious. • Top Risky File Categories Detected for Email Attachments—Lists the top risky file categories that were detected from files received as e-mail attachments. • Top Risky Email Attachments Detected by Count—Lists the top risky files that are detected from email attachments. • Top Users Receiving Risky Email Attachments—Lists the top users who are receiving risky file attachments through e-mail. • Top Risky Email Attachments Detected per Top Users—Lists the top users and their most risky file attachments. • Top Risky Email Sender Domains by Count—Lists the top risky sender domains based on the threat level of file attachments sent in email. • Top Sender Domains of Risky File Attachments by Count—Lists the top sender domains with risky file attachments and the count of how many times the risky file attachments that were detected. • Actions on SMTP Malicious Email by Count—Lists actions taken for malicious SMTP e-mails.

Table 89: ATP Threat Assessment Report Contents (Continued)

Report Category	Definition
	<ul style="list-style-type: none"> • Actions on IMAP Malicious Email by Count—Lists actions taken for malicious IMAP e-mails.
Devices	<p>This section contains the following information:</p> <ul style="list-style-type: none"> • Zero submissions—List of devices that have not submitted files in the past 30 days. • Expiring Devices—List of devices that are going to expire in next 60 days.

Secure Edge Reports

IN THIS CHAPTER

- [About the Secure Edge Reports Page | 197](#)

About the Secure Edge Reports Page

IN THIS SECTION

- [Tasks You Can Perform | 197](#)

To access this page, select **Monitor > Reports > Secure Edge Reports**.

Secure edge report displays the data transfer details like monthly data allocation and usage at various regions. You can view the total outbound data transfer by region for the current month in comparison to the previous 11 months.

Tasks You Can Perform

You can view and download the outbound data transfer reports from this page, as shown in [Table 90 on page 198](#).

Table 90: Secure Edge Report Contents

Report Category	Definition
Summary	<p>A summary segment shows the following items for the current month:</p> <ul style="list-style-type: none"> • Total Data Transfer for current month—The actual data transfer occurred until date in the current month. • Monthly Allocation—The maximum data transfer limit allocated for the current month. • Overage—The excess data transferred beyond the monthly allocation.
Outbound Data Transfer by Region	<p>You can view the outbound data transfer in a graph and a tabular format. At various regions, you can view data transferred in the current month and in the previous 11 months.</p>

To download the Secure Edge reports, select the required month and year from the drop down list on the top right corner of the Secure Edge Reports page and click **Download Report**.

NOTE: You can update the report recipients by clicking **Update Report Recipients**.

4

PART

SRX

- Device Management-Devices | 201
- Device Management-Configuration Templates | 250
- Device Management-Images | 266
- Device Management-Security Packages | 274
- SRX Policy | 279
- SRX Policy-Device View | 332
- Security Subscriptions-IPS | 334
- Security Subscriptions-Content Security | 386
- Security Subscriptions-Decrypt Profiles | 440
- Security Subscriptions-SecIntel | 459
- Security Subscriptions-Anti-Malware | 477
- Security Subscriptions-Secure Web Proxy | 489
- IPsec VPN | 494
- IPsec VPN-VPN Profiles | 575
- IPsec VPN-Extranet Devices | 587
- NAT-NAT Policies | 590
- NAT-NAT Pools | 612
- Identity-JIMS | 619
- Identity-Active Directory | 628
- Identity-Access profile | 637

Device Management-Devices

IN THIS CHAPTER

- [About the Devices Page | 202](#)
- [Add Devices to Juniper Security Director Cloud | 222](#)
- [Manage Device Subscriptions | 228](#)
- [Create a Device Group | 229](#)
- [Edit a Device Group | 230](#)
- [Create a Preprovision Profile | 231](#)
- [Edit a Preprovision Profile | 232](#)
- [Delete Devices From Juniper Security Director Cloud | 233](#)
- [Add a License to a Device | 233](#)
- [Import a Device Certificate | 235](#)
- [Resynchronize a Device with Juniper Security Director Cloud | 237](#)
- [Out-of-Band Changes Overview | 237](#)
- [Resolve Out-of-Band Changes | 238](#)
- [Manage Configuration Versions | 239](#)
- [Reboot a Device | 244](#)
- [Enroll SRX Series Firewalls from ATP Cloud to Juniper Security Director Cloud | 245](#)
- [Disenroll SRX Series Firewall from ATP Cloud | 246](#)
- [Upgrade a Device | 247](#)
- [Security Logs Configuration | 248](#)

About the Devices Page

IN THIS SECTION

- [Tasks You Can Perform | 202](#)
- [Field Descriptions - Devices Page | 204](#)
- [Field Descriptions - Device Details Pane | 207](#)
- [Field Descriptions - Device Inventory Page > Overview Tab | 209](#)
- [Field Descriptions - Device Inventory Page > Chassis Tab | 211](#)
- [Field Descriptions - Device Inventory Page > Interfaces Tab | 212](#)
- [Field Descriptions - Device Inventory Page > Device Administration Tab | 214](#)
- [Field Descriptions - Device Inventory Page > Configuration Template Tab | 217](#)
- [Field Descriptions - Device Inventory Page > Junos Detailed Configurations Tab | 217](#)

To access this page, click **SRX > Device Management > Devices**.

The Devices page displays a list of devices that Juniper Security Director Cloud manages. You can view information about the device, such as the software release version, the platform, and various status indicators. You can also view the device inventory details, rollback to a configuration version, resynchronize or reboot a device, and upgrade a device.

To manage devices using Juniper Security Director Cloud, you must first add the devices to Juniper Security Director Cloud. After you add your devices, you can manage the devices using the Devices page.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add devices to Juniper Security Director Cloud. See ["Add Devices to Juniper Security Director Cloud" on page 222](#) .
- Delete a device from Juniper Security Director Cloud. See ["Delete Devices From Juniper Security Director Cloud" on page 233](#) .
- View the details of a device. Select a device, and click **More > Detail**. The details of the device is displayed in a panel on the right side of the page. See [Table 92 on page 207](#) .

- Resynchronize a device with Juniper Security Director Cloud. See ["Resynchronize a Device with Juniper Security Director Cloud"](#) on page 237
- Resolve out-of-band device changes. See ["Resolve Out-of-Band Changes"](#) on page 238 .
- View the active configuration of a device. Select a device, and click **More > View Active Configuration**. The Active Configuration page opens displaying the active configuration of the device.
- View configuration versions of a device. See ["Manage Configuration Versions"](#) on page 239 .
- Reboot a device. See ["Reboot a Device"](#) on page 244 .
- Enroll your SRX Series Firewall to ATP Cloud. See ["Enroll SRX Series Firewalls from ATP Cloud to Juniper Security Director Cloud"](#) on page 245 .
- Disenroll your SRX Series Firewall from ATP Cloud. See ["Disenroll SRX Series Firewall from ATP Cloud"](#) on page 246 .
- Upgrade a device. See ["Upgrade a Device"](#) on page 247 .
- Export device information as a CSV file that can be opened and edited using an application such as Microsoft Excel. Click **More > Export as CSV**.
- Export the device inventory information as a zipped file. Click **More > Export Inventory**.
- Create a group of devices. See ["Create a Device Group"](#) on page 229 .
- Create a preprovision profile to deploy on devices. See ["Create a Preprovision Profile"](#) on page 231 .
- Enable security logging for a device or device cluster. See ["Security Logs Configuration"](#) on page 248 .
- Subscribe your devices to multiple subscriptions. See ["Manage Device Subscriptions"](#) on page 228 .
- View the device inventory information. Select a device, and click **More > View Inventory**. The device inventory page opens displaying the device discovery. See [Table 100 on page 217](#) .
- Add feature licenses for a device. See ["Add a License to a Device"](#) on page 233
- Import local certificates and CA certificates into your devices. See ["Import a Device Certificate"](#) on page 235
- Show or hide columns about a device. Click the Show/Hide columns icon in the top-right corner of the page and select the columns to view on the page.
- Filter information based on select criteria. You can add filters, save the filters, and set any of the filters as default. To add a filter:

1. Click the filter icon on the top-right corner of the page, and select **Add Filter** to open the Add Criteria page.
2. Set the filter conditions, and click **Add**.

The filter is saved and applied on the data. You can save the filter. You can also mark one filter as the default filter.

To remove the filter, click the filter icon, and select **Hide Filter**.

Field Descriptions - Devices Page

[Table 91 on page 204](#) describes the fields on the Devices page.

Table 91: Fields on the Devices Page

Fields	Description
Host Name	Displays the name of the device.
Device Group	Displays the group name if a device is associated a group.

Table 91: Fields on the Devices Page (Continued)

Fields	Description
Inventory Status	<p>After a device is added, it is discovered and synchronized to ensure that the device configurations are in sync with Juniper Security Director Cloud.</p> <p>The Inventory Status column displays the discovery and synchronization status of the device with Juniper Security Director Cloud.</p> <ul style="list-style-type: none"> • Discovery Not Initiated—The device is added to the device list but it is not added completely. To complete adding the device, click Adopt Device, and follow the instructions in "Add Devices or Device Clusters Using Commands" on page 224 . • Discovery Failed—There was an error during the device discovery process or while adding the device to Juniper Security Director Cloud. To view the reason for the failure, hover over the Discovery Failed status. To troubleshoot the issue, see Frequently Asked Questions. • Unknown—The device status is unknown if the device is either not connected to Juniper Security Director Cloud or is down. • In Sync—The settings in the device and Juniper Security Director Cloud are synchronized. • Out of Sync—The settings in the device were updated and not synchronized with Juniper Security Director Cloud. • Sync in Progress—The device is being synchronized to Juniper Security Director Cloud after the device is added, upgraded, or a setting was updated.

Table 91: Fields on the Devices Page (Continued)

Fields	Description
Device Config Status	<p>Indicates when there are differences between the configurations in a device and the configurations in the Junos Detailed Configuration tab for the device in Juniper Security Director Cloud.</p> <p>Click Resolve to view the steps to accept or reject the differences and synchronize the configurations.</p> <p>For more information, see "Resolve Out-of-Band Changes" on page 238 .</p>
Management Status	<p>Displays the connectivity status of the device with Juniper Security Director Cloud. You can manage the device from Juniper Security Director Cloud when the Up status is displayed.</p> <ul style="list-style-type: none"> • Up—The device is connected to Juniper Security Director Cloud. • Down—The device is not connected to Juniper Security Director Cloud.
Device Health Status	<p>Displays the resources used by the device, such as CPU processing power, memory, and storage.</p> <p>The health status is displayed only for devices with subscriptions. The status of the device is color-coded.</p> <ul style="list-style-type: none"> • Green indicates a healthy device with resource usage below 50%. • Orange indicates warnings with resource usage reaching 50% to 80%. • Red indicates errors and heavy resource usage above 80%.

Table 91: Fields on the Devices Page (Continued)

Fields	Description
Subscriptions	<p>Displays the subscriptions to which the device is subscribed.</p> <ul style="list-style-type: none"> • Displays Trial Subscription if you have subscribed the device to the trial subscription. • Displays No Subscription if you have not yet subscribed the device to any subscriptions.
OS Version	<p>Displays the OS firmware version running on the device</p> <p>This field displays Unknown for devices that Juniper Security Director Cloud doesn't manage.</p>
Product Series	<p>Displays the model number of the device.</p> <p>For devices that Juniper Security Director Cloud doesn't manage, the product details are discovered through SNMP. If the product details cannot be discovered, the field displays Unknown.</p>

Field Descriptions - Device Details Pane

[Table 92 on page 207](#) describes the fields on the Device Details pane.

Table 92: Fields on the Device Details Pane

Fields	Description
Basic Information	
Host Name	Displays the name of the device.

Table 92: Fields on the Device Details Pane (Continued)

Fields	Description
OS Version	<p>Displays the OS firmware version running on the device.</p> <p>This field displays Unknown for devices that Juniper Security Director Cloud doesn't manage.</p>
Family	<p>Displays the device family of the selected device.</p> <p>For devices that Juniper Security Director Cloud doesn't manage, the family is the same as the provided vendor name. The field displays Unknown if the vendor name is not available and if SNMP is not used or has failed.</p>
Platform	<p>Displays the model number of the device.</p> <p>For devices that Juniper Security Director Cloud doesn't manage, the platform details are discovered through SNMP. If the platform details cannot be discovered, the field displays Unknown.</p>
Serial Number	<p>The serial number of the device chassis.</p> <p>This field displays Unknown for devices that Juniper Security Director Cloud doesn't manage.</p>
Status Information	

Table 92: Fields on the Device Details Pane (Continued)

Fields	Description
Management Status	<p>Displays the connection status of the device in Juniper Security Director Cloud.</p> <ul style="list-style-type: none"> • Up—The device is connected to Juniper Security Director Cloud. • Down—The device is not connected to Juniper Security Director Cloud. • Discovery Failed—There was an error during device discovery or adding to Juniper Security Director Cloud. You can see the reason for the failure when you hover your mouse cursor over the Discovery Failed status.
Configuration Status	<p>Displays the current state of the device configuration.</p> <ul style="list-style-type: none"> • Unknown—The device status is unknown to Juniper Security Director Cloud. The device is either not connected to Juniper Security Director Cloud or is down. • In Sync—The device is connected to Juniper Security Director Cloud. • Out of Sync—The device is not connected to Juniper Security Director Cloud. • Sync in Progress—The device is being resynchronized to Juniper Security Director Cloud after the device is added or upgraded.

Field Descriptions - Device Inventory Page > Overview Tab

Table 93 on page 210 describes the fields on the Overview tab in the Device Inventory page.

Table 93: Fields on the Overview Tab

Field	Description
Chassis	Displays the port usage and health status of the hardware devices.
System Information	Displays the following details of the devices: <ul style="list-style-type: none"> • Model name • Host name • Serial number—This field displays Unknown for devices that Juniper Security Director Cloud doesn't manage. • Software version—This field displays Unknown for devices that Juniper Security Director Cloud doesn't manage. • System time • System up time • Active users
Subscriptions	Displays the subscriptions attached to the device and the status of the subscriptions.
Rules	Displays the number of rules configured for the device along with the number of used and unused rules.
Memory	Displays the storage resources used by the device.
Security Packages	Displays the name of the installed security packages.
CPU	Displays the CPU processing power used by the device.
Licenses	Displays the number of times an item is licensed.

Table 93: Fields on the Overview Tab (Continued)

Field	Description
Chassis	Displays the port usage and health status of the hardware devices.

Field Descriptions - Device Inventory Page > Chassis Tab

[Table 94 on page 211](#) describes the fields on the Chassis tab in the Device Inventory page.

Table 94: Fields on the Chassis Tab

Field	Description
Model	Displays the model of the selected module.
Serial number	Displays the serial number of the selected module.
Module	Displays the module of the device.
Type	Displays the type of the device.
Model	Displays the model of the device.
Version	Displays the version of the device software.
Part Number	Displays the part number of the device.
Serial Number	Displays the serial number of the device.

Table 94: Fields on the Chassis Tab *(Continued)*

Field	Description
Physical Interfaces	<p>Displays standard information about physical interfaces connected to the device in the type-/fpc/pic/port format where type indicates the media type that identifies the network device. For example, ge-0/0/6.</p> <p>Click View to go to the Interfaces tab.</p>
Description	<p>Displays an optional description for this interface configured on the device.</p> <p>The description can be a text string that contains up to 512 characters. Longer strings are truncated to 512 characters. If there is no information, the column is empty.</p>

Field Descriptions - Device Inventory Page > Interfaces Tab

Table 95 on page 212 describes the fields in the Interfaces tab.

Table 95: Fields on the Interfaces Tab

Field	Description
Interface Name	Displays the interface that is used to connect to Juniper Security Director Cloud.
IPv4 Address	<p>Displays the IPv4 address assigned to the logical interface.</p> <p>If you do not add a logical interface to a physical interface, this column will be blank.</p>

Table 95: Fields on the Interfaces Tab (Continued)

Field	Description
IPv6 Address	<p>Displays the IPv6 address assigned to the logical interface.</p> <p>The IPv6 address is displayed only if the device has an IPv6 address. If you do not add a logical interface to a physical interface, this column will be blank.</p>
IfIndex	Displays the unique identifying number associated with a physical or logical interface.
Admin Status	Displays the administrative status of the physical interface, which can be Up or Down .
Operational Status	Displays the link status of the interface, which can be Up or Down .
VLAN ID	<p>Displays the VLAN ID assigned to the logical interface.</p> <p>If you do not add a logical interface to a physical interface, this column will be blank.</p>
MTU	Displays the maximum transmission unit (MTU) size on the physical interface.
Speed	Displays the speed (Mbps) at which the interface is running.
Duplex Mode	<p>Displays the connection characteristic.</p> <ul style="list-style-type: none"> • Automatic-If the connection mode is negotiated. • Full-Duplex-If the connection is full duplex. • Half-Duplex-If the connection is half duplex.
Link Type	Displays the link level type of the physical interface.

Table 95: Fields on the Interfaces Tab *(Continued)*

Field	Description
Linecard	Displays the number of interface slots.

Field Descriptions - Device Inventory Page > Device Administration Tab

Table 96 on page 214 describes the fields on the Licenses tab.

Table 96: Fields on the Licenses Tab

Field	Description
Name	Displays the name of the license associated with the device.
Status	<p>Displays the status of the license, which can be:</p> <ul style="list-style-type: none"> • Active: When the license validity is less than 30 days, the status also indicates the number of days left until expiry. • Expired <p>Only valid licenses are included in the license count calculation.</p>
Expiry Date	Displays the expiry date of the licensed feature.
Total Licenses	Displays the total licenses available for the feature.
Used Licenses	Displays the total licenses used for the feature.
Required Licenses	Displays the total licenses required for the feature.
Install License	<p>The option to add licenses to the device.</p> <p>See "Add a License to a Device" on page 233 .</p>

Table 97 on page 215 describes the fields on the Certificates tab.

Table 97: Fields on the Certificates Tab

Field	Description
Certificate ID	Displays the unique identification of the certificate.
Issuer Organization	Displays the details of the organization that issued the certificate.
Status	<p>Displays the expiration status of the certificate:</p> <ul style="list-style-type: none"> • If you set the certificate to be renewed automatically, the status displayed depends on the renewal period selected from the Edit Certificate Settings page. For example, if you select the renewal period as 1 month, the Status field displays Less than 1 month before expiry. • If you set the certificate to be manually renewed, the status displayed depends on the expiration notification time for the certificate. For example, Less than 2 weeks before expiry. • If the expiration date of the certificate does not meet the expiration notification time yet, the Status field displays –. • If the certificate has expired, the Status field displays Expired.
Expiry Date	Displays the date and time when the certificate expires.
Encryption Type	<p>Displays the type of the certificate:</p> <ul style="list-style-type: none"> • Root certificate • Trusted certificate

Table 97: Fields on the Certificates Tab (Continued)

Field	Description
Import	The option to import certificates into the device. See "Import a Device Certificate" on page 235 .
Generate Default Trusted CAs	The option to generate default trusted CA profiles. See "Import a Device Certificate" on page 235 .

[Table 98 on page 216](#) describes the fields on the Software tab.

Table 98: Fields on the Software Tab

Field	Description
Software Name	Displays the name of the installed software package.
State Type	State Type
Software Description	Displays the description of the software package.
Version	Displays the version number of the installed software package.

[Table 99 on page 216](#) describes the fields on the Security Packages tab.

Table 99: Fields on the Security Packages Tab

Field	Description
Version	Displays the currently installed security package version.
License	Displays the number of licenses associated with the security package. Click the link to see the details of the licenses.

Table 99: Fields on the Security Packages Tab *(Continued)*

Field	Description
Name	Displays the name of the currently installed security package.

Field Descriptions - Device Inventory Page > Configuration Template Tab

Table 100 on page 217 describes the fields on the Configuration Template tab on the Device Inventory page.

Table 100: Fields on the Configuration Template Tab

Field	Description
Name	Displays the name of the configuration template.
Deployment Status	Displays the deployment status of the configuration template, which can be No configuration , Ready to deploy , or Deployed .
Last Deployed	Displays the date when the configuration template was deployed.
Description	Displays the description of the configuration template.
Validation	<p>Displays the status of the configuration templates validation job, which can be Success, Failed, or Inprogress.</p> <p>This field is temporarily populated when you click Validate on the Configuration Template page.</p>



Field Descriptions - Device Inventory Page > Junos Detailed Configurations Tab

The **Junos Detailed Configuration** tab enables you to configure Junos OS for an SRX Series Firewall. You can configure interfaces, general routing information, routing protocols, user access, and system hardware properties.

The left pane lists the Junos OS components. The **Quick Links to Sections** in the right pane provides links to sections in a particular component. You can click the required link to navigate directly to the corresponding section.

[Table 101 on page 218](#) describes the icons, Call To Action (CTA) buttons, and different statuses displayed on the **Junos Detailed Configuration** tab.

Table 101: Icons, CTA Buttons, and Statuses on Junos Detailed Configuration Tab

Icon, CTA Buttons, or Status Displayed	Description
Deploy successful	Displayed when all the configuration(s) are deployed successfully on the device.
Deployment in progress	Displayed when the configuration(s) deployment is in-progress.
Deploy pending	Displayed when configuration(s) are pending deployment.
Last deployed	Displays the number of hours or days since the last deployment and the email address of the user who deployed the configuration(s).
Preview	Click to preview the configuration(s) that are pending deployment on the device.
Deploy	Click to deploy the configuration(s) on the device. When you click Deploy , the options to modify the configurations are disabled.
	Use to search and navigate to a specific component, section, or parameter.
	Displayed if a Junos component has configuration(s) that are pending deployment.
Restore To Last Deployed State	Click to restore the configured parameter, section, or component to its earlier state.

[Table 102 on page 219](#) describes the Junos OS components that you can configure from the **Junos Detailed Configuration** tab.

Table 102: Junos OS Components

Component	Description
Access	Use this section to configure essential user access and authentication features. Essential user access features include login classes, user accounts, access privilege levels, and user authentication methods. For more information, see the User Access and Authentication Administration Guide for Junos OS .
Accounting Options	Use this section to configure collection interval, file to contain accounting data, specific fields and counter names on which statistics must be collected. For more information, see the Network Management and Monitoring Guide .
Bridge Domains	Use this section to configure Layer 2 bridging on your SRX Series Firewall. For more information, see the Layer 2 Bridging, Address Learning, and Forwarding User Guide .
Class of Service	Use this section to configure class of service (CoS) to define service levels that provide different delay, jitter, and packet loss characteristics to applications served by specific traffic flows. Applying CoS features to each device in your network ensures quality of service (QoS) for traffic throughout your entire network. For more information, see the Class of Service User Guide (Security Devices) .
Dynamic Profiles	Use this section to create dynamic profiles to use with DHCP or PPP client access. For more information, see the Broadband Subscriber Sessions User Guide .
Firewall	Use this section to configure firewall filters and policers. For more information, see the Routing Policies, Firewall Filters, and Traffic Policers User Guide .
Forwarding Options	Use this section to configure traffic forwarding options. For more information, see the Broadband Subscriber Management Wholesale User Guide .

Table 102: Junos OS Components (Continued)

Component	Description
Interfaces	Use this section to provide information about interfaces, interfaces set, and interface range used on the device. For more information, see the Interfaces User Guide for Security Devices .
Junos ES Root configuration	Use this section to configure JSRC to interact with an SAE in an SRC environment to authorize and provision subscribers. For more information, see the Broadband Subscriber Sessions User Guide .
Multi-Chassis	Use this section to configure consistency check parameters for a multichassis link aggregation group.
PoE	Use this section to configure PoE interfaces, FPC configurations, and corresponding notifications. For more information, see the Interfaces User Guide for Security Devices .
Policy Options	Use this section to configure routing policies. For more information, see the Routing Policies, Firewall Filters, And Traffic Policers User Guide .
Protocols	Use this section to configure the protocols for a routing instance.
Routing Instances	Use this section to configure IPv4 and IPv6 routing protocols and settings. For more information, see the Routing Protocols Overview .

Table 102: Junos OS Components (Continued)

Component	Description
Security	<p>Use this section to configure the following:</p> <ul style="list-style-type: none"> • Security policies • Security zones • Security screens • Cloud • Internet Key Exchange (IKE) configurations • Application Layer Gateway (ALG) • Security logging
Services	<p>Use this section to configure the router or switch settings to connect to the local router or switch. For more information, see the Broadband Subscriber Sessions User Guide.</p>
Session Limit Group	<p>Use this section to configure the maximum allowed number of concurrent web management sessions. For more information, see the Flow-Based and Packet-Based Processing User Guide for Security Devices.</p>
SMTP	<p>Use this section to configure SMTP server settings for the SRX Series Firewall.</p>
SNMP	<p>Use this section to configure SNMP implementation in Junos OS.</p>
Switch Options	<p>Use this section to configure Layer 2 learning and forwarding properties for a VLAN or a virtual switch. For more information, see the Ethernet Switching User Guide.</p>
System	<p>Use this section to configure and monitor system log messages. For more information, see the Network Management and Monitoring Guide.</p>

Table 102: Junos OS Components *(Continued)*

Component	Description
VLANs	Use this section to configure the VLAN properties on the device. For more information, see the Ethernet Switching User Guide .
VMHost	Use this section to configure VM host management properties. For more information, see the Junos OS Software Installation and Upgrade Guide .
WLAN	Use this section to configure WLAN properties on the device. For more information, see the Interfaces User Guide for Security Devices .

RELATED DOCUMENTATION

[Add Devices to Juniper Security Director Cloud | 222](#)

[Manage Device Subscriptions | 228](#)

[About the Subscriptions Page | 1009](#)

[Delete Devices From Juniper Security Director Cloud | 233](#)

[Manage Configuration Versions | 239](#)

[Reboot a Device | 244](#)

[Resynchronize a Device with Juniper Security Director Cloud | 237](#)

[Upgrade a Device | 247](#)

[Create a Device Group | 229](#)

[Create a Preprovision Profile | 231](#)

Add Devices to Juniper Security Director Cloud

IN THIS SECTION

● [Before You Begin | 223](#)

- Add Devices to Juniper Security Director Cloud | 224
- Add Devices or Device Clusters Using Commands | 224
- Add Devices Using Zero Touch Provisioning | 225
- Add Device by Scanning QR Code | 227

Before You Begin

- Make sure that each of the SRX Series Firewall ports can communicate with an FQDN of Juniper Security Director Cloud . The FQDN of each home region is different.

[Table 103 on page 223](#) contains the region-wise mapping details of the SRX Series Firewall ports and the Juniper Security Director Cloud FQDNs.

Table 103: Home Region to FQDN Mapping

Region	Purpose	Port	FQDN
North Virginia	ZTP	443	jsec2-virginia.juniperclouds.net
	Outbound SSH	7804	srx.sdcloud.juniperclouds.net
	Syslog TLS	6514	srx.sdcloud.juniperclouds.net
Ohio	ZTP	443	jsec2-ohio.juniperclouds.net
	Outbound SSH	7804	srx.jsec2-ohio.juniperclouds.net
	Syslog TLS	6514	srx.jsec2-ohio.juniperclouds.net

- Use TCP port 53 and UDP port 53 to connect to Google DNS servers (IP addresses—8.8.8.8 and 8.8.4.4). The Google DNS servers are specified as the default servers in the factory settings of the

SRX Series Firewalls. You must use these default DNS servers when you use ZTP to onboard the firewalls. You can use private DNS servers when you use other methods to onboard the firewalls. Note that you must make sure that the private DNS servers can resolve the Juniper Security Director Cloud FQDNs.

Add Devices to Juniper Security Director Cloud

You can add devices to Juniper Security Director Cloud and manage your network security for these devices. There are multiple ways to add devices to Juniper Security Director Cloud. Choose the method that's right for you:

- **Add Devices Using Commands** - Juniper Security Director Cloud generates commands for adding a device or device cluster. You can copy the commands and paste them into the device console. When you commit the commands to the device, Juniper Security Director Cloud discovers and adds the device or device cluster to the cloud. See ["Add Devices or Device Clusters Using Commands" on page 224](#) for details.
- **Add Devices With Zero Touch Provisioning** - With Zero Touch Provisioning (ZTP) you can configure and provision devices automatically. See ["Add Devices Using Zero Touch Provisioning" on page 225](#) for details.
- **Add Devices Using J-Web** - See [Add an SRX Series Firewall to Juniper Security Director Cloud](#) in the J-Web User Guide for SRX Series Firewalls for details.
- **Add Devices from Security Director** - See [Add Devices to Security Director Cloud](#) in the Security Director User Guide for details.
- **Add Devices by scanning QR code** - Juniper Security Director Cloud allows you to onboard the cloud-ready SRX firewalls by scanning the device QR code. See ["Add Device by Scanning QR Code" on page 227](#) .

Add Devices or Device Clusters Using Commands

Juniper Security Director Cloud generates commands for adding a device or a device cluster. You can copy and paste the commands into the device console. When you commit the commands to the device, Juniper Security Director Cloud discovers and adds the device or the device cluster to the cloud.

1. Select **SRX > Device Management > Devices**.

The Device page opens.

2. Click **+** icon.

The Add Devices page opens.

3. Click **Adopt SRX Devices**.

4. Select one of the following options:

- **Devices** to add individual devices.

- **Clusters** to add device clusters.

5. Enter the number of devices or device clusters to add to Juniper Security Director Cloud in the **Number of SRX devices to be adopted** field, and click **OK**.

You can add a maximum of 50 devices or device clusters at one time.

A message confirming that the new device or device cluster is added is displayed. The Devices page opens with the newly added device or device cluster listed in the table.

NOTE: At this point, Juniper Security Director Cloud has not yet completely added the device or device cluster, so the Connection Status displays **Discovery Not Initiated**.

6. On the Devices page, in the Connection Status column for the new device, click one of the following options:

- **Adopt Device** to add a device.
- **Adopt Cluster** to add a device cluster.

The Adopt Devices page opens with the commands that you need to commit to the device.

7. Copy the commands and paste it to your device edit prompt, and press **Enter** to run the commands.

If you are adding a device cluster, paste these commands to the CLI of the primary device of the cluster.

8. Type **Commit**, and press **Enter** to commit the changes to the device.

You can view the status of the process, by going to the **Administration > Jobs** page.

When you commit the commands to the device, the device discovery process starts in Juniper Security Director Cloud. You can refresh the Devices page and see the status Discovery in progress in the Connection Status column.

When Juniper Security Director Cloud discovers and adds a device or a device cluster, the Connection Status changes to **Up**. If the process fails, the Connection Status changes to **Discovery failed**.

Hover your mouse cursor over the **Discovery failed** message to see the reason for the failure.

Add Devices Using Zero Touch Provisioning

You can configure and provision devices automatically using Zero Touch Provisioning (ZTP). ZTP reduces the manual intervention for adding devices to a network. See the following table for ZTP supported devices by Juniper Security Director Cloud.

Table 104: ZTP Supported Devices

ZTP Supported Device	Supported Junos OS Release
SRX300, SRX320, SRX340, SRX345, and SRX550 HM SRX Series Firewalls	Junos OS Release 18.4R3 and later
SRX380	Junos OS Release 20.1R1 and later
SRX1500	Junos OS Release 20.2R1 and later
SRX1600, SRX2300	Junos OS Release 23.4R1 and later

NOTE: To add other devices models, configure the basic device settings and connectivity, and add the device using ["Add Devices or Device Clusters Using Commands"](#) on page 224 .

Power on the devices to add to Juniper Security Director Cloud.

1. Select **SRX >Device Management > Devices.**

The Devices page opens.

2. Click **Add Devices.**

The Add Devices page opens.

3. To manually enter the device details, click **Register SRX Devices for ZTP, and do the following:**

a. Enter the serial number of the device.

b. Set a root password for the device.

The password must contain at least six characters and can consist of alphanumeric and special characters without spaces.

c. To add multiple devices, click **+** and enter the device details.

d. To add multiple devices and use the same root password for all devices, select **Use this password for all devices** for Device 1.

e. Click **OK**.

4. To upload device information as a CSV file, click **Register Devices for ZTP > Upload CSV File, and do the following:**

a. Click **Download sample CSV file** to download the sample CSV file.

- b. Open the CSV file, add the serial number and root password of the devices that you want to add, and save the changes.
- c. Browse for the CSV file and click **OK**.

The CSV file must be in a specific format for the devices to be added. Use the sample CSV file to enter the device details in the correct format and upload the file.

The devices are added to Juniper Security Director Cloud. You can view the devices at **Device Management > Devices**.

Add Device by Scanning QR Code

You can add cloud-ready SRX Series Firewalls to Juniper Security Director Cloud by scanning the QR code available on the firewall. Your SRX Series Firewall is cloud-ready if it has a QR claim code on the front or the back panel.

Before you begin, ensure the following:

- The firewall is powered on.
 - The firewall is not already added in an organization. You can add a firewall in only one organization.
1. Scan the QR code on the SRX Series Firewall using a mobile device that is connected to the Internet.
 2. Click the displayed link to go to the Juniper Security Director Cloud login page.
 3. Enter your account email address and password and click **Login**.
If you do not have an account, go to <https://sdcloud.juniperclouds.net> on a different device, create an account, and then retry.
 4. Select the organization to add the firewall.
 5. Enter the root password for the firewall with a minimum of six characters without spaces and click **Add Device**.

The firewall is added to Juniper Security Director Cloud and the device discovery is automatically initiated. You can log in to the portal and manage the firewall after the discovery is complete.

NOTE: After you log in, the session is valid for 60 minutes. During this time, you can add multiple firewalls without entering the account email address and password.

SEE ALSO

[About the Devices Page | 202](#)

[Manage Device Subscriptions | 228](#)

[Subscriptions Overview | 1007](#)

[Delete Devices From Juniper Security Director Cloud | 233](#)

[Manage Configuration Versions | 239](#)

[Reboot a Device | 244](#)

[Resynchronize a Device with Juniper Security Director Cloud | 237](#)

[Upgrade a Device | 247](#)

Manage Device Subscriptions

IN THIS SECTION

- [Device Subscriptions Overview | 228](#)
- [Associate Your Devices with Subscriptions | 228](#)

Device Subscriptions Overview

Device subscriptions are used to manage devices in Juniper Security Director Cloud. To manage devices using Juniper Security Director Cloud, you must purchase the device subscription for the required number of devices, add the subscription in Juniper Security Director Cloud, and then associate your devices to the device subscriptions.

For more details about:

- Subscriptions, see [Datasheet](#). To purchase device subscriptions, contact your sales representative or account manager.
- Adding subscriptions to Juniper Security Director Cloud, see ["Add a Subscription" on page 1011](#) .

Associate Your Devices with Subscriptions

Before associating your devices with subscriptions, ensure that:

- You have valid device subscriptions. Contact your sales representative or account manager to purchase device subscriptions.
- You added the purchased device subscriptions in Juniper Security Director Cloud. See ["Add a Subscription" on page 1011](#) .

1. Select **SRX > Device Management > Devices**.

NOTE: For devices that are not associated with subscriptions, the **Subscriptions** column displays **No subscription**.

The Devices page opens

2. Select the devices, and click **Manage Subscriptions**.

You can select maximum 50 devices to manage subscriptions of multiple devices simultaneously. The selected devices must belong to the same product series and have the same subscription type. You can find the subscription type on the **Administration > Subscription** page.

The Manage Subscriptions page opens.

3. Choose the device subscriptions from the **Subscription** dropdown list.

The Subscription dropdown list is a dynamic list that contains generic subscriptions and subscriptions that are compatible with the selected devices along with trial subscriptions.

After associating your devices with subscription, you cannot remove the subscriptions. You can transfer the subscriptions to another device. Device subscriptions are freed up when you delete the devices from the Devices page.

4. Click **OK**.

The devices are associated with the device subscriptions.

You can view the details of the device subscriptions on the **SRX > Device Management > Devices** page.

Create a Device Group

You can group devices logically to deploy and to manage configurations on the devices.

You can group only devices with the Discovery Not Initiated as the Management Status.

1. Click **SRX > Device Management > Devices**.

The Devices page opens.

2. Click the **Device Groups** tab.

3. Click **+**.

The Create Device Group page opens.

4. Configure the following fields:

- **Name**—Enter a unique name for the device group containing maximum 63 characters without spaces. The name must begin with an alphanumeric character and can also contain special characters such as colons, hyphens, forward slashes, periods, and underscores.

- **Description**—Enter a description for the device group containing maximum 900 alphanumeric characters. The description can also contain special characters except ampersand, lesser than sign, greater than sign, or an empty line.
- **Devices**—Select the devices in the left table and click > to move to the right table and assign them to the device group.

5. Click **OK**.

Juniper Security Director Cloud creates a group of the selected devices lists the group on the Device Groups tab of the Devices page.

RELATED DOCUMENTATION

| [Create a Preprovision Profile](#) | 231

Edit a Device Group

1. Click **SRX > Device Management > Devices**.

The Devices page opens.

2. Click the **Device Groups** tab.

3. Click the edit (pencil) icon.

The Edit Device Group page opens.

4. Edit the following fields:

- **Name**—Enter a unique name for the device group containing maximum 63 characters without spaces. The name must begin with an alphanumeric character and can also contain special characters such as colons, hyphens, forward slashes, periods, and underscores.
- **Description**—Enter a description for the device group containing maximum 900 alphanumeric characters. The description can also contain special characters except ampersand, lesser than sign, greater than sign, or an empty line.
- **Devices**—Select the devices in the left table and click > to move to the right table and assign them to the device group.

5. Click **OK**.

Juniper Security Director Cloud updates the device group and lists the updated group on the Device Groups tab of the Devices page.

RELATED DOCUMENTATION

| [Create a Device Group](#) | 229

Create a Preprovision Profile

Preprovision profiles contain a predefined set of policies that Juniper Security Director Cloud deploys on devices while onboarding.

After you adopt a physical device, Juniper Security Director Cloud triggers the discovery process and deploys minimal configuration to the device and changes the status of the device to In Sync. Then Juniper Security Director Cloud verifies if a preprovision profile is mapped to the device and deploys the corresponding policies on the device.

You can select only devices with Discovery Not Initiated as the Management Status to include in the preprovisioned profile.

1. Click **SRX > Device Management > Devices**.
The Devices page opens.
2. Click the **Preprovision Profiles** tab.
3. Click **Preprovision Devices**.
The Preprovision Devices page opens.
4. Enter a unique name for the preprovision profile with a maximum of 29 characters in **Preprovision profile name**.
5. In the **Devices** tab, select the devices and device groups to include in the preprovisioned profile.
6. Click the **Configuration Templates** tab.
7. Select the configuration templates to deploy on the devices and device groups.
8. Optional: Click **Configure Parameters** to configure the template.
The Configure Parameters page opens.
9. Configure the following types configuration template parameters:
 - Global
 - Device-level

The parameters of the configuration template are dynamic and depend on the selected template. See "[Add a Configuration Template](#)" on page 255 for an explanation of the parameters.
10. Click the **SRX Policies** tab.
11. Select the SRX policies to deploy on the devices.
12. Click **OK**.

Juniper Security Director Cloud creates a preprovision profile to deploy on the devices and device groups during onboarding. It lists the preprovision profiles in the Preprovision Profiles tab of the Devices page.

Hover your cursor over the numbers depicting the number of objects configured in the profile to view the objects.

RELATED DOCUMENTATION

[Edit a Preprovision Profile | 232](#)

[Create a Device Group | 229](#)

[Add a Configuration Template | 255](#)

Edit a Preprovision Profile

1. Click **SRX > Device Management > Devices**.

The Devices page opens.

2. Click the **Preprovision Profiles** tab.

3. Click **Preprovision Devices**.

The Preprovision Devices page opens.

4. Edit the following settings:

- **Preprovision profile name**—Enter a unique name for the preprovision profile with a maximum of 29 characters in **Preprovision profile name**.
- **Devices** tab—Select the devices and device groups to include in the preprovisioned profile.
- **Configuration Templates** tab—Select the configuration templates to deploy on the devices and device groups.
- **Configure Parameters** in the Configuration Templates tab—Configure the global and device-level parameters of the configuration template.
- **SRX Policies** tab—Select the SRX policies to deploy on the devices.

5. Click **OK**.

Juniper Security Director Cloud updates the preprovision profile and lists the preprovision profile in the Preprovision Profiles tab of the Devices page.

RELATED DOCUMENTATION

[Create a Preprovision Profile](#) | 231

Delete Devices From Juniper Security Director Cloud

If you do not want Juniper Security Director Cloud to manage a device anymore, you must remove or delete the device from Juniper Security Director Cloud.

1. Select **SRX > Device Management > Devices**.

The Devices page opens

2. Select the devices to remove, and click the delete icon on the top-right corner of the page.

If provisioning services, such as firewall policies or configuration templates, are associated with the device that you want to delete, select the **Force delete** option. If the device you want to delete is provisioned, and you do not select the **Force delete** option, the device will not be deleted.

The Delete Devices page opens asking for confirmation of the delete operation. The Delete Devices page also contains information about the topology where the devices are configured along with a warning that the VPN configurations for the device too will be deleted.

If the configurations of some devices could not be deleted, Juniper Security Director Cloud displays a message identifying the devices to manually delete the configuration using CLI.

3. Click **Yes** to delete the device.

The device is deleted from Juniper Security Director Cloud.

As part of this process, the initial configuration on the device to enable the device and Juniper Security Director Cloud to communicate with each other is deleted.

Add a License to a Device

Add a license for a software feature to a device or a device cluster. Each license is associated with a feature, such as IPS, content security, and is valid for only one device. You can add a license to a device either by uploading a license file or by copying and pasting the license key.

1. Select **SRX > Device Management > Devices**.

The Devices page opens.

2. Select the device or the device cluster, and click **More >View Inventory** to view the inventory.
3. Click **Device Administration** tab, and click **Licenses**.
4. Click **Install License**.

The Add License page opens.

5. Complete the configuration of the license according to the guidelines provided in [Table 105 on page 234](#).

Table 105: Fields on the Add License Page

Field	Description
Options	<ul style="list-style-type: none"> • Select Copy and paste license to copy the license key from the license file and paste it in the License text box. <p>NOTE: You must not edit the key.</p> <ul style="list-style-type: none"> • Select Upload license to browse and upload a license file in the .txt format.
License	<p>If you selected Copy and paste license, copy the license information and paste into this text box.</p> <p>You will have received the license information in an e-mail when you purchased the license.</p> <p>For a device cluster, you will see options to copy and to paste license information for each device in the cluster. You can provide different licenses for different devices in a device cluster.</p>
License file	<p>If you selected Upload license, browse and upload the license file.</p> <p>For a device cluster, you will see options to browse for license files for each device in the cluster. You can upload different license files for different devices in a device cluster.</p>

6. Click **OK**.

The feature license is added to the device or the device cluster.

RELATED DOCUMENTATION

| [About the Devices Page](#) | 202

Import a Device Certificate

Import local certificates and CA certificates from your computer into the managed device to authenticate 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.

1. Select SRX > Device Management > Devices.

The Devices page opens.

2. Select the device or the device cluster, and click More >View Inventory.

3. Click Device Administration > Certificates.

4. Click one of the following:

- **Import** in the Local Certificates section to open the Import Certificate page.
- **Import** in the CA Certificates section to open the Import CA Certificate page.

Click **Generate Default Trusted CAs** if you need to generate default trusted CA profiles.

5. Complete the configuration of the certificate according to the guidelines provided in [Table 106 on page 235](#).

Table 106: Fields on Import Certificate Page

Field	Description
Certificate ID	<p>Enter a unique value for the certificate ID for an externally generated certificate.</p> <p>The certificate ID is used to create a key pair along with the algorithm to associate with the key.</p>
Upload Certificate	<p>The option to navigate to and upload the certificate.</p> <p>Click Browse to navigate to the location of the certificate. Juniper Security Director Cloud supports only the PEM format for local certificates.</p>

Table 106: Fields on Import Certificate Page (Continued)

Field	Description
Upload Private Key	The option to navigate to and upload the private key. Click Browse to navigate to the location of the private key. Juniper Security Director Cloud supports only the PEM format for private keys.
Passphrase	Enter the passphrase used to protect the private key or key pair of the certificate file.

Table 107: Fields on the Import CA Certificate Page

Field	Description
CA Profile ID	Enter a unique value for the CA profile ID for an externally generated certificate. The CA profile ID is used to create a key pair along with the algorithm to associate with the key.
Upload certificate	The option to navigate to and upload the certificate. Click Browse to navigate to the location of the certificate. Juniper Security Director Cloud supports only the CER format for CA certificates.

6. Click **OK**.

If the certificate content is validated successfully, the certificate is imported.

After importing a certificate, you can use the certificate when you create an SSL proxy profile and for IPsec VPN peers authentication.

RELATED DOCUMENTATION

| [About the Devices Page](#) | 202

Resynchronize a Device with Juniper Security Director Cloud

When you resynchronize a managed device, the configuration changes made on the device and the inventory resources, such as certificates and licenses, are synchronized with the Juniper Security Director Cloud database.

For example, when a managed device is updated by a device administrator using the CLI or the GUI of the device and you trigger a manual resynchronization, the device configuration on the physical device is synchronized with the Juniper Security Director Cloud database.

1. Select **SRX > Device Management > Devices**.

The Devices page opens.

2. Select the device to resynchronize, and click **More > Resynchronize with Network**.

A job is created for the resynchronization process and the details are displayed on the top of the page. Click **Administration > Jobs** to view the job.

When the job completes successfully, the device resynchronization is complete.

RELATED DOCUMENTATION

[About the Devices Page | 202](#)

[Add Devices to Juniper Security Director Cloud | 222](#)

[Subscriptions Overview | 1007](#)

[Manage Device Subscriptions | 228](#)

[Delete Devices From Juniper Security Director Cloud | 233](#)

[Manage Configuration Versions | 239](#)

[Reboot a Device | 244](#)

[Upgrade a Device | 247](#)

Out-of-Band Changes Overview

Out-of-band changes are the changes that you make to a device configuration using any method other than using Juniper Security Director Cloud UI. Out-of-band changes include configuration changes that you make by using the device commands. If you add or change a device configuration using Junos command, then these configuration changes do not match with the configuration stored in Juniper Security Director Cloud.

You must resolve the out-of-band change conflicts by accepting or rejecting the out-of-band device changes in the Juniper Security Director Cloud. For example, if you add a zone to a device using Junos command, the device's configuration stored in Juniper Security Director Cloud does not match with the device configuration. As a result, you will not see the newly added zone information on Juniper Security Director Cloud. You must accept the out-of-band zone configuration in Juniper Security Director Cloud to use the zone for creating or editing security policy, NAT, or VPN.

When you make out-of-band device configuration changes, the Juniper Security Director Cloud changes the device configuration state to **Out of Sync** and displays a notification for device configuration change. You can view a list of all **Out of Sync** devices on the **SRX > Device Management > Devices** page. To return the device configuration state to **In Sync**, you must resolve the conflicts by accepting or rejecting the out-of-band changes. This task (accepting or rejecting the out-of-band device changes) synchronizes the device's configuration stored in Juniper Security Director Cloud to match the device configuration.

Resolve Out-of-Band Changes

You can resolve the out-of-band changes by accepting or rejecting the configuration changes.

To resolve out-of-band changes:

1. Select **SRX > Device Management > Devices**.

For the out-of-band changes, the **Device Config Status** field shows that the device configuration is changed.

2. Select the device and click **Resolve**.

The page for resolving the conflicts shows the following information:

- **SD Cloud Config Changes**—Changes that you have added using Juniper Security Director Cloud UI.
- **Device Config Changes**—Changes that you have added to the device using commands.

3. Resolve the out-of-band changes by taking the appropriate action as described in the table.

Table 108: Resolve out-of-band changes

Action	Description
Reject the out-of-band changes.	<p>a. Click Reject Device Config Changes to delete the device configurations that are added via device commands or any other way apart from Juniper Security Director Cloud UI.</p> <p>A confirmation message is displayed. You can preview the out-of-band device configuration changes using the Preview link in the confirmation message.</p> <p>b. Click Yes to confirm.</p> <p>A notification message with job details is displayed.</p> <p>On the Device page, the Device Config Status field is cleared and it indicates that there are no more out-of-band device configuration changes to resolve.</p> <p>The rejected out-of-band device changes are rolled back.</p>
Accept the out-of-band changes.	<p>a. Click Accept Device Config Changes to add the out-of-band device changes to Juniper Security Director Cloud. A confirmation message to accept the out-of-band device configuration changes is displayed.</p> <p>NOTE: Accepting the out-of-band device changes will discard any changes shown in the SD Cloud Config Changes with the changes shown in Device Config Changes in the resolve conflict page.</p> <p>b. Click Yes to accept the out-of-band device changes to Juniper Security Director Cloud.</p> <p>On the Device page the Device Config Status field is cleared and it indicates that there are no more out-of-band device configuration changes to resolve.</p>

Manage Configuration Versions

IN THIS SECTION

- [View Configuration Versions | 240](#)
- [Edit Configuration Version Description | 241](#)
- [Pin a Configuration Version | 241](#)

- [Rollback to a Configuration Version | 242](#)
- [Compare Configuration Versions | 243](#)

Configuration files in Juniper Security Director Cloud are created when the device configuration data from managed devices are backed up to the Juniper Security Director Cloud database for the first time.

A separate configuration file is created in the database for each managed device. Each time the configuration of a device changes, a new version of the configuration file is created on the device, which can then be backed up to the Juniper Security Director Cloud database or to a remote server at a fixed time or at a set recurrence interval periodically.

Centralized configuration file management enables you to maintain multiple versions of your device configuration files in Juniper Security Director Cloud. This helps you recover device configuration files in case of a system failure and maintain consistent configuration across multiple devices.

NOTE: When you change the configuration of a device using Juniper Security Director Cloud, the portal processes this configuration change in a similar manner to a scenario where you would change the configuration without using Juniper Security Director Cloud.

In both such scenarios, the device becomes out of sync with Juniper Security Director Cloud's security policies. Juniper Security Director Cloud overwrites such device configurations with the original configuration when it deploys the security policies again. Use the configuration preview option to view the configuration changes.

You must resynchronize out-of-sync devices with Juniper Security Director Cloud. See ["Resynchronize a Device with Juniper Security Director Cloud" on page 237](#).

The following sections describe how you can pin important configuration versions, edit a configuration version description, roll back to a particular configuration version, or compare two configuration versions.

View Configuration Versions

You can view information about all configuration versions of a device that are backed up in the Juniper Security Director Cloud database.

1. Select **SRX > Device Management > Devices**.

The Devices page opens.

2. Select the device or device cluster to view the configuration versions, and click **More > Configuration Versions**.

The Configuration Versions page opens displaying the previous ten configuration versions for the selected device or device cluster in the Version History pane. The page displays the following information:

- **Version Number**—The version number of the configuration file. The files listed in order of the most recent to the oldest versions.
- **Name**—The name of the configuration versions. This is the device serial number with the .conf file extension.
- **Creation Date**—The date and time the different versions of the configuration are created in the Juniper Security Director Cloud database. Version 1 corresponds to the time when you back up a device configuration for the first time from the device.

By default, Juniper Security Director Cloud stores the previous ten configuration versions.

3. Select any configuration file to see a preview of the file in the Preview pane on the right side of the page.

Edit Configuration Version Description


You can edit the description of each configuration version to make them intuitive to understand when you want to pin or rollback to a particular configuration version.

1. Select **SRX > Device Management > Devices**.

The Devices page opens.

2. Select the device or the device cluster to view the configuration files, and click **More > Configuration Versions**.

The Configuration Versions page opens displaying the previous ten versions of the configuration files for the selected device or the device cluster in the Version History pane.

3. Select the configuration version to edit the description, and click  on the top right of the page. The Add Description page opens.

4. Update the description as required, and click **OK**.

The updated description of the configuration version is displayed in the Configuration Versions.

Pin a Configuration Version

By default, Juniper Security Director Cloud, stores the previous ten configuration versions of a device or a device cluster. If the number of backed up configuration versions exceeds ten, the oldest configuration version is deleted and the latest version is stored.

Juniper Security Director Cloud allows you to pin certain configuration versions as important. These versions can be either golden versions without errors or configurations for specific requirements. Pinned configuration versions are never deleted even when new configuration versions are created. You can pin a maximum of three configuration versions as important.

If you have already pinned three configuration versions and pin a fourth configuration version, the first pinned configuration version is deleted. For example, if you pinned Version 1, Version 2, and Version 3 in succession, and if you pin Version 4, the pinned Version 1 is deleted.

1. Select **SRX > Device Management > Devices**.

The Devices page opens.

2. Select the device or device cluster to view the configuration files, and click **More >Configuration Versions**.

The Configuration Versions page opens displaying the previous ten versions of the configuration files for the selected device or the device cluster in the Version History pane.

3. Select the configuration version to pin, and click the pin icon on the top right of the page.

The pin symbol is displayed against the configuration version indicating that the version is pinned.

Rollback to a Configuration Version

The Rollback option enables you to deploy any version of the saved configurations to the device.

Restoring a configuration version involves overriding the device's running configuration file with the selected version of the configuration backup file from Juniper Security Director Cloud.

NOTE: When you rollback the configuration version of a device using Juniper Security Director Cloud, the portal processes this configuration change in a similar manner to a scenario where you would rollback the configuration without using Juniper Security Director Cloud.

In both such scenarios, the device becomes out of sync with Juniper Security Director Cloud's security policies. Juniper Security Director Cloud overwrites such device configurations with the original configuration when it deploys the security policies again. Use the configuration preview option to view the configuration changes.

You must resynchronize out-of-sync devices with Juniper Security Director Cloud. See ["Resynchronize a Device with Juniper Security Director Cloud" on page 237](#).

1. Select **SRX > Device Management > Devices**.

The Devices page opens.

2. Select the device or device cluster to rollback the configuration files, and click **More >Configuration Versions**.

The Configuration Versions page opens displaying the previous ten versions of the configuration files for the selected device or the device cluster in the Version History pane.

3. Select the configuration version to rollback to, and click **Rollback**.

The Rollback Operation pop-up opens asking you for confirmation to continue the rollback operation.

4. Click **Yes**.

A job is created for the rollback operation and the details are displayed on the top of the page. Click **Administration > Jobs** to view the job.

Once the job completes the device configuration rollback is complete. The configuration resources of the device are resynchronized and the device is ready for use.

Compare Configuration Versions

Juniper Security Director Cloud enables you to compare two device configuration versions by using the Compare option.

You can view the device configuration versions side by side to compare and see the total number of differences, the date and time of the last commit operation, and the number of changes made.

NOTE: When you compare versions, each configuration parameter in one version is set side by side with the same parameter in the other version. Therefore, you might see multiple pages of configuration for a single parameter in one version, whereas the same parameter in the other version might be only a few lines long.

1. Select **SRX > Device Management > Devices**.

The Devices page opens.

2. Select the device or device cluster to compare configuration versions, and click **More > Configuration Versions**.

The Configuration Versions page opens displaying the previous ten versions of the configuration files for the selected device or the device cluster in the Version History pane.

3. Select the configuration versions to compare to, and click **Compare**.

The Comparison page opens displaying the delta between the two versions. [Table 109 on page 243](#) describes what the color-coded text indicates.



Table 109: Comparison Page Legend

Text Color	Description
Black text	Indicates content that is common to both files
Green text	Indicates content in the source file on the left that is not contained in the target file on the right

Table 109: Comparison Page Legend (Continued)

Text Color	Description
Blue text	Indicates content in the target file on the right that is not contained in the source file on the left
Pink text	Indicates content that is changed.

The status bar shows the current page number and the total number of pages, along with navigation controls to move from page to page and to refresh the display.

- To locate differences in configuration, click  to view the previous difference or  to view the next difference.

SEE ALSO

[About the Devices Page | 202](#)

[Add Devices to Juniper Security Director Cloud | 222](#)

[Manage Device Subscriptions | 228](#)

[Subscriptions Overview | 1007](#)

[Delete Devices From Juniper Security Director Cloud | 233](#)

[Resynchronize a Device with Juniper Security Director Cloud | 237](#)

[Reboot a Device | 244](#)

[Upgrade a Device | 247](#)

Reboot a Device

The Reboot option is useful in scenarios where you need to reboot a device during a software upgrade.

- You can only reboot devices for which the connection status is up.
 - In a device cluster, you can reboot the primary and secondary devices independently.
- Select **SRX > Device Management > Devices**.
The Devices page opens.
 - Select the device or device cluster to reboot, and click **More > Reboot Device**.

A job is created for the reboot process and the details are displayed on the top of the page. Click **Administration** > **Jobs** to view the job.

When the job completes successfully, the device reboot is complete.

If some of the devices fail to reboot, you can use the **Retry on Failed Devices** action to retry rebooting the devices that failed to reboot.

RELATED DOCUMENTATION

[Add Devices to Juniper Security Director Cloud | 222](#)

[Manage Device Subscriptions | 228](#)

[Subscriptions Overview | 1007](#)

[Delete Devices From Juniper Security Director Cloud | 233](#)

[Manage Configuration Versions | 239](#)

[Resynchronize a Device with Juniper Security Director Cloud | 237](#)

[Upgrade a Device | 247](#)

Enroll SRX Series Firewalls from ATP Cloud to Juniper Security Director Cloud

You can enroll the existing SRX Series Firewalls (available in ATP Cloud) to Juniper Security Director Cloud. After the enrollment, you can use the Juniper Security Director Cloud to access ATP Cloud related screens for the SRX Series Firewalls.

Before You Begin

Before enrolling your SRX Series Firewall, you must map your security realm from ATP Cloud to Juniper Security Director Cloud. For more information, see [Map an Existing ATP Realm to Juniper Security Director Cloud](#).

About the Task

Using the **Enroll to ATP** menu, you can obtain commands to enroll your SRX Series Firewall (from ATP Cloud) to Juniper Security Director Cloud. The enrollment commands perform basic configuration tasks such as:

- Download and install the certificate authorities (CAs) onto your SRX Series Firewall.
- Create local certificates and enroll the certificates with the cloud server.
- Establish a secure connection to the cloud server.

To enroll your SRX Series Firewall from ATP Cloud to Juniper Security Director Cloud:

1. Select **SRX > Device Management > Devices**.

The Devices page opens.

2. Select the device or device cluster and click **More > Enroll to ATP**.

The page with enrollment commands is displayed.

3. Based on the Junos OS version on your device, copy the relevant command to your clipboard and click **OK**.

4. Log on to your SRX Series Firewall and paste the command into the Junos OS CLI (operational mode).

NOTE:

- The command is valid for 7 days.
- Running the enrollment command will overwrite the existing enrollments for your device.

5. Press **Enter**.

NOTE: If the operation fails, dis-enroll the device and then re-enroll it.

A message about successful device enrollment is displayed on your device.

RELATED DOCUMENTATION

| [Disenroll SRX Series Firewall from ATP Cloud | 246](#)

Disenroll SRX Series Firewall from ATP Cloud

You can use the **Disenroll from ATP** option in Juniper Security Director Cloud to remove an SRX Series Firewall from ATP Cloud. You need not log in to ATP Cloud to remove the enrolled SRX Series Firewall.

1. Select **SRX > Device Management > Devices**.

The Devices page opens.

2. Select the device or device cluster and click **More >Disenroll from ATP**.

The page displays the disenrollment commands.

3. Based on the Junos OS version on your device, copy the relevant command to your clipboard and click **OK**.

4. Log on to your SRX Series Firewall and paste the command into the Junos OS CLI (operational mode).

NOTE:

- The command is valid for 7 days.
- Running the `disenroll` command will commit any uncommitted configuration changes. It will also cause any previously generated `disenroll` commands to stop working.

5. Press **Enter**.

A message about successful device disenrollment is displayed on your SRX Series Firewall.

RELATED DOCUMENTATION

| [Enroll SRX Series Firewalls from ATP Cloud to Juniper Security Director Cloud](#) | 245

Upgrade a Device

A device image is a software installation package that enables you to upgrade to or downgrade from one software release to another.

Juniper Security Director Cloud facilitates the management of device images by enabling you to upload device images from your local file system and deploy the image on a device or multiple devices of the same device family simultaneously.


You can download device images from <https://www.juniper.net/customers/support/>.

1. Select **SRX > Device Management > Devices**.

The Devices page opens.

2. Select the device or device cluster to upgrade, and click **More > Upgrade Devices**.

The Upgrade Devices page opens displaying the platform and current software version deployed on the device or device cluster.

3. Select the device or device cluster to upgrade, and click  on the top-right corner of the Select devices table.

To upgrade multiple devices of same device model or a different device model that supports common image, select the devices to upgrade, and click **Bulk Select Image**.

4. Select the image to upgrade the device or device cluster to in the **Selected Image** column.

5. Click  to proceed with the upgrade.

6. Click one of the following options:

- **Run Now** to immediately trigger the upgrade on the device or device cluster.
- **Schedule Later** to upgrade the device later and specify a date and time to for the upgrade.

7. Click **OK**.

A job is created for the upgrade process and the details are displayed on the top of the page. Click **Administration > Jobs** to view the progress of the job.

While the device is being upgraded, the device goes into maintenance mode and you cannot perform any operations on the device. After the device is upgraded and connects back to Juniper Security Director Cloud, the device is rebooted, the device inventory is resynchronized, and the device is available for all operations.

RELATED DOCUMENTATION

[About the Devices Page | 202](#)

[Add Devices to Juniper Security Director Cloud | 222](#)

[Subscriptions Overview | 1007](#)

[Manage Device Subscriptions | 228](#)

[Delete Devices From Juniper Security Director Cloud | 233](#)

[Manage Configuration Versions | 239](#)

[Reboot a Device | 244](#)

[Resynchronize a Device with Juniper Security Director Cloud | 237](#)

Security Logs Configuration

After the device is discovered by the Juniper Security Director Cloud, the device is automatically configured to stream the security logs to Juniper Security Director Cloud.

NOTE: By default, Juniper Security Director Cloud configures the security logs for the devices. The security logs are not configured for the following conditions:

- Device is using a management interface fxp0 as the source interface. Only the revenue ports are allowed for source interface configuration of security logging.
- During device discovery, if the CA certificate or the local certificate deploy fails, then it will result in non-configuration of security logs.


To configure the security logs:

1. Select **SRX > Device Management > Devices**.


The Devices page opens.

2. Click **Security Logs Configuration**.

The Security Logs Configuration page opens displaying all the devices.

3. Select the device or device cluster to configure security logging, and click  on the top-right of the page.

4. Enable **Security Log Status** for the device or device cluster.

5. Select the source interface from the drop down list, and click .

A message appears asking you to confirm security logging configuration for the rest of the devices.

6. Click one of the following options:

- **Yes** to go ahead with the process.
- **No** to stop the process and configure security logging for other devices or device clusters of your choice.

If you click **Yes**, the job is created to push the syslog configuration to the device or device cluster.

When the job completes, security logging is configured for the device or device cluster.

RELATED DOCUMENTATION

| [About the Devices Page](#) | 202

Device Management-Configuration Templates

IN THIS CHAPTER

- [Configuration Templates Overview | 250](#)
- [Configuration Templates Workflow | 252](#)
- [About the Configuration Templates Page | 252](#)
- [Add a Configuration Template | 255](#)
- [Preview and Render a Configuration Template | 261](#)
- [Deploy a Configuration Template on to a Device | 262](#)
- [Edit, Clone, and Delete a Configuration Template | 263](#)

Configuration Templates Overview

IN THIS SECTION

- [Benefits | 252](#)

Juniper Security Director Cloud provides configuration templates to provision configurations, both during onboarding and throughout the device life cycle, for Juniper Networks and other third-party devices. By using configuration templates, you can deploy customized configurations on devices.

You can use a configuration template in following ways:

- **Globally**—You can define the configuration (for example, SNMP Configuration) to be applied to all the devices managed by Juniper Security Director Cloud.
- **Device-specific**—You can define a configuration that is specific to a device; for example, BGP configuration.

By default, Juniper Security Director Cloud provides some predefined configuration templates. See [Table 110 on page 251](#) for the list of the predefined configuration templates. You can also create your own templates by cloning an existing template and modifying its settings. Templates can be added by administrators or users with privilege to add configuration templates.

[Table 110 on page 251](#) lists the predefined configuration templates.

Table 110: Predefined Configuration Templates

Name	Description
AE_DEVICE_COUNT	Configure the aggregated Ethernet interfaces on a device.
BANNER	Configure the banner that appears when you log in to a device.
DNS	Configure Domain Name System (DNS) server settings on a device.
DOMAIN_NAME	Configure the domain name on a device.
HOSTNAME	Configure the host name on a device.
LLDP	Enable and configure Link Layer Discovery Protocol (LLDP) on all interfaces of a device.
LOCAL_USER	Configure a local user on a device.
NETCONF	Configure NETCONF on a device.
NTP	Configure Network Time Protocol (NTP) settings on a device.
SNMP	Configure basic SNMP version 2 (SNMPv2) parameters on a device.
SSH	Configure SSH parameters on a device.
SYSLOG	Configure system log settings on a device.
DHCP	Configure DHCP Pool and DHCP Server Group parameters on a device.

You can deploy the configuration template directly on a device. See ["Deploy a Configuration Template on to a Device" on page 262](#) .

Benefits

Configuration templates provide a mechanism to create customized configurations and push the configurations to one or more devices. This helps you to deploy configurations beyond the standard configuration templates provided in Juniper Security Director Cloud.

Configuration Templates Workflow

The high-level workflow for configuration templates is as follows:

1. Use a pre-existing template (skip to step 2) or create a template using one of the following methods:
 - Clone an existing configuration template and modify the cloned template. See ["Edit, Clone, and Delete a Configuration Template" on page 263](#) .
 - Add a configuration template by specifying the template configuration and logic. See ["Add a Configuration Template" on page 255](#) .
2. (Optional) Preview and validate the configuration template before deploying the configuration template directly on a device. See ["Preview and Render a Configuration Template" on page 261](#) .
3. Deploy a configuration template directly on one or more devices that were previously activated, which enables you to deploy templates that were added after a device was activated or to deploy additional configuration to devices. You can deploy configuration templates to devices from the Configuration Templates See ["Deploy a Configuration Template on to a Device" on page 262](#) .

About the Configuration Templates Page

IN THIS SECTION

- [Tasks You Can Perform | 253](#)
- [Field Descriptions | 254](#)

To access this page, click **SRX > Device Management > Configuration Templates** in the left navigation menu.

Tasks You Can Perform

You can perform the following tasks from this page:

- View details of a configuration template. Select a configuration template and click **More > Detail** or hover over the configuration template and click the detailed view icon. The details of *<Template-Name>* pane appears on the right side of the page displaying the configuration template details.
- Add a configuration template. See ["Add a Configuration Template" on page 255](#)
- Preview a configuration template. See ["Preview and Render a Configuration Template" on page 261](#)
- Deploy a configuration template on one or more devices. See ["Deploy a Configuration Template on to a Device" on page 262](#)
- Clone, edit, or delete a configuration template. See ["Edit, Clone, and Delete a Configuration Template" on page 263](#)
- Filter Entries—Filter the table entries by adding new filtering criteria.

Hover over the **Filter** (funnel) icon and select **Add Filter**. On the **Add Criteria** page, select the filtering criteria from the **Field** and **Condition** list, and enter the text to be compared in the **Value** field. Click **Add**.

The filtered table entries are listed and the filter criteria name is displayed above the table column names.

You can click the cross (X) icon (next to the filter name) to remove the filtering criteria.

NOTE:

- You can add multiple filtering criteria. Once you add the multiple filtering criteria, you can select the **And** condition to display the entries matching all the filtering criteria or select the **Or** condition to display the entries matching any one of the filtering criteria.
- Quick filter: Save the filtering criteria as quick filters. Once you have added all the filtering criteria, you can save a particular criteria or multiple criteria for future use by clicking **Save**.

On the **Save Filter** window, enter a name for the filter, optionally toggle the **Set as Default** button if you want to use this filtering criteria by default, and click **OK**.

The saved filters are displayed under **Quick Filters** when you hover over the Filter (funnel) icon. You can then apply these saved filters to the table entries.

- **Show/Hide Columns**—Choose to show or hide a specific column in the table.
Hover over the **More Options** (vertical ellipsis) > **Show/Hide Columns** and select the *Column-Name* check box of the columns you want to display in the table.
- **Reset Preference**—Reset the displayed columns to the default set of columns for each tab in the table.
Hover over the **More Options** (vertical ellipsis) and select **Reset Preference**.
- **Sort Entries**—Click the column name to highlight the up and down arrows next to the column name. Sort the table entries in ascending or descending order of that column by clicking the up or down arrow respectively.

Field Descriptions

[Table 111 on page 254](#) displays the fields on the Configuration Templates page.

Table 111: Fields on the Configuration Templates Page

Field	Description
Name	The name of the configuration template.
Format	The format in which the configuration template is defined—CLI or XML.
Family	The device family for which the configuration template is applicable: <ul style="list-style-type: none"> • Juniper-SRX
Description	A description of the configuration template.
Last Updated	The date and time when the configuration template was last updated, in the Month DD, YYYY HH:MM:SS format.
Created by	The user who created the configuration template. <i>System</i> indicates that the template is a predefined template.

Add a Configuration Template

To add a configuration template, you should either be a user with administrative privileges or have the privilege to add configuration templates.

NOTE:

- Before you add the configuration template, ensure that you have the device configuration ready.
- We recommend that you use a working device configuration to add the configuration template.

To add a configuration template:

1. Select **SRX > Device Management > Configuration Templates** on the left navigation menu.

The Configuration Templates page appears.

2. Click the **Add** icon (+).

The Add Configuration Template page (wizard) appears.

NOTE: Fields marked with an asterisk (*) are mandatory.

3. Configure the fields on the Basic Information tab according to the guidelines provided in [Table 112 on page 256](#).

4. Click **Next** to go to the Template Configuration tab.

5. Add the configuration on the Template Configuration tab.

You can view a sample configuration by clicking the **Sample Configuration** link.

You can do the following in the editor provided for entering the configuration:

- Copy the required configuration stanza from a device and create a template from parameters in the configuration.
 - Refer to the sample configuration file for adding the configuration.
 - Parameterize variables by using double curly braces `{{}}`.
6. Click **Next** to go to the Generated UI tab, where you can view the UI for the parameters that you entered.
 7. Perform one or more actions on the Generated UI tab, as explained in [Table 113 on page 256](#).
 8. Click **Save**.

The configuration template is added and you are returned to the Configuration Templates page, where a confirmation message appears.

[Table 112 on page 256](#) lists fields to be entered on the Basic Information tab of the Add Configuration Templates page.

Table 112: Fields on the Basic Information Tab of the Add Configuration Templates Page

Field	Description
Template Name	Enter a unique name for the configuration template. The name can only contain alphanumeric characters and hyphens; 64-characters maximum.
Description	Enter a description for the configuration template; 255-characters maximum..
Configuration Format	Select the output format for the configuration template: <ul style="list-style-type: none"> • CLI (default) • XML
Device Family	Juniper-SRX

[Table 113 on page 256](#) lists the actions that you can perform on the Generated UI tab of the Add Configuration Templates page.

Table 113: Generated UI Actions

Action	Description
Reorder the UI	Drag and drop individual fields, grids, or sections to change the order in which the parameters appear on the UI.

Table 113: Generated UI Actions (Continued)

Action	Description
Modify the settings for a field, section, or grid	<p>To modify the settings for a field, section, or grid:</p> <ol style="list-style-type: none"> 1. Click the Settings (gear) icon next to the field, section, or grid. <p>The Form Settings pane appears on the right side of the page, displaying the Basic Settings and Advanced Settings tabs.</p> <ol style="list-style-type: none"> 2. Modify the fields on these tabs, as needed. See Table 114 on page 258 for an explanation of the fields on these tabs. 3. Click Save Settings for each field to save your changes. <p>The modifications that you made are displayed on the UI.</p>
Reset the generated UI	<p>Click Undo all Edits to discard the changes that you made and undo the changes made on the UI.</p>
Preview configuration	<p>Preview the configuration defined in the configuration template.</p> <p>To preview a configuration template:</p> <ol style="list-style-type: none"> 1. Click Preview Configuration. <p>The Preview Configuration page appears, displaying the configuration that was rendered based on the values that you entered.</p> <ol style="list-style-type: none"> 2. Check if the configuration is rendered correctly. <ul style="list-style-type: none"> • If the configuration is not rendered correctly, click the close (X) icon to go back and make modifications as needed. • If the configuration is rendered correctly, click OK. <p>You are returned to the Generated UI page.</p>

[Table 114 on page 258](#) lists the fields on the Form Settings pane.

Table 114: Form Settings

Setting	Guideline
<i>Basic Settings Tab</i>	Fields populated in this tab are based on the input type that you select.
Input Type	<p>Select the input type for the parameter in the configuration template:</p> <ul style="list-style-type: none"> • Text (default): If the input value for the parameter is a string of characters. • Number: If the input value for the parameter is a number. • Email: If the input value for the parameter is an e-mail address. • IPv4: If the input value for the parameter is an IPv4 address. • IPv4 Prefix: If the input value for the parameter is an IPv4 prefix. • IPv6: If the input value for the parameter is an IPv6 address. • IPv6 Prefix: If the input value for the parameter is an IPv6 prefix. • Toggle Button (Boolean): If the input value for the parameter is a boolean value (true or false). • Dropdown: If the input value for the parameter is selected from a list. • Password: If the input value for the parameter is a password. The value that you enter is masked (default). (Optional) Click the Show Password (eye) icon to unmask the password. • Confirm Password: If the input value for the parameter is to confirm the password. If you select this option, a Confirm Password field appears on the UI. The value that you enter is masked (default). (Optional) Click the Show Password (eye) icon to unmask the password.
Label	Enter the label that you want displayed (on the UI) for the parameter.
Default Value	Specify a default value for the parameter.

Table 114: Form Settings (Continued)

Setting	Guideline
Validate	<p>For Text input type, select one or more validation criteria against which the input value will be checked:</p> <ul style="list-style-type: none"> • No Space • Alpha and Numeric • Alpha, Numeric, and Dash • Alpha, Numeric, and Underscore <p>If the value that you entered for the parameter on the UI does not meet the selected validation criteria, an error message appears.</p> <p>NOTE: For greater control of input values, you can use the regular expression option in the Advanced Settings tab.</p>
Description	<p>Enter an explanation for the parameter, which will appear when you hover over the Help (?) icon for the parameter; the maximum length allowed is 256 characters.</p>
Global Scope	<p>Click the toggle button to make the parameter common across all devices to which the configuration template is being deployed. If you disable the toggle button, which is default, the parameter must be specified for each device.</p>
Hidden	<p>Click the toggle button to hide the parameter on the UI when you preview and deploy the template.</p> <p>Typically, this option is used to hide a parameter and display it in the template only when an event is triggered. By default, the toggle button is disabled, which means that the parameter is displayed.</p>
Required	<p>Click the toggle button to make the parameter mandatory; parameters that are mandatory are marked with an asterisk (*) on the UI.</p>
Maximum Value	<p>For parameters that are numbers, enter the maximum value (up to 16 digits) for the input.</p>

Table 114: Form Settings (Continued)

Setting	Guideline
Minimum Value	For parameters that are numbers, enter the minimum value (up to 16 digits) for the input.
Visibility for Disabled	For Boolean parameters, select one or more parameters that must appear on the UI when the toggle button is disabled (boolean value is FALSE).
Visibility for Enabled	For Boolean parameters, select one or more parameters that must appear on the UI when the toggle button is enabled (boolean value is TRUE).
Resource Type	<p>For Dropdown input type, select the type of resource from which you want to retrieve data:</p> <ul style="list-style-type: none"> • Static Resource—Resources in the list on the UI are mapped to the values that you specify. <ul style="list-style-type: none"> • To add a static resource: <ol style="list-style-type: none"> 1. Click the Add (+) icon. Cells appear in the List Values table. 2. Click inside the cells to specify values for the Label (name for the option in the list), Value (value for the option in the list), and Visibility (conditional visibility based on the option selected from the list) fields. 3. Click ✓ (check mark) to save your changes. The values that you specified are displayed in the List Values table. • To edit a static resource, select the resource and click the Edit (pencil) icon. • To delete a static resource, select the resource and click the Delete (X) icon.

Table 114: Form Settings (Continued)

Advanced Settings Tab

Regexp	<p>Enter a regular expression (regex pattern) to validate the input value.</p> <p>A regular expression defines a search pattern that is used to match characters in a string.</p> <p>For example, the regular expression [A-Z] matches the input with the characters A through Z.</p> <p>If the input consists of characters other than A through Z, an error message (as specified in the Invalid Message field) appears.</p>
Invalid Message	<p>Enter an error message that you want displayed on the UI when the input value does not match the specified regular expression.</p>

Event List

Event Name	Select an event from the list based on which the parameter is conditionally displayed.
Event Handler	Enter a JavaScript function that specifies the actions that the event handler takes in response to an event.

Preview and Render a Configuration Template

You must be an administrator or a user with the preview privilege to preview configuration templates.

You can use the Preview workflow to validate a configuration template by entering values for the configuration template and then render the template to view the configuration.

We recommend that you use this workflow to validate a configuration template before deploying it on a device.

To preview and render a configuration template:

1. Select **SRX > Device Management > Configuration Templates**.
The Configuration Templates page appears.
2. Select the configuration template that you want to preview and click **Preview**.
The Template Preview for *Template-Name* page appears.
3. In the CONFIGURE tab, specify values for the parameters as needed.

NOTE: Fields marked with an asterisk (*) are mandatory.

4. After you have entered the necessary parameters, click **PREVIEW**.

The **PREVIEW** tab renders the configuration based on the values that you specified.

5. Check if the configuration was rendered correctly.

If the configuration was not rendered correctly, you can modify the configuration template as needed. See .

6. Click **Close**.

You are returned to the Configuration Templates page. You can deploy the configuration on a device.

Deploy a Configuration Template on to a Device

You can deploy a configuration template directly on one or more devices that were previously activated. This enables you to add configurations to devices after a device was activated or to deploy additional configuration to the device.

To deploy a configuration template on a device, you must either be an administrator or a user with the privilege to deploy configuration on devices.

To deploy a configuration template to one or more devices:

1. Select **SRX > Device Management > Configuration Templates**.

The Configuration Templates page appears.

2. Select the configuration template to deploy and click **Deploy to Devices**.

The list of devices to which the configuration template can be deployed appear in the Configuration Templates page.

3. Do one of the following:

- If you have not set values for the parameters in the configuration template, click **Set Parameters**.

The Template Parameters page appears.

- a. In the Configure tab, set values for the parameters.

- b. Click **Preview** to view and to render the configuration.

If the configuration is fine, click **OK** or change the configuration in the Preview tab if you want to change the configuration.

On clicking **OK**, a message indicating that the configuration is successful appears and you return to the Devices list.

- c. (Optional) Click **Validate** to validate the configuration on the device.

A message indicating that a job is created for the validation appears. You can view the status of the validation from the **Administration > Jobs** page.

4. Click **Deploy**.

The Deploy page appears.

5. Do one of the following:

- Click **Run Now** to deploy the configuration on the selected devices immediately.
- Click **Schedule Later** to deploy the configuration later.

If you choose to deploy the configuration later, you must enter the date (in MM/DD/YYYY format) and time (in HH:MM:SS 24-hour or AM/PM format) that you want the deployment to occur.

6. Click **OK**.

The settings are saved and you are returned to the Configuration Templates page. A confirmation message appears indicating that a job is created. For each device, a separate task is triggered in the job to deploy the configuration. You can view the status of the validation from the **Administration > Jobs** page.

Edit, Clone, and Delete a Configuration Template

IN THIS SECTION

- [Edit a Configuration Template | 263](#)
- [Clone a Configuration Template | 264](#)
- [Delete a Configuration Template | 264](#)

You must be an administrator or a user with edit, clone, and delete privileges for the configuration templates.

Edit a Configuration Template

NOTE: You cannot edit predefined configuration templates.

To edit a Configuration Template:

1. Select **SRX > Device Management > Configuration Templates**.

The Configuration Templates page appears.

2. Select the configuration template that you want to modify and click the **Edit** (pencil) icon.

The Edit Configuration Template page appears. The fields on this page are similar to the fields in the Add Configuration Template workflow.

3. Modify the fields.

See "[Add a Configuration Template](#)" on page 255 for an explanation of the fields.

NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **OK**.

The modifications are saved and a confirmation message is displayed. If the configuration template was previously deployed on a device, then you must redeploy the configuration template for the changes to take effect.

Clone a Configuration Template

To clone a configuration template:

1. Select **SRX > Device Management > Configuration Templates**.

The Configuration Templates page appears.

2. Select the configuration template that you want to clone and click **Clone**.

The Clone Configuration Template page appears.

3. In the **Template Name** field, enter a unique template name. The name can only contain alphanumeric characters and hyphens up to a maximum of 64 characters.

4. Click **OK**.

In the Configuration Templates page, a confirmation message appears at the top of the page indicating the status of the clone operation.

After a template is cloned successfully, you can modify the template if needed. See the preceding section for details.

Delete a Configuration Template

NOTE:

- You cannot delete predefined configuration templates.
- You can delete a configuration template only if the following conditions hold good:
 - You added (created) the template.
 - The template is not deployed on a device.

1. Select SRX > Device Management > Configuration Templates.

The Configuration Templates page appears.

2. Select the configuration template and click the delete icon.

Delete confirmation dialog box opens.

3. Click Yes.

A popup appears indicating whether the deletion was successful or not.

Device Management-Images

IN THIS CHAPTER

- [About the Images Page | 266](#)
- [Image Upgrade Workflow | 268](#)
- [Add an Image | 269](#)
- [Stage an Image | 271](#)
- [Deploy an Image | 272](#)
- [Delete Images | 273](#)

About the Images Page

IN THIS SECTION

- [Tasks You Can Perform | 266](#)
- [Field Descriptions | 267](#)

To access this page, click **SRX > Device Management > Software images**.

A device image is a software installation package used to upgrade or downgrade the operating system running on a network device. Juniper Security Director Cloud helps you to manage (add, stage, deploy, and delete) the entire lifecycle of images of all managed network devices.

Juniper Security Director Cloud can manage the software images running on SRX Series Firewall (both standalone and chassis clusters) and vSRX Virtual Firewall.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add an image. See ["Add an Image" on page 269](#)
- Stage an image. See ["Stage an Image" on page 271](#) .
- Deploy an image. See ["Deploy an Image" on page 272](#) .
- Delete images. See ["Delete Images" on page 273](#) .
- Show or hide columns about a device. Click the Show/Hide columns icon in the top-right corner of the page and select the columns to view on the page.
- Filter information based on select criteria. You can add filters, save the filters, and set any of the filters as default. To add a filter:
 1. Click the filter icon on the top-right corner of the page, and select **Add Filter** to open the Add Criteria page.
 2. Set the filter conditions, and click **Add**.

The filter is saved and the filter is applied on the data. You can save the filter. You can also mark one filter as the default filter.

To remove the filter, click the filter icon, and select **Hide Filter**.
- Sort Entries: Click on a column name to highlight the up and down arrows next to the column name. Sort the table entries in ascending or descending order of the column by clicking the up or down arrow respectively.

Field Descriptions

[Table 115 on page 267](#) displays the fields on the Images page.

Table 115: Fields on the Images Page

Field	Description
Image Name	The name of the software image file.
Version	The version number of the software image. For example, 20.4R1.12

Table 115: Fields on the Images Page (Continued)

Field	Description
Vendor	The vendor of the software image. For example, Juniper Networks.
Family	The device family to which the software image belongs. For example, Juniper-SRX
Supported Platform	The device models on which the software image can be deployed. Only one device model, such as SRX, is listed in this column. A + <Integer> where the integer indicates the number of additional device models supported is displayed next to the device model, such as +2. Click the + <Integer> to view the list of all the other device models on which the image can be deployed.
Size	The size of the software image file in MB or GB.
Uploaded By	The user who uploaded the software image file.

Image Upgrade Workflow

The following is the software image upgrade workflow in Juniper Security Director Cloud:

1. Add a software image in Juniper Security Director Cloud. See ["Add an Image" on page 269](#) .
2. Stage the software image on the device. See ["Stage an Image" on page 271](#) .

Juniper Security Director Cloud validates whether the complete software is copied onto the device by using the checksum of the image. The checksum of the image in Juniper Security Director Cloud is verified with the checksum of the image in the device. If the checksum of the image copied onto the device does not match with the checksum of the device in Juniper Security Director Cloud, the image

copied onto the device is deleted and the image is copied again. If the checksum does not match again, the stage task fails.

3. Deploy the software image. See ["Deploy an Image" on page 272](#).

During the deployment, the following tasks are performed on the device:

- Validation of the image copied onto the device—Juniper Security Director Cloud validates if the complete software is copied onto the device by using the checksum of the image. The checksum of the image in Juniper Security Director Cloud is verified with the checksum of the image in the device. If the checksum of the image copied onto the device does not match with the checksum of the device in Juniper Security Director Cloud, the image copied onto the device is deleted and the image is copied again. If the checksum does not match again, the deploy job fails.
- Upgrade of the image on the device—Juniper Security Director Cloud upgrades devices in the following manner:
 - Single Chassis/Standalone devices—Normal upgrade where the device stops forwarding traffic during the upgrade process.
 - Chassis Clusters (SRX Series Firewalls)—The upgrade or downgrade is possible by using In-Band Cluster Upgrade (ICU) or In-Service Software Upgrade (ISSU). See [Upgrading Devices in a Chassis Cluster Using ICU](#) for details about ICU and [Upgrading a Chassis Cluster Using In-Service Software Upgrade](#) for details about ISSU.
 - vSRX Virtual Firewall Cluster: For vSRX Virtual Firewall clusters, Juniper Security Director Cloud decides whether it has to use ISSU or manually upgrade the cluster nodes.
- Reboot the device—The devices are automatically rebooted after the image is upgraded.

Juniper Security Director Cloud synchronizes with the device after the device connects back.

Add an Image

You can add software images of devices to Juniper Security Director Cloud so that you can manage the lifecycle of the image on the devices. When you need to upgrade or downgrade the image running on a device, you can stage and deploy the required image on the device by using Juniper Security Director Cloud.

NOTE: When you add a software image, only details such as the URL, the checksum details, and the properties are stored on Juniper Security Director Cloud. The actual image is uploaded only when you stage the image. See ["Stage an Image" on page 271](#)

Before you begin, ensure that the device can access the location of the image.

1. Click SRX > Device Management > Software images.

The Images page opens.

2. Click the + icon.

The Add Image page opens.

3. Complete the configuration described in [Fields on the Add Image Page on page 270](#).

4. Click OK.

The image is listed on the Images page.

[Fields on the Add Image Page on page 270](#) lists the fields on the Add Image page.

Table 116: Field on the Add Image Page

Field	Description
Image URL	<p>Enter the URL where the image is located.</p> <p>You can generate the URL on the product-specific Support page of the Juniper Networks website.</p> <p>NOTE: The URL that is generated on the Juniper Networks website is valid for only 15 minutes.</p>
SHA Checksum	<p>Select a valid calculated SHA-1 file checksum from the drop-down list.</p> <p>You can get the relevant checksum from the product-specific Support page of the Juniper Networks website.</p>
Display Name	<p>Enter a name for the images.</p> <p>The name can contain alphanumeric characters and special characters such as underscores and periods.</p>

Table 116: Field on the Add Image Page (*Continued*)

Field	Description
Supported Platform	Select the supported platforms from the drop-down list.
Version	Enter the version of the software image. For example, 15.1R7.9.

Stage an Image

The stage option is useful if you are using a low-bandwidth connection. On low bandwidth connections, manually staging a software image before deploying the image helps prevent the image deployment from timing out because of a slow connection. On high-bandwidth connections, you can choose to stage the image along with the image deployment.

When you stage a software image, the checksum of the image in Juniper Security Director Cloud is verified with the checksum of the image in the device. If the checksum of the image on the device does not match with the checksum in Juniper Security Director Cloud, the image copied on to the device is deleted and the image is copied again.

An administrator or a user with the privileges to add, stage, and deploy software images can stage an image.

NOTE: You must stage or copy a software image onto a device before upgrading the software running on the device.

1. Click **SRX > Device Management > Software images**.

The Images page opens.

2. Select the image, and click **Stage**.

The Stage Image page opens.

You can stage an image onto multiple devices simultaneously.

3. Under **Select Devices**, select one or more devices to stage the image.

4. In the **Stage Image** field, click:

- **Run Now** to stage the image immediately.

- **Schedule Later** to stage the image later, and specify the date and time when to stage the image.

5. Click **OK**.

- If you select **Run Now**, a job is initiated immediately to stage the image.
- If you select **Schedule Later**, a job is initiated at the scheduled date and time to stage the image.

Click **Administration** > **Jobs** to view the job.

Deploy an Image

An administrator or a user with the privileges to add, stage, and deploy software images can deploy images on devices. You can deploy an image on multiple devices simultaneously.

NOTE:

- When you deploy a software image on a device, the device goes into the maintenance state. In the maintenance state:
 - Other actions that impact the device, such as rebooting the device or deploying configuration templates, cannot be performed.
 - Traffic flowing through an SRX Chassis Cluster is not disrupted.
 - Traffic flowing through a standalone device is disrupted.

You can also upgrade images from the Devices page. See ["Upgrade a Device" on page 247](#) .

1. Click **SRX** > **Device Management** > **Software images**.

The Images page opens.

2. Select the device image, and click **Deploy**.

The Deploy Images page opens.

In the Deploy Images page, you can view whether the image is staged on a device. If the image is not staged, the image is copied onto the device and deployed, which increases the deployment time.

3. Under **Select Devices**, select one or more devices to deploy the device image.

4. In the **Deploy Image** field, select a time to run the deployment:

- Click **Run Now** to deploy the image immediately.
- Click **Schedule Later** to deploy the image later, and specify the date and time to deploy the image.

5. Click **OK**.

- If you select **Run Now**, a job is initiated immediately to deploy the image.
- If you select **Schedule Later**, a job is initiated at the scheduled date and time to deploy the image

Click **Administration** > **Jobs** to view the job.

Delete Images

You can delete one or more software images from the Images page when you no longer need to manage the images.

An administrator or a user with the privileges to add, stage, and deploy software images can delete an image. If you delete an image while the image is being staged or deployed, the job initiated to stage or deploy the image fails.

1. Click **SRX** > **Device Management** > **Software images**.

The Images page opens.

2. Select one or more images, and click delete icon.

A confirmation message is displayed.

3. Click **Yes** to delete the images.

The selected images are deleted, and the images are no longer listed on the Images page.

Device Management-Security Packages

IN THIS CHAPTER

- [About the Security Packages Page | 274](#)
- [Install Security Package | 276](#)
- [Enable Automatic Update of Security Package | 277](#)

About the Security Packages Page

IN THIS SECTION

- [Tasks You Can Perform | 274](#)
- [Field Descriptions | 275](#)

To access this page, click **SRX>Device Management>Security Packages**.

Security package consists of IPS Signatures, Application Signatures, and URL Categories.

You can configure your device to install and automatically update the signature at specified intervals.

Tasks You Can Perform

You can perform the following tasks from this page:

- Probe devices to get the latest license details on the devices.

When you add the device for the first time, the device is listed under **Devices and Security package Details** without the license information. To get the license information, you must probe the device. Click **Probe Devices** and click the refresh icon to view the latest license details and the installed security package version on the device.

- Install the latest Security Package on the device. See ["Install Security Package" on page 276](#) for details.
- Enable automatic update of latest security package on the device. See ["Enable Automatic Update of Security Package" on page 277](#)

Field Descriptions

The following table describes the fields for the latest security packages available on Juniper Security Director Cloud.

Table 117: Fields on the Security Packages Page- Latest Security Packages

Fields	Description
Name	Displays the name of the security packages available on the Security Director Cloud.
Version	Displays version for the latest security package available on the Juniper Security Director Cloud.
Published Date	Displays the date when the security package was released.
Detectors	Displays information of the currently installed security package detector version.

The following table describes the fields about the Security Packages currently installed on the devices.

Table 118: Fields on the Security Packages Page-Devices and Security Package Details

Fields	Description
Device Name	Displays the name of the device.
Platform	Displays the model number of the device.
IPS Signature	Displays the IPS signature license details and the installed package version in the device.

Table 118: Fields on the Security Packages Page-Devices and Security Package Details (Continued)

Fields	Description
Application Signature	Displays the Application Signature license details and the installed package version in the device.
URL Category	Displays the URL Category license details and the installed package version in the device.

Install Security Package

Use the **Install Security package** to manually install the latest IPS signature, application signature, or URL category on the devices from Juniper Security Director Cloud.

To install the latest security package on the device:

1. Select **SRX>Device Management>Security Packages**.

The Security Packages page appears.

2. Click **Probe Devices** to get the information about latest license details and security package version installed on the device. Refresh the display information by clicking the refresh icon.

3. From **Latest Security Packages**, select one or more packages listed under and click **Install Security Package**.

The Install security packages page appears.

4. Select the devices to install the packages.

NOTE: IPS Signatures and URL Category packages requires license for installation. Only devices with valid license are listed in the table.

5. From the **Schedule Installation** options, select **Run Now** to install the security package immediately. Select **Schedule at a later time** and specify the date and time at which the security package should be installed.
6. Click **OK**. A job is created. Click the job ID to go to the Jobs page and view the status of the install operation.

RELATED DOCUMENTATION

| [About the Devices Page | 202](#)

Enable Automatic Update of Security Package

You can configure your devices to automatically install and update the security package at specified intervals. For example, you can configure your devices to install the IPS signature on 14th of July at 2:00 a.m and thereafter periodic check and update of the latest IPS signature to happens after every two days.

NOTE: You can enable the automatic update of security package for the devices with management status as **Up** or configuration status as **In Sync**.

To enable automatic update of the latest security package on the device:

1. Select **SRX > Device Management > Security Packages**.
The Security Packages page appears.
2. Click **Auto-update**.
The Enable Auto-Update page appears.
3. Complete the configuration settings according to the guidelines provided in [Table 119 on page 277](#).

Table 119: Fields for the auto-update

Field	Description
Auto-update	Enable automatic update of the latest security package on the devices. By default, auto-update is disabled.
URL	The security package is installed and updated on the devices from the Juniper Networks security website.
Interval	Interval in hours for automatic update after the first installation. For example, if you set the interval to 48 hours, the automatic update for the security package happens after every two days from the first installation date. By default, the interval is 1 hour.

Table 119: Fields for the auto-update *(Continued)*

Field	Description
Start date & time	Start date and time for the first automatic update of the security package.
Devices	Select the devices from the available column and click > to add the devices to list of selected devices for enabling automatic update of the security package.

4. Click **OK**.

A job is created. Click the job ID to go to the Jobs page and view the status of the operation.

RELATED DOCUMENTATION

| [About the Devices Page](#) | 202

SRX Policy

IN THIS CHAPTER

- Security Policy Overview | 280
- About the SRX Policy Page | 282
- Rule Placement Analysis | 284
- About the Security Policy Rules Page | 286
- Add a Security Policy | 290
- Edit and Delete a Security Policy | 293
- Reorder a Security Policy | 295
- Import Security Policies Overview | 296
- Import Security Policies | 298
- About the Manage Policy Versions Page | 299
- Create a Policy Version | 301
- View Policy Version Details | 301
- Compare Policy Versions | 304
- Roll Back a Policy Version | 306
- Delete a Policy Version | 307
- Add a Security Policy Rule | 307
- Edit, Clone, and Delete a Security Policy Rule | 313
- Reorder a Security Policy Rule | 315
- Configure Global Options | 315
- Configure Default Rule Option | 318
- Select a Security Policy Rule Source | 318
- Select a Security Policy Rule Destination | 319
- Select Applications and Services | 321
- Common Operations on a Security Policy Rule | 322
- Deploy Security Policies | 325
- Add SRX Policy Rules to Secure Edge Policy (From SRX Policy Page) | 325

- [Capture IPS Data Packets of Devices | 329](#)

Security Policy Overview

IN THIS SECTION

- [Security Policy and Rule Order Overview | 281](#)

Juniper Security Director Cloud provides the ability to create, modify, and delete security policy and associate the devices with a security policy. Security policies provide security functionality by enforcing rules on traffic that passes through a device. Traffic is permitted or denied based on the action defined in the security policy rules. A security policy rule controls transit traffic within a context that is derived out of the end-points defined in the rule. Rule-based security policies can incorporate both transport layer (Layer 4) and application layer (Layer 7) security constructs in a single rule. The choice of sequence and the assignment happens implicitly based on the endpoints in the rule definition. Security rules consist of source and destination endpoints, IP addresses, user identity, URL categories, services, and applications.

NOTE: If a device (CPE or next-generation security) is running Junos OS Release 18.2R1 or later, a security policy acts as a unified security policy. In a unified security policy, dynamic application can be used as a match condition along with the existing match conditions. Therefore, a separate application security is not configured on the device to allow or block traffic to an application.

A security policy provides the following features:

- Permit, reject, deny, redirect, or tunnel the traffic based on the application in use.
- Identifies not only HTTP but also any application running on top of it, enabling you to properly enforce policies. For example, an application security rule could block HTTP traffic from Facebook but allow Web access to HTTP traffic from Microsoft Outlook.
- Advanced security protection by specifying one or more of the following:
 - Intrusion prevention system (IPS) profile
 - Content security profile

- SSL proxy profile

Rules are categorized as zone-based rules and global rules.

- Zone-based-rules are the rules with zones as source and destination endpoints. The parameters that you can define for zone-based rules are listed in [Table 120 on page 281](#).
- Global rules gives the flexibility to perform action on the traffic without any zone restrictions. [Table 120 on page 281](#) lists the parameters for global rules.

Table 120: Parameters for Zone-based and Global rules

Sources	Destinations	Applications/ Services	Action	Advanced Security Options	Supported Options
Zone	Zone	Applications	Permit	IPS Profile	Schedules
Addresses	Addresses	Services	Deny	Content Security Profile	Logging
Identity	URL Categories		Reject	SSL Proxy Profile	Rule Options
			Redirect		
			Tunnel		

Security Policy and Rule Order Overview

Security policies and rules execute in the order of their appearance. You must be aware of the following:

- Security policies and the rules within a security policy are applied from top to bottom. For example, a security policy **P1** has two rules *Rule-a* and *Rule-b*. Security policy **P2** has two rules *Rule-a* and *Rule-b*. The security policy **P1** has sequence number **1** and the security policy **P2** has sequence number **2**. After deploying, the security policies and rules are applied in the following sequence:
 1. **P1** *Rule-a*
 2. **P1** *Rule-b*
 3. **P2** *Rule-a*
 4. **P2** *Rule-b*
- Newly created security policies and rules go to the end of the list.
- You can change the order of security policies and rules. See ["Reorder a Security Policy" on page 295](#) and ["Reorder a Security Policy Rule" on page 315](#) for details.

- The last security policy in the policy list is the default policy, which has the default action of denying all traffic.
- A security policy rule can mask another security policy rule.

About the SRX Policy Page

IN THIS SECTION

- [Tasks You Can Perform](#) | 282
- [Field Descriptions](#) | 282

To access this page, select **SRX>Security Policy>SRX Policy**.

Use the SRX Policy page to view and manage security policies associated with SRX Series Firewalls.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a security policy. See ["Add a Security Policy" on page 290](#) .
- Edit or delete a security policy. See ["Edit and Delete a Security Policy" on page 293](#) .
- Add a rule to security policy. See ["Add a Security Policy Rule" on page 307](#) .
- Import a security policy. See ["Import Security Policies" on page 298](#) .
- Deploy a security policy. See ["Deploy Security Policies" on page 325](#) .
- Search for a security policy. Click the Search icon in the top right corner of the page to search for a security policy.

You can enter partial text or full text of the keyword in the text box and press Enter.

The search results are displayed on the same page.

Field Descriptions

[Table 121 on page 283](#) provides guidelines on using the fields on the Policy List page.

Table 121: Fields on the Policy List Page

Field	Description
Seq.	Order number for the policy.
Name	Name of the security policy.
Rules	Number of rules associated with the policy. If no rule is associated with the policy Add Rule link is displayed. For more information, see "Add a Security Policy Rule" on page 307
Devices	Number of devices associated with the policy.
Status	Displays the deployment status of the security policy. <ul style="list-style-type: none"> • Deploy Successful • Deploy Pending • Deploy Failed • Deploy scheduled • Deploy in progress • Redeploy required
Modified By	The user who modified the policy.
Last Modified	The date and time when the policy was modified.
Description	Description of the security policy.

Rule Placement Analysis

Over a period of time, security policy rules can become inefficient as rules become disorganized, causing some rules to become ineffective. This primarily occurs because of a lack of timely notification to end users when new rules are added that can adversely affect the other rules in the rule base.

Juniper Security Director Cloud addresses this problem by analyzing the rule placement and suggesting the correct rule placement to avoid the anomalies in the rules for a given policy.

NOTE:

- You can enable the rule placement analysis when you create a security policy or edit an existing security policy.
- Rule placement analysis suggestion is available only for newly created rules in a security policy.

Rule placement analysis identifies the security policy rules that contain the following issues:

- **Shadowing**—Occurs when a rule higher in the order of the rule base matches with all the packets of a rule lower in the order of the rule base.
- **Redundancy**—Occurs when two or more rules that perform the same action on the same packets along with the same settings or configurations.

The following list shows the rule placement analysis behavior for different types of security policy rules:

- **Exact match**—If a newly created rule has identical values with an existing rules for **Sources**, **Destination**, **Application/Services**, and **Action** fields, then the new rule should be placed after an existing rule.
- **Exact match with different action**—If a newly created rule is identical with an existing rules for **Sources**, **Destination**, **Application/Services** fields, with different **Action**, then the new rule should be placed before the existing rule.
- **New Rule is a subset of existing rule**—If a newly created rule is a subset of an existing rule, then the new rule should be placed before an existing rule.
- **New Rule is a super set of existing rule**—If a newly created rule is a super set of an existing rule, then the new rule should be placed after the existing rule.
- **Partial match**—If a newly created rule is partially matching an existing rule, then the newly created rule should be placed above an existing rule.

- **No match or no overlap**—If a newly created rule that has no overlap with the existing rules, then the newly created rule should be placed at the top of the existing rules.

The following table shows few examples of rule placement analysis for different types of rules:

Table 122: Examples of Rule Placement Analysis

Condition	Rule 1 (Existing)	Rule 2 (New)	Suggested Rule Placement
Exact match	<ul style="list-style-type: none"> • Source: Any • Destination: Any • Application: App1 • Action: Permit 	<ul style="list-style-type: none"> • Source: Any • Destination: Any • Application: App1 • Action: Permit 	Place Rule 2 after Rule 1.
Exact match with a different action	<ul style="list-style-type: none"> • Source: Any • Destination: Any • Application: App1 • Action: Permit 	<ul style="list-style-type: none"> • Source: Any • Destination: Any • Application: App1 • Action: Deny 	Place Rule 2 before Rule 1.
New Rule is a subset of existing rule	<ul style="list-style-type: none"> • Source: Group-A(A1, A2,A3,A4) • Destination: Any • Service: S1 • Action: Deny 	<ul style="list-style-type: none"> • Source: A1 • Destination: Any • Service: S1 • Action: Deny 	Place Rule 2 before Rule 1.
Rule 2 is super set of an existing rule	<ul style="list-style-type: none"> • Source: A1 • Destination: Any • Service: S1 • Action: Deny 	<ul style="list-style-type: none"> • Source: Group-A(A1, A2,A3,A4) • Destination: Any • Service: S1 • Action: Deny 	Place Rule 2 after Rule 1.

Table 122: Examples of Rule Placement Analysis (*Continued*)

Condition	Rule 1 (Existing)	Rule 2 (New)	Suggested Rule Placement
Partial match	<ul style="list-style-type: none"> • Source: Any • Destination: Any • Service: Group-S(S1, S2, S3) • Application: App1 • Action: Permit 	<ul style="list-style-type: none"> • Source: Any • Destination: Any • Service: S1 • Application: Group-A (App1, App2) • Action: Permit 	Place Rule 2 before Rule 1.
No match or no overlap	<ul style="list-style-type: none"> • Source: 172.16.1.0/8 • Destination: Any • Service: S1 • Application: App1 • Action: Deny 	<ul style="list-style-type: none"> • Source: Any • Destination: 10.0.0.1/8 • Service: S2 • Application: App2 • Action: Permit 	Place Rule 2 before Rule 1.

RELATED DOCUMENTATION

[Add a Security Policy | 290](#)

[Edit and Delete a Security Policy | 293](#)

About the Security Policy Rules Page

IN THIS SECTION

 [Tasks You Can Perform | 287](#)

To access this page, click **SRX > Security Policies > Security Policies** and click on security policy rule link. Use Security Policy Rules page to view and manage policy rules associated with the devices. You can filter and sort this information to get a better understanding of what you want to configure.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a security policy rule. See ["Add a Security Policy Rule" on page 307](#) .
- Modify, clone, or delete security policy rules. See ["Edit, Clone, and Delete a Security Policy Rule" on page 313](#) .
- Deploy a security policy. See ["Deploy Security Policies" on page 325](#) .
- Search for a security policy rule. Click the search icon in the top right corner of the page to search for a security policy rule. You can enter partial text or full text of the keyword in the text box and press Enter. The search results are displayed on the same page.
- Show or hide columns. Click the **Show Hide Columns** icon at the top right corner of the page.

Field Descriptions

[Table 123 on page 287](#) provides guidelines on using the fields on the **Security Policy Rule** page.

Table 123: Fields on the Security Policy Rules Page

Field	Description
Seq	Order number for the policy. Policy lookup is performed in the order that the policies are configured. The first policy that matches the traffic is used.

Table 123: Fields on the Security Policy Rules Page *(Continued)*

Field	Description
Hit Count	<p>Displays how often a particular policy is used based on traffic flow. The hit count is the number of hits since the last reset.</p> <p>Example: The hit count is especially useful when you are using a large policy set and you want to verify which rules are highly utilized and which ones are rarely used. Specifically, if you see that some of the rules are not being used, you can verify that the rules are not being shadowed by another policy.</p> <p>This helps you manage the device without having to generate traffic manually.</p>
Name	Name of the security policy rule.
Sources	Source endpoint to which a security policy rule applies. A source endpoint consists of zones, addresses, and identities.
Destinations	Destination endpoint to which a security policy rule applies. A destination endpoint can be zones, addresses, and URL categories.
Applications/Services	Applications and services associated with the security policy.

Table 123: Fields on the Security Policy Rules Page (*Continued*)

Field	Description
Action	<p>Action applies to all traffic that matches the specified criteria.</p> <ul style="list-style-type: none"> • Permit—Device permits traffic using the type of security authentication applied to the policy. • Deny—Device silently drops all packets for the session and does not send any active control messages such as TCP Resets or ICMP unreachable. • Reject—Device sends a TCP reset if the protocol is TCP, and device sends an ICMP reset if the protocols are UDP, ICMP, or any other IP protocol. This option is useful when dealing with trusted resources so that applications do not waste time waiting for timeouts and instead get the active message. • Redirect—The redirect URL or a custom message to be shown when HTTP requests are blocked. • Tunnel—Device permits traffic using the type of VPN tunneling options you applied to the policy.

Table 123: Fields on the Security Policy Rules Page (*Continued*)

Field	Description
Security Subscriptions	<p>Security subscription options:</p> <ul style="list-style-type: none"> • IPS—IPS profile to monitor and prevent intrusions. • Content Security— Content security profile for protection against multiple threat types including spam and malware, and control access to unapproved websites and content. <p>NOTE: To select Juniper NextGen Content security profile, the Junos OS version must be 23.3R1 or later.</p> <ul style="list-style-type: none"> • Decrypt profile— Decrypt profile performs SSL encryption and decryption between the client and the server to obtain granular application information and enable you to apply advanced security subscriptions protection and detect threats. • Anti-malware profile— The anti-malware profile lets you define which files to send to the ATP cloud for inspection and the action to be taken when malware is detected. • SecIntel profile group— SecIntel profile group are used to add SecIntel profiles, such as C&C, DNS, and infected hosts.
Options	Displays scheduling, logging, and rule option information applicable to the security policy rule.
Deploy Status	Displays the deployment status.

Add a Security Policy

A security policy enforces rules for transit traffic, in terms of what traffic can pass through the security, and the actions that need to take place on traffic as it passes through the security.

Use this page to add a security policy and assign it to one or more devices.

NOTE: A single policy can have both zone based rules and global rules for the devices.

To add a security policy:

1. Select **SRX > Security Policies > Security Policies**.

The Security Policy page appears.

2. Click the plus icon (+).

The Add Security Policy page appears.

3. Complete the configuration settings according to the guidelines provided in [Table 124 on page 291](#).

NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **OK**.

The new security policy is created and a confirmation message is displayed.

Table 124: Fields on the Add Security Policy Page

Field	Description
Name	Enter a unique string of alphanumeric characters that can include spaces and some special characters. The maximum length is 255 characters.

Table 124: Fields on the Add Security Policy Page (Continued)

Field	Description
Rule placement analysis	<p>Enable the rule placement analysis for the newly created rules. The rule placement analysis helps you to avoid anomalies by suggesting the correct rule placement.</p> <p>NOTE:</p> <ul style="list-style-type: none"> You can enable the rule placement analysis when you create a security policy or edit an existing security policy. Rule placement analysis suggestion is available only for newly created rules in a security policy. <p>When you create a rule, Juniper Security Director Cloud performs the rule placement analysis. The Suggested Rule Placement page suggests appropriate rule position with a reason for the rule placement suggestion. Click Accept to accept the suggested rule placement. Click Reject to go back to rules page and modify the rule.</p>
Description	Enter a description for the policy; the maximum length is 255 characters.
All devices	Select the toggle button to apply the security policy to all devices.
Select Devices	Select the devices from the Available column and click the right-arrow to move the devices to the Selected column.
Sequence No.	Select this option to specify the policy sequence number. This number identifies the location of your policy in relation to the entire sequence.

Table 124: Fields on the Add Security Policy Page (*Continued*)

Field	Description
Change Sequence Number	Click the link and use the Select Policy Sequence page to move and place the policy to your preferred sequence in the list. This helps you to organize your policy in the required sequence.

RELATED DOCUMENTATION

| [Rule Placement Analysis](#) | 284

Edit and Delete a Security Policy

IN THIS SECTION

- [Edit a Security Policy](#) | 293
- [Delete a Security Policy](#) | 294

You can edit and delete security policies from the **SRX > Security Policies > Security Policies** page.

Edit a Security Policy

To modify the parameters configured for a security policy:

1. Select **SRX > Security Policies > Security Policies**.
The **Security Policy** page appears, displaying the list of security policies.
2. Select the security policy that you want to edit, and then click the pencil icon.
The Edit Security Policy page appears displaying the same options that you entered while creating the security policy.
3. Modify the parameters following the guidelines provided in "[Add a Security Policy](#)" on page 290
4. Click **OK** to save the changes.
The modified policy appears on the **Security Policy** page.

Delete a Security Policy

You may delete a policy in Juniper Security Director Cloud if:

- A new policy is created for the device.
- The existing policy is obsolete.
- The policy was updated directly on the device.
- The policy was not deployed after it was imported from the device.

After you reassign all devices in a policy to a different policy or import the device policy, you must deploy both the policies simultaneously to delete the old policy.

You cannot edit the security policy that is marked to be deleted. However, you can edit the rules for the policy.

1. Go to SRX > Security Policy > SRX Policy.

The **Security Policies** page is displayed.

2. If devices were never assigned to the policy, perform the following steps:

- a. Select the policy and click the delete icon.
- b. Click **Yes** to confirm that you want to delete the policy.
The policy is deleted in Juniper Security Director Cloud.

3. If one or more devices are assigned to the policy, perform the following steps:

- a. Select the policy and click the edit icon.
The **Edit Security Policy** page is displayed.
- b. Unassign the devices, click **OK**, and then click **Yes**
The number of unassigned devices is displayed in the **Status** column in the **Security Policies** page.
- c. Reassign the devices to a different policy or import the policy from the device.
- d. Select both the old and new policies and click **Deploy**.
The **Deploy** page is displayed.
- e. Click **OK**.
Jobs are created to undeploy the existing policy from the devices and the new policy on the devices. You can view the job status on the **Jobs** page.
- f. On the **Security Policies** page, select the old policy, click the delete icon, and then click **Yes** to confirm.
The policy is deleted in Juniper Security Director Cloud.

Reorder a Security Policy

By default, new security policies go to the end of a policy list. Therefore, it is possible for a security policy to eclipse or overshadow another security policy. You can correct the security policy overshadowing by simply changing the order of the security policies, putting the more specific one first. The **Seq.** (sequence number) field in the security policies allow you to change the policy order. This number identifies the location of your policy in relation to the entire sequence.

Steps to change the security policy order:

1. Select **SRX > Security Policy > SRX Policy**.

The **Security Policies** page is displayed with a list of security policies.

2. Select the security policy that you want to edit, and then click the pencil icon.

The Edit Security Policy page is displayed with the same options that you entered while creating the security policy.

3. Click **Reorder**.

The Select Policy Sequence page is displayed.

4. Move the policy to the desired location by using **Move Policy Up** or **Move Policy Down** options.

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

The reordered policy list appears on the **Security Policy** page.

NOTE:

- If you move a security policy, the sequence numbers of all the security policies are automatically adjusted.
- If the same device has more than one security policy, then based on the sequence number of the security policies for the zone pair, the rules are pushed to the device. For example, a security policy **P1** has sequence number **2** and security policy **P2** has sequence number **1**, and both the policies are assigned the same device **D1**. The security policy **P1** is configured from *untrust* zone to *trust* zone with rule *Rule-a*. The security policy **P2** is configured from *untrust* zone to *trust* zone with rule *Rule-b*. If you select these two policies and deploy, then the security policy **P2** (sequence number 1) with rule *Rule-a* is deployed to the device first and then the security policy **P1** (sequence number 2) with *Rule-b* is deployed.
- Global security policies have the similar ordering scheme as that of zone pair security policy order.

Import Security Policies Overview

Juniper Security Director Cloud supports importing policy configurations from next-generation security devices. You can discover existing policy configuration while onboarding next-generation security device (non-ZTP).

Juniper Security Director Cloud uses object name as the unique identifier for an object (such as addresses, services, schedulers, SSL profiles, content security, IPS, and Layer 7 applications). During policy import, all objects supported by Juniper Security Director Cloud are imported and all objects names are compared between what is in Juniper Security Director Cloud and what is on the next-generation security device. A conflict occurs when the name of the object to be imported matches an existing object, but the value of the object does not match. The object conflict resolution (OCR) operation is triggered to resolve the object name conflicts.

- If the object name does not exist in Juniper Security Director Cloud, the object is added to Juniper Security Director Cloud.
- If the object name exists in Juniper Security Director Cloud with the same content, the existing object in Juniper Security Director Cloud is used.
- If the object name exists in Juniper Security Director Cloud with different content, the object conflict resolution operation is triggered. The following conflict resolution options are available.
 - Rename object
 - This is the default option.
 - By default, the suffix "_1" is added to the object name. Alternatively you can specify a new unique name.
 - Deploying the policy will delete the original object and add the object with the new name.
 - There is no functional change to the security policy (labels only).
 - Overwrite with imported value
 - The object in Juniper Security Director Cloud is replaced with the object from the import operation.
 - The change will be reflected for all other devices that use this object after the policy deployment.
 - There is no functional change to the security policy.
 - There might be possible traffic impact to all other devices that use this object the next time the other device is updated from Juniper Security Director Cloud.
 - Keep existing object

- The object name in Juniper Security Director Cloud is used instead of what is on the next generation security device.
- Policy deployment for the imported security policy will show the modification.
- There might be possible traffic impact to this security because the content is different in some way.

The following section provides an example for importing policies. Here we use Address as an object type and see how to resolve the object name conflicts.

The existing objects in Juniper Security Director Cloud are listed in [Table 125 on page 297](#) .

Table 125: Existing address in Juniper Security Director Cloud

Object Name	Existing Value
Address 1	198.51.100.10
Address 2	198.51.100.20
Address 3	198.51.100.30

The existing objects in the next generation security device are listed in [Table 126 on page 297](#) .

Table 126: Existing address in next-generation security device

Object name	Existing Value
Address 1	203.0.113.10/32
Address 2	203.0.113.20/32
Address 3	203.0.113.30/32

During policy import, OCR is triggered and the object conflicts between next generation security device and Juniper Security Director Cloud. The resolution that we have chosen is listed in [Table 127 on page 298](#) .

Table 127: OCR while importing policies to Juniper Security Director Cloud

Object Name in Juniper Security Director Cloud	Object Type in Juniper Security Director Cloud	Existing Value in Juniper Security Director Cloud	Imported Value to Juniper Security Director Cloud	Conflict Resolution	New Object Name in Juniper Security Director Cloud
Address 1	Address	198.51.100.10	203.0.113.10	Keep Existing Object	Address1_1
Address 2	Address	198.51.100.2	203.0.113.20	Overwrite with Imported value	Address2_1
Address 3	Address	198.51.100.30	203.0.113.30	Rename Object	Address3_1

The object values and the result after resolving conflicts are listed in [Table 128 on page 298](#) .

Table 128: After importing policies to Juniper Security Director Cloud

Discovered Object Name in Juniper Security Director Cloud	Discovered Value in Juniper Security Director Cloud	Result
Address 1	198.51.100.10	No change
Address 2	203.0.113.20	Content changed
Address 3	198.51.100.30	No change
Address3_1	203.0.113.30	Address3_1 create

Import Security Policies

Use this page to manually import a security policy from the discovered or onboarded devices.

To import a security policy:

1. Select **SRX > Security Policies > Security Policies**.

The Security Policy page appears.

2. Click **Import**.

The Import Security Policies page appears displaying a list of discovered devices (next generation security devices).

3. Select the device from which you want to import the security policies and click **Next**.
The Discovered Services tab appears.
4. Select the Security Policy and NAT policy services that you want to import and click **Next**.
The Resolve Conflicts tab appears.
5. For any conflicts with the imported objects, object conflict resolution (OCR) operation is triggered. The Conflicts window displays all the conflicts between Juniper Security Director Cloud and the next-generation security device. Select an object from the Conflicts window and click on any of the below option to resolve the object conflict.

The resolution options are:

- **Rename Object**— Rename the imported object. By default, the suffix "**_1**" is added to the object name, or you can specify a new name.
- **Overwrite with imported value**— The object in Juniper Security Director Cloud is replaced with the object from the import operation.
- **Keep existing object**— The object name in Juniper Security Director Cloud is used instead of what is on the next-generation security device.

6. Click **Finish**.

A summary of the discovered services is listed.

7. Review the summary and click **OK** to import the security policies.

The security policies are imported from next-generation security device to Juniper Security Director Cloud. You can view the imported policy from the Security Policy page.

RELATED DOCUMENTATION

[Edit and Delete a Security Policy | 293](#)

[Deploy Security Policies | 325](#)

[Edit, Clone, and Delete a Security Policy Rule | 313](#)

About the Manage Policy Versions Page

IN THIS SECTION

- [Tasks You Can Perform | 300](#)

To access this page, click **SRX > Security Policies > Security Policies** and select the security policy rule link click **More > Manage Policy Versions**.

Use the Manage Policy Versions page to view or manage all available versions of a selected policy.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a policy version. See "[Create a Policy Version](#)" on page 301 .
- View policy version details. See "[View Policy Version Details](#)" on page 301 .
- Rollback to a specific version. See "[Roll Back a Policy Version](#)" on page 306 .
- Delete a policy version. See "[Delete a Policy Version](#)" on page 307 .
- Show or hide columns. Click the **Show Hide Columns** icon at the top right corner of the page.

Field Descriptions

[Table 129 on page 300](#) provides guidelines on using the fields on the **Manage Policy Versions** page.

Table 129: Fields on the Manage Policy Versions Page

Field	Description
Policy Version	The name of the policy version.
Created By	The user who created the policy version.
Created On	The date and time when the policy version was created.
Description	Description for the policy version.

Create a Policy Version

NOTE: During policy deploy, Juniper Security Director Cloud takes an automatic snapshot of the policy. This topic explains to create a policy version by taking snapshot.

You can create a policy version by taking a snapshot. You can create versions for all types of policies including All Devices, Group, Device, and Device exceptions.

By default, the maximum 10 versions are maintained for a policy. If the maximum limit is reached, the oldest version will be removed before saving a new version for that policy.

NOTE: Administrator can change the maximum number of default versions that are allowed per policy by changing the **Snapshots per policy** in the organization settings. See "[About the Organization Page](#)" on page 1051 for details.

Versioning and rollback are independent operations for each policy. For example, if you take a snapshot of a group firewall policy, or rollback to a previous firewall policy version, it does not change the version for all device policy rules. You must separately version each policy rule.

To create policy version:

1. Select **SRX > Security Policies > Security Policies**.
The Security Policies page appears.
2. Select the security policy and click **More > Take Snapshot-Manage Policy Versions**.
The Snapshot page appears.
3. Enter your comment in the **Description** field (maximum 255 characters) and click **OK**.
The Snapshot Policy page shows the status of the version.

RELATED DOCUMENTATION

[View Policy Version Details](#) | 301

[About the Organization Page](#) | 1051

View Policy Version Details

You can view the details of the policy versions associated with a security policy.

To view the details of policy versions:

1. Select **SRX > Security Policies > Security Policies**.

The Security Policies page appears.

2. Select the check box next to the policy and then right-click the policy or click **More**.

A list of actions appears.

3. Select **Manage Policy Versions**.

The Manage Version page appears.

4. Select the version that you want to view details and click **View Details**.

[Table 130 on page 302](#) provides the fields on the **Version Details** page.

Table 130: Policy Version Detail Fields

Field	Description
Version Details	
Policy Version	Policy version showing the latest policy version at the top.
Created By	E-mail address of the user who created the policy.
Created On	The date and time when the policy was created.
Policy Details	
Name	Name of the security policy.
Rules	Number of rules associated with the policy.
Description	Description for the security policy.
Rules	
Seq	Order number for the policy.
Rule Name	Security policy rule name.
Sources	Source endpoint to which a security policy rule applies. A source endpoint consists of zones, addresses, and identities.

Table 130: Policy Version Detail Fields *(Continued)*

Field	Description
Destinations	Destination endpoint to which a security policy rule applies. A destination endpoint can be zones, addresses, and URL categories.
Applications/ Services	Applications and services associated with the security policy.
Action	<p>Action applies to all traffic that matches the specified criteria.</p> <ul style="list-style-type: none"> • Permit—Device permits traffic using the type of security authentication applied to the policy. • Deny—Device silently drops all packets for the session and does not send any active control messages such as TCP Resets or ICMP unreachable. • Reject—Device sends a TCP reset if the protocol is TCP, and device sends an ICMP reset if the protocols are UDP, ICMP, or any other IP protocol. This option is useful when dealing with trusted resources so that applications do not waste time waiting for timeouts and instead get the active message. • Redirect—The redirect URL or a custom message to be shown when HTTP requests are blocked. • Tunnel—Device permits traffic using the type of VPN tunneling options you applied to the policy.
Security Services	<p>Hover your cursor over the highlighted advanced security options to view the details:</p> <ul style="list-style-type: none"> • IPS—Displays the IPS profile information including IPS rules and exempt rules. • Content Security— Displays the content security profile information for protection against multiple threat types including spam and malware, and control access to unapproved websites and content. • Decrypt—Displays SSL proxy profile. • SecIntel—Displays SecIntel profiles such as C&C, DNS, and infected hosts. • Anti-malware—Displays the anti-malware profiles associated with the security policy version.

Table 130: Policy Version Detail Fields *(Continued)*

Field	Description
Options	Displays scheduling, logging, and rule option information applicable to the security policy rule.

Compare Policy Versions

You can compare two different versions of a policy to make decisions such as, roll back to a previous version of a policy or make certain configuration changes and deploy the security policy again. You can compare the policy versions and view the following changes that are made in the latest policy version.

- Added, deleted, or revised rules.
- Changes made for rule positions. For example, a rule is moved inside a group or a rule that is taken out of a group.
- Rules that are unchanged in the the latest policy version.
- Object-level changes such as changes in source, destination, application or services, action, security subscriptions, and options.

To compare two different versions of a policy:

1. Select **SRX > Security Policy > SRX Policy**.

The Security Policies page appears.

2. Select the check box for the security policy and click **More > Manage Policy Versions**.

The policy version page appears.

3. Select the versions to compare and click **Compare**.

NOTE: You can compare only two versions of a policy at a time.

The compare versions page appears by showing the color-coded legends and count for the added, deleted, revised, and moved rules. View the differences according to the guidelines provided in [Table 131 on page 305](#) .

For the field descriptions, see [Table 123 on page 287](#) .

Table 131: Guidelines for Compare Policy Versions

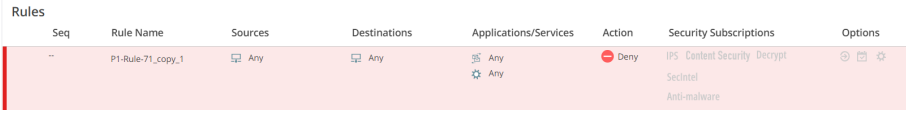

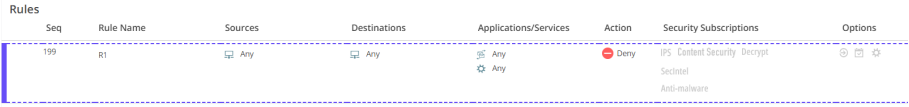
Items to view	Description																																
<p>Added rules</p>	<p>These rules are displayed with green background.</p>  <table border="1"> <thead> <tr> <th>Seq</th> <th>Rule Name</th> <th>Sources</th> <th>Destinations</th> <th>Applications/Services</th> <th>Action</th> <th>Security Subscriptions</th> <th>Options</th> </tr> </thead> <tbody> <tr> <td>3</td> <td>R2_New-rule</td> <td>Any</td> <td>Any</td> <td>Any</td> <td>Deny</td> <td>IPS, Content Security, Decrypt, SecIntel, Anti-malware</td> <td></td> </tr> </tbody> </table>	Seq	Rule Name	Sources	Destinations	Applications/Services	Action	Security Subscriptions	Options	3	R2_New-rule	Any	Any	Any	Deny	IPS, Content Security, Decrypt, SecIntel, Anti-malware																	
Seq	Rule Name	Sources	Destinations	Applications/Services	Action	Security Subscriptions	Options																										
3	R2_New-rule	Any	Any	Any	Deny	IPS, Content Security, Decrypt, SecIntel, Anti-malware																											
<p>Deleted rules</p>	<p>These rules are displayed with red background.</p>  <table border="1"> <thead> <tr> <th>Seq</th> <th>Rule Name</th> <th>Sources</th> <th>Destinations</th> <th>Applications/Services</th> <th>Action</th> <th>Security Subscriptions</th> <th>Options</th> </tr> </thead> <tbody> <tr> <td>--</td> <td>P1-Rule-71_copy_1</td> <td>Any</td> <td>Any</td> <td>Any</td> <td>Deny</td> <td>IPS, Content Security, Decrypt, SecIntel, Anti-malware</td> <td></td> </tr> </tbody> </table>	Seq	Rule Name	Sources	Destinations	Applications/Services	Action	Security Subscriptions	Options	--	P1-Rule-71_copy_1	Any	Any	Any	Deny	IPS, Content Security, Decrypt, SecIntel, Anti-malware																	
Seq	Rule Name	Sources	Destinations	Applications/Services	Action	Security Subscriptions	Options																										
--	P1-Rule-71_copy_1	Any	Any	Any	Deny	IPS, Content Security, Decrypt, SecIntel, Anti-malware																											
<p>Revised rules</p>	<p>These rules are displayed with orange background.</p>  <table border="1"> <thead> <tr> <th>Seq</th> <th>Rule Name</th> <th>Sources</th> <th>Destinations</th> <th>Applications/Services</th> <th>Action</th> <th>Security Subscriptions</th> <th>Options</th> </tr> </thead> <tbody> <tr> <td>2</td> <td>R2</td> <td>SITE-A, 192.0.2.0/8, unauthenticated...</td> <td>SITE-B, 10.0.0.0/8</td> <td>APP-1, SERVICE-1</td> <td>Deny</td> <td>IPS, Content Security, Decrypt, SecIntel, Anti-malware</td> <td>Rule Diff</td> </tr> </tbody> </table>	Seq	Rule Name	Sources	Destinations	Applications/Services	Action	Security Subscriptions	Options	2	R2	SITE-A, 192.0.2.0/8, unauthenticated...	SITE-B, 10.0.0.0/8	APP-1, SERVICE-1	Deny	IPS, Content Security, Decrypt, SecIntel, Anti-malware	Rule Diff																
Seq	Rule Name	Sources	Destinations	Applications/Services	Action	Security Subscriptions	Options																										
2	R2	SITE-A, 192.0.2.0/8, unauthenticated...	SITE-B, 10.0.0.0/8	APP-1, SERVICE-1	Deny	IPS, Content Security, Decrypt, SecIntel, Anti-malware	Rule Diff																										
<p>Object-level changes in revised rules</p>	<p>Click Rule Diff option to view the object-level changes. To view the detailed differences for objects, click the View Detailed Rule Diff option. This will show object level differences for the entire policy.</p>																																
<p>Unchanged rules</p>	<p>These are the rules that are not changed between the two policy versions. Unchanged rules are shown using white background. By default, the unchanged rules are shown in collapsible format. Click the >UNCHANGED RULES menu to view all the unchanged rules.</p>  <table border="1"> <thead> <tr> <th>Seq</th> <th>Rule Name</th> <th>Sources</th> <th>Destinations</th> <th>Applications/Services</th> <th>Action</th> <th>Security Subscriptions</th> <th>Options</th> </tr> </thead> <tbody> <tr> <td colspan="8">> UNCHANGED RULES (86 Rules)</td> </tr> <tr> <td>5</td> <td>R5</td> <td>Any</td> <td>Any</td> <td>Any</td> <td>Deny</td> <td>IPS, Content Security, Decrypt, SecIntel, Anti-malware</td> <td></td> </tr> <tr> <td>6</td> <td>R6</td> <td>Any</td> <td>Any</td> <td>Any</td> <td>Deny</td> <td>IPS, Content Security, Decrypt, SecIntel, Anti-malware</td> <td></td> </tr> </tbody> </table>	Seq	Rule Name	Sources	Destinations	Applications/Services	Action	Security Subscriptions	Options	> UNCHANGED RULES (86 Rules)								5	R5	Any	Any	Any	Deny	IPS, Content Security, Decrypt, SecIntel, Anti-malware		6	R6	Any	Any	Any	Deny	IPS, Content Security, Decrypt, SecIntel, Anti-malware	
Seq	Rule Name	Sources	Destinations	Applications/Services	Action	Security Subscriptions	Options																										
> UNCHANGED RULES (86 Rules)																																	
5	R5	Any	Any	Any	Deny	IPS, Content Security, Decrypt, SecIntel, Anti-malware																											
6	R6	Any	Any	Any	Deny	IPS, Content Security, Decrypt, SecIntel, Anti-malware																											

Table 131: Guidelines for Compare Policy Versions (*Continued*)

Items to view	Description																
Moved rules	<p>Rules that are moved to different position or group. The moved rules are shown using dotted lines. You can view the previous position or group by hovering over the sequence number field for that rule.</p>  <table border="1" data-bbox="516 491 1419 596"> <thead> <tr> <th>Seq</th> <th>Rule Name</th> <th>Sources</th> <th>Destinations</th> <th>Applications/Services</th> <th>Action</th> <th>Security Subscriptions</th> <th>Options</th> </tr> </thead> <tbody> <tr> <td>199</td> <td>R1</td> <td>Any</td> <td>Any</td> <td>Any</td> <td>Deny</td> <td>IPS Content Security, Decrypt, Sentinel, Anti-malware</td> <td></td> </tr> </tbody> </table>	Seq	Rule Name	Sources	Destinations	Applications/Services	Action	Security Subscriptions	Options	199	R1	Any	Any	Any	Deny	IPS Content Security, Decrypt, Sentinel, Anti-malware	
Seq	Rule Name	Sources	Destinations	Applications/Services	Action	Security Subscriptions	Options										
199	R1	Any	Any	Any	Deny	IPS Content Security, Decrypt, Sentinel, Anti-malware											
Go back to comparison page	<p>You can go back and view the policy version page by clicking the <Manage Policy Versions link.</p>																

RELATED DOCUMENTATION

| [About the Security Policy Rules Page](#) | 286

Roll Back a Policy Version

You can revert a policy version to a specific previous version.

To roll back the selected version so it becomes the current version:

1. Select **SRX>Security Policies>Security Policies**.

The Security Policies page appears.

2. Select the check box next to the policy for which you are rolling back a version, and then right-click the policy or click **More**.

A list of actions appears.

3. Select **Manage Policy Versions**.

4. Select the version that you want to make as the current version, and click **Rollback**.

The rollback operation replaces all the rules and rule groups of the current version with rules and rule groups from the selected version. The **Resolve Conflicts** section displays any conflicts between the versioned data and the current objects in the system. Select an object from the **Resolve Conflicts** and click one of the below options to resolve the object conflict.

- **Rename**—Rename the imported object. By default, the suffix "**_1**" is added to the object name, or you can specify a new name.

- **Overwrite**—The object in Juniper Security Director Cloud is replaced with the object imported from the snapshot version.



CAUTION: Overwriting an object may impact other device configurations.

- **Retain**—The object name in Juniper Security Director Cloud is used instead of what is on the policy snapshot version.
5. Click **OK** to replace the current policy with the versioned data. A summary of the snapshot policy is shown by clicking Snapshot.

Delete a Policy Version

To delete a policy version:

1. Select **SRX > Security Policies > Security Policies**.
The Security Policies page appears.
2. Select the policy right-click the policy or click **More**.
A list of actions appears.
3. Select **Manage Policy Versions**.
The Manage Version page appears.
4. Select the policy version you want to delete and click delete icon.
A warning message is displayed.
5. Click **Yes** to confirm the deletion.

Add a Security Policy Rule

Use this page to add a security policy rule that controls transit traffic within a context. 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.

You can also enable advanced security protection by specifying one or more of the following:

- Content security profile
- Decrypt profile
- Intrusion prevention system (IPS) profile

- Anti-malware profile
- Secintel profile group
- secure Web proxy profile

To configure a security policy rule:

1. Select **SRX>Security Policy>SRX Policy**.
The Security Policies page appears.
2. Click the security policy to which you want to add the rule.
The *Security-Policy-Name* page appears.
3. Click the add icon (+).
The option to create security policy rule appears inline on the The *Security-Policy-Name* page.
4. Complete the configuration according to the guidelines provided in [Table 132 on page 308](#) .

Table 132: Fields on the Security Policy Name Page

Field	Description
General Information	
Name	Enter a unique string beginning with a number or letter and consisting of letters, numbers, dashes and underscores. No spaces are allowed and the maximum length is 63 characters. If you do not enter a name, the rule is saved with a default name assigned by Juniper Security Director Cloud.
Description	Enter a description for the policy rule; maximum length is 900 characters. The description must be a string excluding '&', '<', '>' and '\n' characters.

Table 132: Fields on the Security Policy Name Page (*Continued*)

Field	Description
Sources	<p>Click the add icon (+) to select the source endpoint on which the security policy rule applies, from the displayed list of zone, addresses, and users.</p> <p>NOTE: You can choose to save a rule as a zone-based rule or a global rule for the following conditions:</p> <ul style="list-style-type: none"> • The Save rule option is enabled in the organization settings. See "Save rule option" on page 1053 • You have selected single zone as source and single zone as destination.
Destinations	<p>Click the add icon (+) to select the destination endpoint on which the security policy rule applies, from the displayed list of zone, addresses, and URL categories.</p> <p>NOTE: You can choose to save a rule as a zone-based rule or a global rule for the following conditions:</p> <ul style="list-style-type: none"> • The Save rule option is enabled in the organization settings. See "Save rule option" on page 1053 • You have selected single zone as source and single zone as destination.
Applications/Services	<p>Click the add icon (+) to select the applications and services.</p> <p>The secure Web proxy feature does not support unified policies. So, if you want to associate a secure Web proxy profile with the rule, you must disable the Applications toggle switch. However, you can select the required applications when you configure the secure Web proxy profile.</p>

Table 132: Fields on the Security Policy Name Page (*Continued*)

Field	Description
Action	<p>From the drop-down menu, select the action for the traffic between the source and destination.</p> <ul style="list-style-type: none"> • Permit—Device permits the traffic. • Deny—Device silently drops all packets for the session and does not send any active control messages such as TCP Resets or ICMP unreachable. • Reject—Device drops the packet and sends the following message based on traffic type: <ul style="list-style-type: none"> • TCP traffic: Device sends the TCP reset message to the source host • UDP traffic: Device sends the ICMP message “destination unreachable, port unreachable”. • For all other traffic: Device drops the packet without notifying the source host. • Redirect—When a policy blocks HTTP or HTTPS traffic with a reject action, you can define a response in the unified policy to notify the connected client. Redirect Options: <ul style="list-style-type: none"> • Message— Select the message from the drop-down list or click Create redirect message and enter the message (in the Block Message field). • URL— Select the redirect URL from the drop-down list or click Add redirect URL and enter the redirect URL. • Tunnel—Device permits traffic using the type of VPN tunneling options you applied to the policy.

Table 132: Fields on the Security Policy Name Page (Continued)

Field	Description
Security Subscriptions	<p>NOTE: This field is enabled only if you either select Permit or Reject for the action.</p> <ul style="list-style-type: none"> <p>IPS profile— When you set the action to Permit, you can specify an IPS profile by selecting a profile from the list (under IPS Profiles).</p> <p>You specify an IPS profile to monitor and prevent intrusions.</p> <p>Content Security profile— When you set the action to Permit, you can specify a content security profile by selecting a profile from the list (under Content Security Profiles).</p> <p>You specify a content security profile for protection against multiple threat types including spam and malware, and control access to unapproved websites and content.</p> <p>You can add a new content security profile by clicking + in the End Points pane and selecting Content Security Profiles.</p> <p>Decrypt profile—</p> <p>You can configure decrypt profile when the action is Permit or Reject or Redirect.</p> <p>Decrypt profile performs SSL encryption and decryption between the client and the server to obtain granular application information and enable you to apply advanced security subscriptions protection and detect threats.</p> <p>Anti-malware profile—When you set the action to Permit, you can assign the anti-malware profile to the security policy by enabling the toggle. The anti-malware profile lets you define which files to send to the ATP cloud for inspection and the action to be taken when malware is detected.</p>

Table 132: Fields on the Security Policy Name Page (*Continued*)

Field	Description
	<ul style="list-style-type: none"> • SecIntel profile group– When you set the action to Permit, you can assign the SecIntel profile group to the security policy by enabling the toggle. SecIntel profile group are used to add SecIntel profiles, such as C&C, DNS, and infected hosts. • Secure Web Proxy– When you set the action to Permit, you can enable the toggle switch to assign the secure Web proxy profile. A secure Web proxy profile enables applications to bypass a proxy server and connect to a web server directly. For more information about secure Web proxy profile, see "About the Secure Web Proxy Page" on page 489 . • Customize– Use this option to configure the security subscriptions for the policy. If there is no default profile configured, you can configure it using the customize option or set the default profile using Global options. See "Configure Global Options" on page 315 for more details.
Options	
Schedule	Policy schedules enable you to define when a policy is active, and thus are an implicit match criterion. You can define the day of the week and the time of the day when the policy is active. for example, you can define a security policy that opens or closes access based on business hours. Select a pre-saved schedule and the schedule options are populated with the selected schedule data.
Session initiate logs	Select this option to enable logging of events when sessions are created.

Table 132: Fields on the Security Policy Name Page (Continued)

Field	Description
Session close logs	Select this option to enable logging of events when sessions are closed. When logging is enabled, the system logs at session close time by default.
Rule options	Use this page to create an object to specify redirect options, Authentication, TCP-options, and action for destination-address translated or untranslated packets.

5. Click the check mark icon ✓ to save the changes.

A new security policy rule with the provided configuration is saved and a confirmation message is displayed. Based on the source and destination end points, the rules are categorized as zone-based rules and global rules.

Edit, Clone, and Delete a Security Policy Rule

IN THIS SECTION

- [Edit a Security Policy Rule | 313](#)
- [Clone a Security Policy Rule | 314](#)
- [Delete a Security Policy Rule | 314](#)

You can edit, clone, and delete security policy rules from the **SRX > Security Policies > Security Policies** page.

Edit a Security Policy Rule

To modify the parameters configured for a security policy rule:

1. Select **SRX > Security Policies > Security Policies**.

The **Security Policy** page appears, displaying the list of security policies.

2. Click the security policy for which you want to edit the security policy rules.
The security policy rules are displayed in the Security Policy page.
3. Click the pencil icon that appears on the right side of the rule.
The **Security Policy** page displays the same options as those that appear when you create a new security policy rule.
4. Modify the parameters following the guidelines provided in ["Add a Security Policy Rule" on page 307](#) .
5. Click ✓ to save the changes.
The modified rule appears on the **Security Policy** page.

Clone a Security Policy Rule

To clone a security policy rule:

1. Select **SRX > Security Policies > Security Policies**.
The **Security Policy** page appears, displaying the rules associated with the policy.
2. Click the security policy for which you want to clone the security policy rules.
The security policy rules are displayed in the Security Policy page.
3. Right-click and select **Clone**. Alternatively, click **More** drop-down menu and select **Clone**.
The **Security Policy** page displays the same options as those that appear when you create a new security policy rule. Update the cloned rule as required.
4. Click **Save** to save the changes. If you want to discard your changes, click **Cancel** instead.
5. Click ✓ to save the changes.
The modified rule appears on the **Security Policy** page.

Delete a Security Policy Rule

To delete a security policy rule:

1. Select **SRX > Security Policies > Security Policies**.
The **Security Policy** page appears, displaying the rules associated with the policy.
2. Click the security policy for which you want to delete the security policy rules.
The security policy rules are displayed in the Security Policy page.
3. Select the security policy rule you want to delete, and then click the delete icon that appears on the right side of the rule. Click **Delete**.
An alert message appears, verifying that you want to delete the selected rule.
4. Click **Yes** to delete the selected rule.
The selected rule is deleted from the policy.

Reorder a Security Policy Rule

The security policy applies the security rules to the transit traffic within a context (*from-zone* to *to-zone*). The action of the first rule that matches the traffic is applied to the packet. If there is no matching rules, the packet is dropped. The rules are matched from top to bottom, so it is a good idea to place more specific rules near the top of the list.

For example, a security policy **P1** is configured from *untrust* zone to *trust* zone with two rules rule *Rule-a* and *Rule-b* respectively. If you select *Rule-a* and move it to the bottom, Juniper Security Director Cloud generates a command to push the *Rule-b* to first place in the device.

Steps to move security policy rule order:

1. Select **SRX > Security Policy > SRX Policy**.
The **Security Policy** page appears, displaying the list of security policies.
2. Click the security policy that you want to edit.
The security policy page is displayed with a list of rules.
3. Select the rule to be reordered.
4. Click **More**, and select any of the following options to change the rule ordering.
 - Move Top
 - Move Up
 - Move Down
 - Move Bottom

The modified rule order is displayed on the Security Policy page.

5. Preview and deploy the security policy with the reordered rules. For details, see "[Deploy Security Policies](#)" on page 325

Configure Global Options

You can configure the global options by setting the default security settings and default security subscriptions. The global options are tenant-level configurations and are applicable for all the devices under the tenant.

- **Default Security Settings**—The security policy takes some time to detect the L7 application in a traffic and act upon it. The default profiles help in providing security during that time. Configure the default security settings.

- **Default Security Subscriptions**—You can set the default profiles to apply to a firewall rule. You can customize these settings at rule level. The default profiles are applied to a security policy rule, only if the profiles are enabled for that rule.

To configure the global options for a security policy:

1. Select **SRX > Security Policies > Security Policies**.

The Security Policy page appears.

2. Click **Global options**.

The Global Options page appears displaying a list of default settings.

3. Complete the configuration according to the guidelines provided in [Table 133 on page 316](#).

Table 133: Fields on the Global Options Page

Field	Description
Default security settings	
IPS profile	An IPS profile that will be set as default IPS policy.
Content Security profile	A content security profile that will be set as default-configuration for content security.
Decrypt profile	A decrypt profile that will be set as a default decrypt profile.
Anti-malware profile	An anti-malware profile that will be set as a default anti-malware profile.
Secintel Profile Group	A selected secintel profile group that will be set as a default Secintel profile group.
Default Security Subscriptions	
IPS profile	Select an IPS profile to assign to policy rules. The selected IPS profile is applied as a default IPS profile when you enable the IPS toggle button is at rule level. See "Add a Security Policy Rule" on page 307 . NOTE: You can customize an IPS profile at the rule level. The rule-level IPS profile takes precedence over the default IPS profile that you select using the global option.

Table 133: Fields on the Global Options Page (Continued)

Field	Description
Content Security profile	<p>Select a content security profile to assign to policy rules. The selected content security profile is applied as a default content security profile when you enable the Content Security toggle button is at rule level. See "Add a Security Policy Rule" on page 307 .</p> <p>NOTE: You can customize an content security profile at the rule level. The rule-level content security profile takes precedence over the default content security profile that you select using the global option.</p>
Decrypt profile	<p>Select the decrypt profile to assign to policy rules. The selected decrypt profile is applied as a default decrypt profile when you enable the Decrypt profile toggle button at rule level. See "Add a Security Policy Rule" on page 307 .</p> <p>NOTE: You can customize the decrypt profile at the rule level. The rule-level decrypt profile takes precedence over the default decrypt profile that you select using the global option.</p>
Anti-malware profile	<p>Select an anti-malware profile to assign to policy rules. The selected anti-malware profile is applied as a default anti-malware profile when you enable the Anti-malware profile toggle button at rule level. See "Add a Security Policy Rule" on page 307 .</p> <p>NOTE: You can customize an anti-malware profile at the rule level. The rule-level anti-malware profile takes precedence over the default anti-malware profile that you select using the global option.</p>

Table 133: Fields on the Global Options Page (Continued)

Field	Description
Secintel Profile Group	<p>Select a Secintel profile group to assign to policy rules. The selected Secintel profile group is applied as a default Secintel profile group when you enable the Secintel Profile Group toggle button at rule level. See "Add a Security Policy Rule" on page 307</p> <p>NOTE: You can customize a Secintel profile group at the rule level. The rule-level Secintel profile group takes precedence over the default Secintel profile group that you select using the global option.</p>

4. Click **OK**.

A confirmation message is displayed.

Configure Default Rule Option

You can set the default rule options to apply to a security policy rule. The default rule options are applied when you enable the **Rule options** toggle at the rule level. However, you can customize the rule options at rule level. The rule-level customization takes precedence over the default rule option.

To configure the default rule option:

1. Select **SRX > Security Policies > Security Policies**.

The Security Policy page appears.

2. Select the security policy rule and click **Set Default Rule Option**.

The Set Default Rule Options page appears displaying a list of default settings.

3. Select the default rule options from the available list alternatively you can create the new rule option by clicking on **Create New**. See ["Create Rule Options" on page 849](#).

4. Click **OK**.

The default rule option is added.

Select a Security Policy Rule Source

You can view and select the source end point from the complete list of zone, addresses, including the identity of such source end point.

1. Click the **Sources** field. A list of relevant endpoints are displayed.
2. Complete the configuration according to the guidelines provided in [Table 134 on page 319](#)

Table 134: Source Fields on the Security Policy Rule Page

Field	Description
Zone	For SRX Series Firewalls, specify a source zone (from-zone) to define the context for the policy. Zone policies are applied on traffic entering one security zone (source zone) to another security zone (destination zone).
Addresses	<p>Enter one or more address names or address set names.</p> <ul style="list-style-type: none"> • Any—Add any address to the security policy rule. • Specific—Select the check box beside each address you want to include in the address group. Click the greater-than icon (>) to move the selected address or addresses from the Available column to the Selected column. Note that you can use the fields at the top of each column to search for addresses. See "Create Addresses or Address Groups" on page 863 .
Identity	Specify the source identity to be used as match criteria for the policy. You can have different policy rules based on user roles and user groups. Click the greater-than icon (>) to move the selected user identity from the Available column to the Selected column. You can select a source identity from the available list or you can create a new identify by clicking add icon (+).

3. Click **OK** to select the end point as a source.

Select a Security Policy Rule Destination

You can view and select the destination end point from the complete list of zones and addresses.

1. Click on **Destinations**. A list of relevant end points are displayed.
2. Complete the configuration according to the guidelines provided in [Table 135 on page 320](#)

Table 135: Destination Fields on the Security Policy Rule Page

Field	Description
Zone	<p>For SRX Series Firewalls, specify a destination zone (to-zone) to define the context for the policy. Zone policies are applied on traffic entering one security zone (source zone) to another security zone (destination zone).</p>
Addresses	<p>Enter one or more address names or address set names.</p> <ul style="list-style-type: none"> • Any—Add any address to the security policy rule. • Specific—Select the check box beside each address you want to include in the address group. Click the greater-than icon (>) to move the selected address or addresses from the Available column to the Selected column. Note that you can use the fields at the top of each column to search for addresses. See "Create Addresses or Address Groups" on page 863 .
URL Categories	<p>Select the URL category:</p> <ul style="list-style-type: none"> • None • Any—Add any URL to the security policy rule. • Specific—Select the check box beside each URL you want to include. Click the greater-than icon (>) to move the selected URLs from the Available column to the Selected column.

3. Click **OK** to select the end point as a destination.

Select Applications and Services

IN THIS SECTION

- [Add Applications and Services to Security Policy Rule | 321](#)

The following procedures provides various methods using which you can add applications and services to the security policy rule.

Add Applications and Services to Security Policy Rule

You can add the applications and services to the existing security policy rule name.

1. Click on **Applications/Services**. Applications & Services page is displayed.
2. Complete the configuration according to the guidelines provided in [Table 136 on page 321](#)

Table 136: Applications and Services Fields on the Security Policy Rule Page

Field	Description
Applications	<p>Select one of the following options for the applications:</p> <ul style="list-style-type: none"> ● Any—Add any application to the security policy rule. ● None ● Specific—Click the Add Application link or + icon to add the application and select the check boxes next to the application to be added. <p>NOTE: You can search for a specific application by entering the search criteria in the search field. You can search the applications by their name.</p>

Table 136: Applications and Services Fields on the Security Policy Rule Page (*Continued*)

Field	Description
Services	<p>Select one of the following options for the services:</p> <ul style="list-style-type: none"> • Default—Junos-default services. • Any—Add any service to the security policy rule. • Specific—Select the check box beside each service you want to include. Click the greater-than icon (>) to move the selected service or services from the Available column to the Selected column. Note that you can use the fields at the top of each column to search for services.

3. Click **OK** to add the selected applications and services to the security policy rule.

Common Operations on a Security Policy Rule

You can perform common operations on a security policy rule from the *Security Policy* page.

To perform common operations on a security policy rule:

1. Select **SRX > Security Policies > Security Policies**.

The **Security Policy** page appears.

2. Click the security policy rule and click **More**.

The drop-down menu shows common operations for a security policy rule.

3. Complete the configuration according to the guidelines provided in the following table.

Table 137: Common Operations on Security Policy Rules Page

Field	Description
Add Rule Before	Add a rule before an existing rule.
Add Rule After	Add a rule after an existing rule.

Table 137: Common Operations on Security Policy Rules Page (*Continued*)

Field	Description
Copy	<ul style="list-style-type: none"> • Copy an existing rule and paste it within the policy. • Copy multiple existing rules and paste within same policy. • Copy an existing rule and paste from one policy to another policy. • Copy multiple existing rules and paste from one policy to another policy. <p>NOTE: Copying and pasting of zone based rules to global rules or vice versa is not allowed.</p>
Cut	Cut an existing rule to paste at different order.
Paste	<p>Before—Paste the rules before an existing rule.</p> <p>After—Paste the rules after and existing rule.</p>
Clone	Create a copy of an existing rule.
Enable	Enable the rule.
Disable	Disable the rule.
Move	<p>Move the rule by selecting one of the following options:</p> <ul style="list-style-type: none"> • Move Top • Move Up • Move Down • Move Bottom

Table 137: Common Operations on Security Policy Rules Page *(Continued)*

Field	Description
Clear All Selections	Clear the sections for the rules.
Rule Group	
Create Rule Group	<p>Rule groups are useful to group the specific type of firewall policy rules or arrange the rules for better view.</p> <p>To create a rule group:</p> <ol style="list-style-type: none"> a. Select any security policy rule and create a Rule Group by selecting More > Rule Group > Create Rule Group. b. Enter the name and description for the rule group. c. Click OK to save the changes.
Move to Rule Group	Move any security policy rule to an existing rule group.
Modify Rule Group	<p>To modify a rule group:</p> <ol style="list-style-type: none"> a. Select the rule group. b. Right click the rule group select Rule Group > Modify Rule Group. c. In the modify rule group page, enter the rule group name and description. d. Click OK to save the changes.
Ungroup Rule	Move out specific security policy rule from the rule group.

Table 137: Common Operations on Security Policy Rules Page (Continued)

Field	Description
Ungroup Rule Group	Ungroup rule group is equivalent to deleting a rule group. To remove a rule group from UI, select the rule group and click More> Rule Group > Ungroup Rule Group .

Deploy Security Policies

After adding the rules to the security policies, you can deploy the security policy by clicking the **Deploy** option. You can also deploy one or more policies from the **Security Policy** page.

To deploy security policies:

1. Select **SRX > Security Policies > Security Policies**.
The Security Policy page appears.
2. Select one or more policies and click **Deploy**.
The Deploy page appears.
3. In **Deployment Time** options, select **Run Now** to deploy the policy immediately. Select **Schedule at a later time** and specify the date and time at which the policy should be deployed.
4. Click **Deploy**. A job is created. Click the job ID to go to the Jobs page and view the status of the deploy operation.

NOTE: During deployment, Juniper Security Director Cloud ensures the order of the zone-based rules and global rules within and across the policies.

Add SRX Policy Rules to Secure Edge Policy (From SRX Policy Page)

To migrate your on-premises security policies to Secure Edge, you must convert the security policy rules to Secure Edge policy. Use the Add SRX policy rules to Secure Edge policy page to add rules from the SRX policy to Secure Edge policy.

The Secure Edge policy supports only a single pair of zones (trust to untrust). All the selected zones of the SRX policy in the source endpoints are converted as trust zone. The destination endpoints are converted as untrust zone.

NOTE: Before initiating the conversion of SRX policy rules to Secure Edge policy, the system administrator must ensure that the source identities referred in the SRX policy rules are in-sync with JIMS Secure Edge source identities. This is to avoid any customization issues at a later stage.

To add the SRX policy rules to Secure Edge policy:

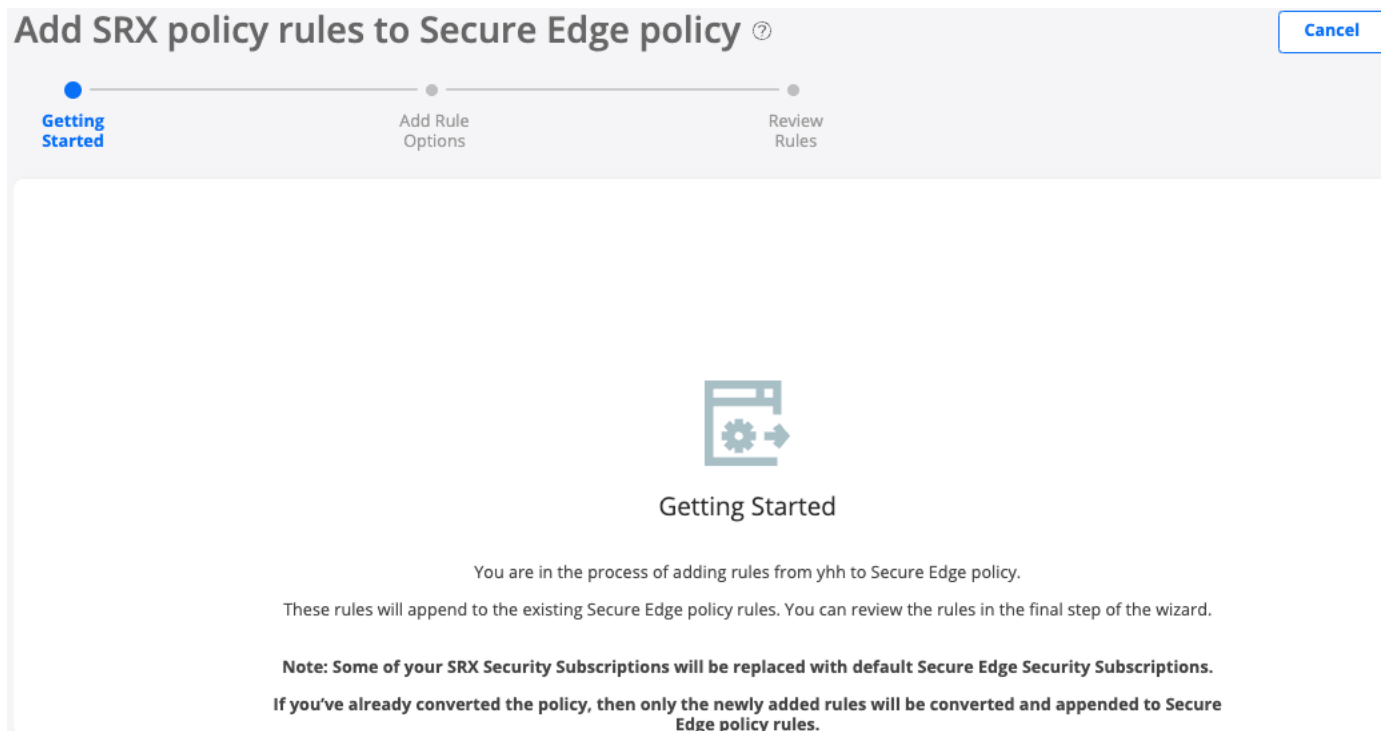
1. Select **SRX > Security Policies > SRX Policy**.

The Security Policies page appears.

2. Select the SRX policy that you want to convert. Right-click or from the More list, select **Add SRX policy rules to Secure Edge policy**.

The Getting Started page provides additional information about adding the SRX policy rules to Secure Edge policy, as shown in [Figure 9 on page 326](#).

Figure 9: Getting Started Page



3. Click **Next**.

4. Complete the configuration as shown in [Table 1 on page 327](#).

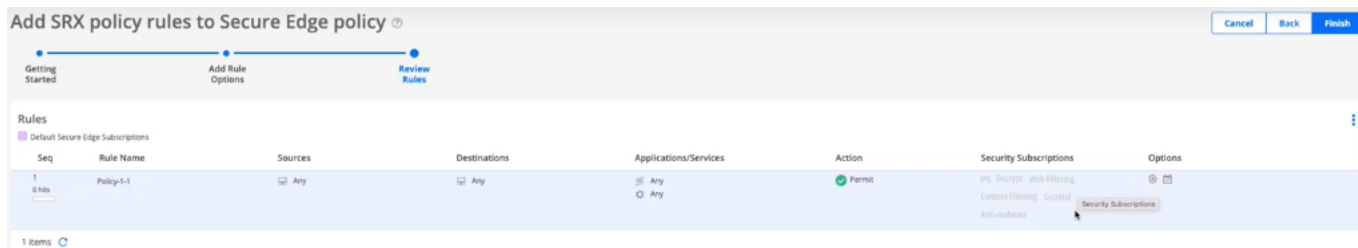
Table 138: Fields on the Add Rule Options page

Field	Description
<i>Add Rule Options</i>	
Name	Name of the SRX policy.
Source (trust) zones	Select zones in the existing rules that are applicable for the Internet. These zones are set as source (trust) zones in the Secure Edge policy rule.
Destination (untrust) zones	Select zones in the existing rules that are applicable for the Internet. These zones are set as destination (untrust) zones in the Secure Edge policy rule.

5. Click **Next**.

The Review Rules Page appears, as shown in [Figure 10 on page 327](#)

Figure 10: Rules Preview Page



6. In the Review Rules page, preview the converted rules.

For the advanced security profiles conversion, Secure Edge policy takes the following actions:

- IPS—Policy is ignored and not converted. Default IPS of Secure Edge policy is associated. For more information, see ["About the IPS Profiles Page" on page 334](#) .
- Content filtering—Policy is ignored and not converted. Default Content filtering profile of Secure Edge policy is associated. For more information, see ["About the Content Filtering Profiles Page" on page 427](#) .
- Decrypt profile—Decrypt profiles are converted as it is except for the root certificate. The root certificate set is converted to Secure Edge with the name "jsec-ssl-proxy-root-cert". The decrypt profile name is prefixed with "jse-".

- Web filtering—Profile is converted and a new Secure Edge Web Filtering profile is created with categories that map to current actions and defaults.
- Antivirus profile—Profile is ignored and not converted.
- Antispam profile—Profile is ignored and not converted.
- SecIntel profile—SecIntel profiles are converted as it is. The profile name is prefixed with “jse-“.
- Anti-malware profiles—SMTP and IMAP Anti-malware profiles are ignored and not converted. HTTP Anti-malware profile is converted as it is. The profile name is prefixed with “jse-“.

7. Click **Finish** after reviewing the rules.

A job is created to add rules to Secure Edge. Once the conversion is successful, you are directly taken to the Secure Edge Policy page under **Secure Edge > Security Policy**. The converted rules are appended at the bottom of the existing Secure Edge policy rules. You can reorder the converted rules. You can perform all the other operations on the converted rules.

Figure 11: Secure Edge Policy Page

Seq	Rule Name	Sources	Destinations	Applications/Services	Action	Security Subscriptions	Options
1	rulewith-headers-user-fa	Any	Any	None	Permit	IPS, Decrypt, Web Filtering, Content Filtering, SecIntel, Anti-malware	
2	Host-53-policy-2-zone-rule_clone	Any	Any	Any	Permit	IPS, Decrypt, Web Filtering, Content Filtering, SecIntel, Anti-malware	
3	Veera-vSR6-53-16-5-1_clone1	Any	Any	Any	Permit	IPS, Decrypt, Web Filtering, Content Filtering, SecIntel, Anti-malware	
4	untrust-trust-rule-max-description	Any	Any	Any	Permit	IPS, Decrypt, Web Filtering, Content Filtering, SecIntel, Anti-malware	
5	Veera-vSR6-53-16-deactivate-ib-rule	Any	Any	Any	Permit	IPS, Decrypt, Web Filtering, Content Filtering, SecIntel, Anti-malware	
6	Zone1-Zone2-webproxy-rule	Any	Any	Any	Permit	IPS, Decrypt, Web Filtering, Content Filtering, SecIntel, Anti-malware	
7	Global-Policy-rules-trust-untrust	Any	Any	Any	Permit	IPS, Decrypt, Web Filtering, Content Filtering, SecIntel, Anti-malware	
8	Global-Policy-rules-trust-untrust_clone	Any	Any	Enhanced, Abused, Drugs	Permit	IPS, Decrypt, Web Filtering, Content Filtering, SecIntel, Anti-malware	
9	Global-Policy-rules-malware-dbl-zone	Any	Any	Any	Redirect	IPS, Decrypt, Web Filtering, Content Filtering, SecIntel, Anti-malware	
10	Policy 1.1	Any	Any	Any	Permit	IPS, Decrypt, Web Filtering, Content Filtering, SecIntel, Anti-malware	

The final step is to deploy the converted policy. Select the policy and click **Deploy**.

NOTE:

- You cannot reconvert SRX policy rules that are already converted to the Secure Edge Policy rules. However, if you have added new rules to that particular SRX policy, only the newly added rules are added to the Secure Edge policy rules.
- Global rules are selected only if they are matched with the selected source and destination zones.

Capture IPS Data Packets of Devices

IN THIS SECTION

- [Configure IPS Rules to Capture IPS Data Packets | 329](#)
- [Configure the IPS Sensor to Capture IPS Data Packets | 330](#)

Configure Juniper Security Director Cloud to capture the IPS data packets of managed SRX Series Firewalls. The configuration involves the following two steps:

- Enabling the logging of IPS packets in the IPS rule associated with the security policy used by the managed devices.
- Configuring the IPS sensor for the devices that are involved in the IPS data packet capture process.

Configure IPS Rules to Capture IPS Data Packets

1. Select **SRX>Security Subscriptions>IPS>IPS Profiles**.

The IPS Profiles page opens.

2. Click the IPS profile name.

The specific IPS profile page opens.

3. Select the IPS rule, click the options icon, and enable **Capture packets**.

4. Click **Advanced**, and complete the configuration according to the guidelines in [Table 139 on page 330](#).

Table 139: Create IPS Rule Settings

Field	Description
Packets before attack	<p>Enter the number of received packets to capture before an attack for further analysis of the attack behavior. The range is from 1 to 255.</p> <p>This field is available only if you enable the Capture packets option.</p>
Packets after attack	<p>Enter the number of received packets to capture after an attack for further analysis of the attack behavior. The range is from 1 to 255.</p> <p>This field is available only if you enable the Capture packets option.</p>
Packet capture timeout	<p>Enter a time limit in seconds for capturing packets received after an attack. No packets are captured after the specified timeout has elapsed. The range is from 1 to 1800 seconds.</p> <p>This field is available only if you enable the Capture packets option.</p>

5. Click ✓ to save your changes.
 - The changes are saved, and a confirmation message is displayed at the top of the page.
 - Capturing data packets for the devices associated with the security policy using IPS rule is enabled.

SEE ALSO

[Create an IPS or an Exempt Rule](#) | 340

Configure the IPS Sensor to Capture IPS Data Packets

1. Select **SRX>Security Policy>SRX Policy**.
The Security Policies page opens.
2. Click **IPS Sensor Settings**.
The IPS Sensor Settings page opens.
3. Select the devices to configure the IPS sensor, and click the edit icon.

The Edit IPS Sensor Settings page opens.

- Complete the configuration according to the guidelines in [Table 140 on page 331](#).

Table 140: Edit IPS Sensor Settings

Setting	Guideline
Devices selected	The devices selected to configure the IPS sensor.
PCAP server	Enter the IP address or host name of the external server.
Source address	Enter the IP address of the source address.
Port number	Enter the port number of the host server where the captured packets are sent.
Maximum sessions	Enter the percentage of the total sessions to include during the packet capture session.
Threshold logging interval	Enter the interval period in minutes between each packet capture session. The range is from 1 to 60 minutes.
Total memory	Enter the percentage of the total memory capacity to use for the packet capture session.

- Click **OK** to save the configuration.

The IPS data packets of the devices configured with the IPS sensor will be captured.

SEE ALSO

| [Create an IPS or an Exempt Rule](#) | 340

SRX Policy-Device View

IN THIS CHAPTER

- [Devices with Security Policies Main Page Fields | 332](#)

Devices with Security Policies Main Page Fields

To access the page, click **SRX > Security Policies > Device View**.

Use this to view detailed information on the number of rules and policies assigned per device. Details help you keep track of the number and order of rules per policy and of all the policies that are assigned to a specific device. You can filter and sort this information to get a better understanding of what you want to view. The following table describes the fields on this page.

Table 141: Devices with Security Policies Main Page Fields

Field	Description
Device Name	Name of the device.

Table 141: Devices with Security Policies Main Page Fields *(Continued)*

Field	Description
Rules	<p>Total number of rules of all the policies assigned to the device. Click the link to view the rules order that are deployed on the device.</p> <p>After clicking the rule number, the page with device name opens. This page displays all the security policies and all the rules associated with each security policy for the device.</p> <p>See Table 123 on page 287 for details about the fields.</p> <p>Use Expand All or Collapse All options to view expanded or collapsed view for all the security policies.</p> <p>You can also search for a specific policy. Click the Search icon in the top right corner of the page to search for a security policy.</p> <p>You can also filter the information based on selected criteria. You can add filters, save the filters, and set any of the filters as default.</p>
Platform	Displays the supported platform. For example: SRX4100 or vSRX Virtual Firewall.
Assigned Policies	List of all assigned security policies. When a device is assigned to any security policy, the policy name is shown in this column.
Installed Policies	List of the security policy names that are deployed to the device.

RELATED DOCUMENTATION

[About the Security Policy Rules Page](#) | 286

Security Subscriptions-IPS

IN THIS CHAPTER

- [About the IPS Profiles Page | 334](#)
- [Create an IPS Profile | 336](#)
- [Edit, Clone, and Delete an IPS Profile | 337](#)
- [About the <IPS-Profile-Name> Page | 339](#)
- [Create an IPS or an Exempt Rule | 340](#)
- [Edit, Clone, and Delete an IPS Rule or an Exempt Rule | 349](#)
- [About the IPS Signatures Page | 351](#)
- [Create an IPS Signature | 358](#)
- [Create an IPS Signature Static Group | 370](#)
- [Create an IPS Signature Dynamic Group | 372](#)
- [Edit, Clone, and Delete an IPS Signature | 380](#)
- [Edit, Clone, and Delete an IPS Signature Static Group | 382](#)
- [Edit, Clone, and Delete an IPS Signature Dynamic Group | 384](#)

About the IPS Profiles Page

IN THIS SECTION

- [Tasks You Can Perform | 335](#)
- [Field Descriptions | 335](#)

To access this page, select **SRX > Security Subscriptions > IPS > IPS Profiles**.

The intrusion prevention system (IPS) profile is deployed on a device by associating the profile with a firewall policy rule, which is deployed on the device. You can associate IPS rules and exempt rules with an IPS profile.

NOTE: Juniper Security Director Cloud supports only IPS Profiles with unified rules. IPS profiles with standard rules are not supported.

Use the IPS Profiles page to manage IPS profiles.

Tasks You Can Perform

- Create an IPS profile—See ["Create an IPS Profile" on page 336](#) .
- Edit, clone, or delete an IPS profile—See ["Edit, Clone, and Delete an IPS Profile" on page 337](#) .
- Manage the IPS rules associated with an IPS profile—Click the *IPS-Profile-Name* to manage the IPS rules associated with the IPS profile. See ["About the <IPS-Profile-Name> Page" on page 339](#) .
- Search for IPS profiles by using keywords—Click the search icon, enter the search term in the text box, and press Enter. The search results are displayed on the same page.
- Sort IPS profiles—Click a column name to sort the data in the grid (table) based on the column name.

NOTE: Sorting is applicable only to some fields.

Field Descriptions

[Table 142 on page 336](#) describes the field on the IPS Profiles page.

Table 142: Fields on the IPS Profiles Page

Field	Description
Policy Name	<p>The name of the IPS profile.</p> <p>Click the <i>IPS-Profile-Name</i> to manage the IPS rules associated with the IPS profile. The <i>IPS-Profile-Name</i> page opens.</p> <p>See "About the <IPS-Profile-Name> Page" on page 339 .</p>
Rules	<p>Indicates the count of rules created in the IPS profile.</p> <p>Click the rule count to manage the IPS rules associated with the IPS profile. The <i>IPS-Profile-Name</i> page opens.</p> <p>See "About the <IPS-Profile-Name> Page" on page 339 .</p>
Predefined / Custom	<p>Indicates whether the IPS profile was system-generated (Predefined) or created by a user (Custom).</p>
Description	<p>The description of the IPS profile.</p>

Create an IPS Profile

Juniper Security Director Cloud contains predefined intrusion prevention system (IPS) profiles. You can create customized IPS profiles from the Create IPS Profile page.

To create a customized IPS profile:

1. Select **SRX > Security Subscriptions > IPS > IPS Profiles**.

The IPS Profiles page opens.

2. Click the add (+) icon.

The Create IPS Profile page opens.

3. Complete the configuration according to the guidelines in [Table 143 on page 337](#) .

NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **OK**.

The IPS Profiles page opens with a confirmation message indicating that the IPS profile is created.

After you create an IPS profile, you can add one or more IPS or exempt rules to the profile, and use the IPS profile in a firewall policy intent.

Table 143: Create IPS Profile Settings

Setting	Guideline
Name	<p>Enter a unique name for the IPS profile that is a string of maximum 127 characters without spaces.</p> <p>The string can contain alphanumeric characters and special characters, such as colons, hyphens, periods, and underscores.</p>
Description	<p>Enter a description of maximum 255 characters for the IPS profile.</p>

Edit, Clone, and Delete an IPS Profile

IN THIS SECTION

- [Edit an IPS Profile | 337](#)
- [Clone an IPS Profile | 338](#)
- [Delete IPS Profiles | 338](#)

Edit an IPS Profile

You can edit only customized IPS profiles, and not predefined (system-generated) profiles.

To edit a customized IPS profile:

1. Select **SRX > Security Subscriptions > IPS > IPS Profiles**.
The IPS Profiles page opens.
2. Select a customized IPS profile, and click the edit (pencil) icon.
The Edit IPS Profile page opens.
3. Modify the IPS profile fields. See ["Create an IPS Profile" on page 336](#) .

NOTE: You cannot modify the IPS profile name.

4. Click **OK** to save your changes.
The IPS Profiles page opens with a message that the IPS profile was successfully updated.

If the IPS profile is referenced in a firewall policy intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.

Clone an IPS Profile

Cloning enables you to easily create a new IPS profile based on an existing one. You can clone predefined or customized IPS profiles and modify the parameters.

To clone an IPS profile:

1. Select **SRX > Security Subscriptions > IPS > IPS Profiles**.
The IPS Profiles page opens.
2. Select an IPS profile and select **More > Clone**.
The Clone IPS Profile page opens.
3. Modify the IPS profile fields. See ["Create an IPS Profile" on page 336](#) .
4. Click **OK** to save your changes.
The IPS Profiles page opens with a message that the IPS profile was successfully created.

Delete IPS Profiles

NOTE: You can delete only customized IPS profiles that are not referenced in a firewall policy intent. You cannot delete predefined (system-generated) IPS profiles.

To delete the customized IPS profiles:

1. Select **SRX > Security Subscriptions > IPS > IPS Profiles**.
The IPS Profiles page opens.
2. Select one or more customized IPS profiles, and click the delete (trash can) icon.
A warning message asking you to confirm the deletion is displayed.

3. Click **Yes** to proceed with the deletion.

The IPS Profiles page opens with a message indicating the status of the delete operation.

About the <IPS-Profile-Name> Page

IN THIS SECTION

- [Tasks You Can Perform | 339](#)
- [Field Descriptions | 340](#)

To access this page, select **SRX > Security Subscriptions > IPS > IPS Profiles > *IPS-Profile-Name***.

The intrusion prevention system (IPS) profile is deployed on a device by associating the profile with a firewall policy intent, which is deployed on the device. You can associate IPS rules or exempt rules with an IPS profile.

Use this page to view, add, modify, clone, or delete the IPS rules and exempt rules in the IPS profiles.

Tasks You Can Perform

- Create an IPS rule—See "[Create an IPS or an Exempt Rule](#)" on page 340 .
- Create an exempt rule—See "[Create an IPS or an Exempt Rule](#)" on page 340 .
- Edit, clone, or delete an IPS rule or an exempt rule—See "[Edit, Clone, and Delete an IPS Rule or an Exempt Rule](#)" on page 349 .
- Search for rules by using keywords—Click the search icon, enter the search term in the text box, and press Enter. The search results are displayed on the same page.
- Filter rules—Click the filter icon (funnel), and specify one or more filtering criteria. The filtered results are displayed on the same page.

NOTE: Filtering is applicable only to some fields.

Field Descriptions

Fields on the <IPS-Profile-Name> Page on page 340 describes the fields on the *IPS-Profile-Name* page.

Table 144: Fields on the <IPS-Profile-Name> Page

Field	Description
Name	The name of the IPS rule or exempt rule.
IPS Signatures	<p>Displays the IPS signatures associated with the IPS rule or exempt rule.</p> <p>If multiple signatures are associated with the rule, the number of additional signatures is displayed. Hover over the number to view the full list of signatures.</p>
Action	Displays the action to be taken when the IPS rule is matched.
Options	<p>Displays the following options for IPS rules:</p> <ul style="list-style-type: none"> • The logging options configured if advance settings (to be taken when the rule is matched) are configured. Hover over the arrow icon to view the logging options configured. • The advance settings configured if advance settings (to be taken when the rule is matched) are configured. Hover over the gear icon to view the advance settings configured.

Create an IPS or an Exempt Rule

IN THIS SECTION

- Create an IPS Rule | 341

You can create intrusion prevention system (IPS) rules or exempt rules only for customized IPS profiles.

Create an IPS Rule

To create an IPS rule:

1. Select **SRX>Security Subscriptions>IPS>IPS Profiles**.

The IPS Profiles page opens.

2. Click ***IPS-Profile-Name***.

The *IPS-Profile-Name* page opens.

3. Click the add (+) icon on the IPS Rules tab.

The parameters for an IPS rule are displayed inline at the top of the page.

4. Complete the configuration according to the guidelines in [Table 145 on page 341](#).

NOTE: Fields marked with an asterisk (*) are mandatory.

5. Click the check mark (✓) to save your changes.

The changes are saved and a confirmation message is displayed at the top of the page.

You can use the IPS profile in a firewall policy intent. When you deploy the firewall policy on the device, the IPS and exempt rules associated with the profile are also deployed.

Table 145: Create IPS Rule Settings

Setting	Guideline
Name	<p>Juniper Security Director Cloud generates a unique rule name by default. You can modify the name.</p> <p>The name must begin with an alphanumeric character and can contain maximum 63 characters, which includes alphanumeric characters and some special characters, such as colons, hyphens, forward slashes, periods, and underscores.</p>

Table 145: Create IPS Rule Settings (Continued)

Setting	Guideline
Description	Enter a description containing maximum 1024 characters for the rule.
IPS Signatures	<p>Add one or more IPS signatures and IPS signature static and dynamic groups to be associated with the rule:</p> <ol style="list-style-type: none"> <li data-bbox="847 632 1424 758">a. Click inside the text box with the + icon. A list of IPS signatures and IPS signature static and dynamic groups opens. <li data-bbox="847 789 1424 852">b. (Optional) Click the add (+) icon to add signatures. The Add IPS Signatures popup window opens. <li data-bbox="847 884 1424 947">c. (Optional) Enter a search term and press Enter to filter the list of items displayed. <li data-bbox="847 978 1424 1083">d. Click a list item to add it to the IPS signatures and IPS signature static or dynamic groups associated with the rule. <li data-bbox="847 1115 1424 1178">e. (Optional) Repeat the preceding step to add more signatures, static groups, and dynamic groups.

Table 145: Create IPS Rule Settings (Continued)

Setting	Guideline
Action	<p>Select the action to be taken when the monitored traffic matches the attack objects specified in the rules:</p> <ul style="list-style-type: none"> • Recommended (default)—Uses the action that Juniper Networks recommends when an attack is detected. All predefined attack objects have a default action associated with the objects. • No action—No action is taken. Use this action to only generate logs for some traffic. • Drop Connection—Drops all packets associated with the connection and prevents traffic for the connection from reaching its destination. Use this action to drop connections for traffic that is not prone to spoofing. • Drop Packet—Drops a matching packet before it can reach its destination but does not close the connection. Use this action to drop packets for attacks in traffic that is prone to spoofing, such as UDP traffic. Dropping a connection for such traffic could result in a denial of service that prevents traffic from a legitimate source IP address. • Close Client—Closes the connection and sends an RST packet to the client, but not to the server. • Close Server—Closes the connection and sends an RST packet to the server, but not to the client. • Close Client and Server—Closes the connection and sends a TCP reset (RST) packet to both the client and the server. • Ignore Connection—Stops scanning traffic for the rest of the connection if an attack match is found. IPS disables the rulebase for the specific connection.

Table 145: Create IPS Rule Settings (Continued)

Setting	Guideline
	<ul style="list-style-type: none"> • Mark DiffServ—Assigns the specified DSCP value to the packet in an attack and pass the packet on normally. When you select Mark DiffServ, the Code point popup is displayed. <ol style="list-style-type: none"> a. In the Code Point field, enter a DSCP value from 0 to 63. b. Click OK. The previous page opens displaying the entered DSCP value.
Options	<p>Enable one or both the following options to create a log:</p> <ul style="list-style-type: none"> • Log attacks—Enable this option to log attacks. You can enable the Alert flag option in the Advanced settings to add an alert flag to an attack log. • Log packets—Enable this option to log packet capture when a rule matches for further offline analysis of attacker behavior. You can configure the number of pre-attack and post-attack packets to be captured for this attack and limit the duration of the post-attack packet capture by specifying a timeout value. You must configure at least one of the Packets Before, Packets After, or Post Window Timeout fields in the Advanced settings.

Table 146: Advanced

Setting	Guideline
Threat Profiling	

Table 146: Advanced *(Continued)*

Setting	Guideline
Add attacker to feed	Add the IP addresses of the attackers to the feed to configure threat profiles in the IPS rule.
Add target to feed	Add the IP addresses of the attack targets to the feed to configure threat profiles in the IPS rule.
Alert Flag	Enable this option to set the alert flag in the attack log.
Packets Before	<p>Enter the number of received packets that must be captured before an attack for further analysis of the attack behavior.</p> <p>The range is from 1 to 255.</p> <p>This field is available only if you enable the Log packets option.</p>
Packets After	<p>Enter the number of received packets after an attack that must be captured for further analysis of attacker behavior.</p> <p>The range is 1 to 255.</p> <p>This field is available only if you enable the Log packets option.</p>
Post Window Timeout	<p>Enter a time limit in seconds for capturing packets received after an attack. No packets are captured after the specified timeout has elapsed.</p> <p>The range is from 1 to 1800 seconds.</p> <p>This field is available only if you enable the Log packets option.</p>
IP Actions	

Table 146: Advanced (Continued)

Setting	Guideline
Action	<p>Select the action to be taken on future connections that use the same IP address:</p> <p>NOTE: If an IP action matches with multiple rules, then the most severe IP action of all the matched rules is applied. In decreasing order of severity, the actions are block, close, and notify.</p> <ul style="list-style-type: none"> • None (default)—Do not take any action. This is similar to not configuring the IP action. • IP Notify—Do not take any action on future traffic but log the event. • IP Close—Close future connections of new sessions that match the IP address by sending RST packets to the client and server. • IP Block—Block future connections of any session that matches the IP address.

Table 146: Advanced (Continued)

Setting	Guideline
IP Target	<p>Select how the traffic must be matched for the configured IP actions:</p> <ul style="list-style-type: none"> • None—Do not match any traffic. • Destination Address—Matches traffic based on the destination IP address of the attack traffic. • Service—For TCP and UDP, matches traffic based on the source IP address, source port, destination IP address, and destination port of the attack traffic. • Source Address—Matches traffic based on the source IP address of the attack traffic. • Source Zone—Matches traffic based on the source zone of the attack traffic. • Source Zone Address—Matches traffic based on the source zone and source IP address of the attack traffic. • Zone Service—Matches traffic based on the source zone, destination IP address, destination port, and protocol of the attack traffic.
Refresh Timeout	<p>Enable this option to refresh the IP action timeout (entered in the Timeout Value field) if future traffic matches the IP actions configured.</p>
Timeout Value	<p>Configure the number of seconds for the IP action to remain in effect.</p> <p>For example, if you configure a timeout of 3600 seconds (1 hour) and the traffic matches the IP actions configured, the IP action remains in effect for 1 hour.</p> <p>The range is from 0 to 64800 seconds.</p>

Table 146: Advanced (Continued)

Setting	Guideline
Log IP-Action hits	Enable this option to log the information about the IP action against the traffic that matches a rule.
Log IP-Action rule creation	Enable this option to generate an event when the IP action filter is triggered.
Rule Modifiers	
Severity override	<p>Select a severity level to override the inherited attack severity in the rules.</p> <p>The most dangerous level is Critical which attempts to crash your server or gain control of your network, while the least dangerous level is Informational which you can use to discover vulnerabilities in your security systems.</p>
Terminal matching	<p>Enable this option to mark the IPS rule as terminal.</p> <p>When a terminal rule is matched, the device stops matching for the rest of the rules in that IPS profile.</p>

Create an Exempt Rule

To create an exempt rule:

1. Select **SRX>Security Subscriptions>IPS>IPS Profiles**.

The IPS Profiles page opens.

2. Click ***IPS-Profile-Name***.

The *IPS-Profile-Name* page opens.

3. Click the add (+) icon on the IPS Rules tab.

The parameters for an exempt rule are displayed inline at the top of the page.

4. You can configure only the following fields:

- Rule Name
- Description

- IPS Signatures

See [Table 145 on page 341](#) for an explanation of these fields.

5. Click **Save** to save your changes.

The changes are saved and a confirmation message is displayed at the top of the page.

You can use the IPS profile in a firewall policy intent. When you deploy the firewall policy on the device, the IPS and exempt rules associated with the profile are also deployed.

Edit, Clone, and Delete an IPS Rule or an Exempt Rule

IN THIS SECTION

- [Edit an IPS Rule or an Exempt Rule | 349](#)
- [Clone an IPS Rule or an Exempt Rule | 350](#)
- [Delete IPS Rules or Exempt Rules | 350](#)

Edit an IPS Rule or an Exempt Rule

You can edit IPS rules and exempt rules associated only with customized IPS profiles, and not the rules associated with predefined (system-generated) profiles.

To edit an IPS or an exempt rule:

1. Select **SRX > Security Subscriptions > IPS > IPS Profiles**.
The IPS Profiles page opens.
2. Click ***IPS-Profile-Name***.
The *IPS-Profile-Name* page opens.
3. Click either the IPS RULES or the EXEMPT RULES tab, then select the IPS rule.
4. Click edit (pencil) icon.
The rule selected for editing is displayed inline at the top of the page.
5. Modify the rule. See "[Create an IPS or an Exempt Rule](#)" on page 340 .

NOTE: You cannot modify the IPS rule or the exempt rule name.

6. Click the check mark (✓) to save your changes.

The changes are saved and a confirmation message is displayed at the top of the page.

If the IPS or exempt rule belongs to an IPS profile that is referenced in a firewall policy intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.

Clone an IPS Rule or an Exempt Rule

Cloning enables you to easily create an IPS or exempt rule based on an existing one. You can clone IPS and exempt rules associated only with customized IPS profiles, and not rules associated with predefined (system-generated) profiles.

To clone an IPS or an exempt rule:

1. Select **SRX > Security Subscriptions > IPS > IPS Profiles**.

The IPS Profiles page opens.

2. Click ***IPS-Profile-Name***.

The *IPS-Profile-Name* page opens.

3. Select a rule, and select **More > Clone**.

The rule selected for cloning is displayed inline at the top of the page.

4. Modify the rule. See "[Create an IPS or an Exempt Rule](#)" on page 340 .

5. Click the check mark (✓) to save your changes.

The new rule is created and a confirmation message is displayed at the top of the page.

Delete IPS Rules or Exempt Rules

You can delete IPS rules and exempt rules associated only with customized IPS profiles, and not the rules associated with predefined (system-generated) profiles.

To delete IPS rules or exempt rules:

1. Select **SRX > Security Subscriptions > IPS > IPS Profiles**.

The IPS Profiles page opens.

2. Click ***IPS-Profile-Name***.

The *IPS-Profile-Name* page opens.

3. Select one or more rules, and click the delete (trash can) icon.

A warning message asking you to confirm the deletion is displayed.

4. Click **Yes**.

A message indicating the status of the delete operation is displayed at the top of the page.

If the deleted IPS rule or exempt rule belongs to an IPS profile that is referenced in a firewall policy intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.

About the IPS Signatures Page

IN THIS SECTION

- [Tasks You Can Perform | 351](#)
- [Field Descriptions | 352](#)

To access this page, select **SRX > Security Subscriptions > IPS > IPS Signature**.

IPS compares traffic against signatures of known threats and blocks traffic when a threat is detected.

Use the IPS Signatures page to monitor and prevent intrusions using the signatures. You can view, create, modify, clone, and delete IPS signatures, IPS signature static groups, and IPS signature dynamic groups. You can delete only the customized IPS signatures, static groups, and dynamic groups that are not used in the IPS or exempt rules.

Tasks You Can Perform

- View the details of an IPS signature—Select an IPS signature and click **More > Detail**, or mouse over the IPS signature, and click the **Detailed View** icon. The IPS Signature Details View page opens. See [Table 148 on page 354](#) for an explanation of fields on this page.
- View the details of an IPS signature static group—Select an IPS signature static group and click **More > Detail**, or mouse over the IPS signature static group, and click the **Detailed View** icon. The IPS Static Group Details page opens. See [Table 149 on page 356](#) for an explanation of fields on this page.
- View the details of an IPS signature dynamic group—Select an IPS signature dynamic group and click **More > Detail**, or mouse over the IPS signature dynamic group, and click the **Detailed View** icon. The IPS Signature Dynamic Details View page opens. See [Table 150 on page 357](#) for an explanation of fields on this page.
- Create an IPS signature—See ["Create an IPS Signature" on page 358](#) .
- Create an IPS signature static group—See ["Create an IPS Signature Static Group" on page 370](#) .
- Create an IPS signature dynamic group—See ["Create an IPS Signature Dynamic Group" on page 372](#) .
- Edit, clone, or delete an IPS signature—See ["Edit, Clone, and Delete an IPS Signature" on page 380](#) .
- Edit, clone, or delete an IPS signature static group—See ["Edit, Clone, and Delete an IPS Signature Static Group" on page 382](#) .

- Edit, clone, or delete an IPS signature dynamic group—See ["Edit, Clone, and Delete an IPS Signature Dynamic Group"](#) on page 384 .
- Search for IPS signatures, static groups, or dynamic groups by using keywords—Click the search icon, enter the search term in the text box, and press Enter. The search results are displayed on the same page.
- Filter IPS signatures, static groups, or dynamic groups—Click the filter icon (funnel) and select one or more filtering criteria. The filtered results are displayed on the same page.
- Sort IPS signatures, static groups, or dynamic groups—Click a column name to sort the data in the grid (table) based on the column name.

NOTE: Sorting is applicable only to some fields.

- Show or hide columns—Click **Show Hide Columns**.

Field Descriptions

[Table 147 on page 352](#) describes the field on the IPS Signatures page.

Table 147: Fields on the IPS Signatures Page

Field	Description
Name	The name of the IPS signature, IPS signature static group, or IPS signature dynamic group.
Severity	The severity level of the attack that the signature reports.
Category	The category of the attack object.
CVE	Displays the Common Vulnerabilities and Exposures (CVE) identifier or name associated with the threat.
CVSS Score	The Common Vulnerability Scoring System (CVSS) score used as a filter for the dynamic group.

Table 147: Fields on the IPS Signatures Page (*Continued*)

Field	Description
Activation Date	The date when the IPS signature was activated.
Type	<p>The type of IPS signature, which include:</p> <ul style="list-style-type: none"> • Static Group • Dynamic Group • Signature • Protocol Anomaly • Compound Attack
Recommended	Indicates whether the attack objects are recommended by Juniper Networks (True) or not (False).
Action	The action taken when the monitored traffic matches the attack objects added in the IPS rules.
Predefined/Custom	Indicates whether the IPS signature, static group, or dynamic group was system-generated (Predefined) or created by a user (Custom).
CERT	Displays the computer emergency response team (CERT) advisory number associated with the threat.
BUG	Displays the list of bugs that are related to the signature attack.
False Positives	Displays the frequency with which the attack produces a false positive on your network.
Service	The protocol or service that the attack uses to enter your network.

Table 147: Fields on the IPS Signatures Page (Continued)

Field	Description
Performance Impact	The performance impact of the IPS signature.
Direction	The direction of the traffic for which the attack is detected, such as client to server.

Table 148: Fields on the IPS Signature Details View Page

Field	Description
General Info	
Name	The name of the IPS signature.
Description	The description of the IPS signature.
URL(s)	Displays the URLs that have the details about the signature attack. For example, http://www.faqs.org/rfcs/rfc2865.html .
Category	The category of the attack object. See Table 147 on page 352 .
Recommended	Indicates whether the attack objects are recommended by Juniper Networks (True) or not (False). See Table 147 on page 352 .
Action	The action taken when the monitored traffic matches the attack objects added in the IPS rules. See Table 147 on page 352 .
Keywords	The keywords associated with the IPS signature.

Table 148: Fields on the IPS Signature Details View Page (*Continued*)

Field	Description
Severity	<p>The severity level of the attack that the signature reports.</p> <p>See Table 147 on page 352 .</p>
BUGS	<p>Displays the list of bugs that are related to the signature attack.</p> <p>See Table 147 on page 352 .</p>
CERT	<p>Displays the computer emergency response team (CERT) advisory number associated with the threat.</p> <p>See Table 147 on page 352 .</p>
CVE	<p>Displays the Common Vulnerabilities and Exposures (CVE) identifier or name associated with the threat.</p> <p>See Table 147 on page 352 .</p>
Signature Details	
Binding	<p>The protocol or service that the attack uses to enter your network.</p>
Service	<p>For service binding, displays the service the attack uses to enter your network.</p>
Time Count	<p>The number of times that IPS detects the attack in a specified time scope.</p>
Match Assurance	<p>The positives filter to track attack objects based on the frequency that the attack produces a false positive on your network.</p>

Table 148: Fields on the IPS Signature Details View Page (*Continued*)

Field	Description
Performance Impact	The performance impact filter used for the IPS signature.
Signature	<p>Displays (in a table) the signature attack objects configured as part of the IPS signature. For each row, the following fields are displayed:</p> <ul style="list-style-type: none"> • No—A unique identifier for the signature attack object. • Context—The attack context, which defines the location of the signature where IPS must look for the attack. • Direction—The connection direction of the attack. • Pattern—The signature pattern (in Juniper Network's proprietary regular expression syntax) of the attack to be detected. • Regex—The regular expression to match malicious or unwanted behavior over the network. • Negated—Indicates whether the pattern must be excluded from being matched (true) or not (false).

Table 149: Fields on the IPS Static Group Details Page

Field	Description
Name	The name of the IPS signature static group.
Description	The description of the IPS signature static group.

Table 149: Fields on the IPS Static Group Details Page (*Continued*)

Field	Description
Group Members	<p>Displays the IPS signatures or IPS signature dynamic groups that are part of the IPS static group.</p> <p>See Table 147 on page 352 for an explanation of the fields in the table.</p> <p>To view the details, select a row, click More > Detail, or mouse over a row, and click the Detailed View icon. Depending on the object type, the IPS Signature Details View page or IPS Signature Dynamic Details View page opens.</p> <p>See Table 148 on page 354 and Table 150 on page 357 for an explanation of the fields on these pages.</p>

Table 150: Fields on the IPS Signature Dynamic Details View Page

Field	Description
Name	The name of the IPS signature dynamic group.
Severity	The severity filters used for the dynamic group.
Service	The service filters used for the dynamic group.
Category	The category filters used for the dynamic group.
Recommended	Indicates whether predefined attack objects recommended by Juniper Networks are added to the dynamic group (true) or not (false).
Excluded	Indicates whether predefined attack objects recommended by Juniper Networks are excluded from the dynamic group (true) or not (false).
Direction	The traffic direction filters used for the dynamic group.

Table 150: Fields on the IPS Signature Dynamic Details View Page (Continued)

Field	Description
Performance Impact	The performance impact filter used for the dynamic group.
False Positive	The false positive filter used for the dynamic group.
Age of Attack	The age of the attack in years used as a filter for the dynamic group.
CVSS Score	The Common Vulnerability Scoring System (CVSS) score used as a filter for the dynamic group.
File Type	The file type of the attack used as a filter for the dynamic group.
Vulnerability Type	The vulnerability type of the attack used as a filter for the dynamic group.
Object Type	The type of the object (anomaly or signature) used as a filter for the dynamic group.
Vendor Description	The vendor or product that the attack belongs to.

Create an IPS Signature

The signature database in Juniper Security Director Cloud contains predefined intrusion prevention system (IPS) signatures.

You can create customized IPS signatures to block newer attacks or unknown attacks from the Create IPS Signature page. You must have the tenant administrator role or a customized role assigned with the appropriate IPS tasks to create customized IPS signatures.

- When you add multiple members in the Signature and Anomaly fields, a chain-type signature is created.

- When you add anomaly details in the Anomaly field, an anomaly-type signature is created.

To create a customized IPS signature:

1. Select **SRX > Security Subscriptions > IPS > IPS Signatures**.

The IPS Signatures page opens.

2. Select **Create > IPS Signature**.

The Create IPS Signature page opens.

3. Complete the configuration according to the guidelines in [Table 151 on page 359](#).

NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **OK**.

The IPS Signatures page opens with a message indicating that the signature is created.

You can use the new IPS signature in an IPS rule or an exempt rule. You can then reference the IPS profile containing the rule in a firewall policy, which you can deploy on a device.

Table 151: Create IPS Signature Settings

Setting	Guideline
Name	<p>Enter a unique name for the IPS signature that is a string of maximum 60 characters without spaces.</p> <p>The string can contain alphanumeric characters and special characters, such as colons, hyphens, periods, and underscores.</p>
Description	<p>Enter a description of maximum 1024 characters for the IPS signature.</p>
Category	<p>Enter a predefined category or a new category of maximum 63 characters without spaces.</p> <p>The category must begin with an alphanumeric character and can contain special characters, such as hyphens and underscores.</p> <p>You can use categories to group attack objects. Within each category, you can assign severity levels to the groups of attack objects.</p>

Table 151: Create IPS Signature Settings (Continued)

Setting	Guideline
Action	<p>Select the action to take when the monitored traffic matches the attack objects specified in the IPS rule:</p> <ul style="list-style-type: none"> • None—No action is taken. Use this action to only generate logs for some traffic. • Close Client & Server—Closes the connection and sends a TCP reset (RST) packet to both the client and the server. • Close Client—Closes the connection and sends an RST packet to the client, but not to the server. • Close Server—Closes the connection and sends an RST packet to the server, but not to the client. • Ignore—Stops scanning traffic for the rest of the connection if an attack match is found. IPS disables the rulebase for the specific connection. • Drop—Drops all packets associated with the connection, preventing traffic for the connection from reaching its destination. Use this action to drop connections for traffic that is not prone to spoofing. • Drop Packet—Drops a matching packet before it can reach its destination but does not close the connection. Use this action to drop packets for attacks in traffic that is prone to spoofing, such as UDP traffic. Dropping a connection for such traffic could result in a denial of service that prevents traffic from a legitimate source IP address.
Keyword	<p>Enter unique identifiers that can be used to search and to sort signatures.</p> <p>The keywords must relate to the attack and the attack object. For example, Amanda Amindexd Remote Overflow.</p>

Table 151: Create IPS Signature Settings (*Continued*)

Setting	Guideline
Severity	<p>Select a severity level for the attack that the signature will report:</p> <ul style="list-style-type: none"> • Critical—Contains attack objects matching the exploits that attempt to evade detection, cause a network device to crash, or gain system-level privileges. • Major—Contains attack objects matching the exploits that attempt to disrupt a service, gain user-level access to a network device, or activate a Trojan horse previously loaded on a device. • Minor—Contains attack objects matching the exploits that detect reconnaissance efforts attempting to access vital information through directory traversal or information leaks. • Warning—Contains attack objects matching the exploits that attempt to obtain noncritical information or scan a network with a scanning tool. • Info—Contains attack objects matching normal, harmless traffic containing URLs, DNS lookup failures, SNMP public community strings, and peer-to-peer (P2P) parameters. You can use informational attack objects to get information about your network.
Signature Details	

Table 151: Create IPS Signature Settings (Continued)

Setting	Guideline
Binding	<p>Select the protocol or service that the attack uses to enter your network:</p> <ul style="list-style-type: none"> • IP—Matches the attack for a specified protocol type number, which you must enter in the Protocol field. • IPv6—Matches the attack for a specified protocol type number for the header following the IPv6 header, which you must enter in the Next Header field. • TCP—Matches the attack for the specified TCP ports or port ranges, which you must enter in the Port Range(s) field. • UDP—Matches the attack for the specified UDP ports or port ranges. • ICMP—Matches the attack for ICMP packets. • ICMPv6—Matches the attack for ICMPv6 packets. • RPC—Matches the attack for a specified remote procedure call (RPC) program number, which you must enter in the Program Number field. • Service—Matches the attack for a specified service, which you must select from the Service field.
Protocol	<p>For IP binding, enter the transport layer protocol number to match with the attack.</p> <p>The range is from 1 to 139 excluding 1, 6, and 17.</p>
Next Header	<p>For IPv6 binding, enter the transport layer protocol number for the next header following the IPv6 header with which to match the attack.</p> <p>The range is from 1 to 139 excluding 6, 17, and 58.</p>

Table 151: Create IPS Signature Settings (Continued)

Setting	Guideline
Port Range(s)	<p>For the TCP or UDP binding, enter a port number or a port range to match with the attack.</p> <p>Enter the port range in the min port no.-max port no. format.</p>
Program Number	For RPC binding, enter the RPC program number (ID) to match with the attack.
Service	For service binding, select the service to match with the attack.
Time Count	Enter the number of times an IPS detects the attack within the specified time scope before triggering an event.
Time Scope	<p>Enter the scope within which the counting of the attack occurs:</p> <ul style="list-style-type: none"> • Source IP—Detects attacks from the source IP address for the specified time count regardless of the destination IP address. • Dest IP—Detects attacks from the destination IP address for the specified time count regardless of the source IP address. • Peer—Detects attacks between the source and the destination IP addresses of the sessions for the specified time count.

Table 151: Create IPS Signature Settings (Continued)

Setting	Guideline
Match Assurance	<p>Select a false positives filter to track attack objects based on the frequency that the attack produces a false positive on your network:</p> <ul style="list-style-type: none"> • None—No false positive filter is applied. • High—Provides information on the frequently-tracked false positive occurrences. • Medium—Provides information on the occasionally-tracked false positive occurrences. • Low—Provides information on the rarely-tracked false positive occurrences.
Performance Impact	<p>Select appropriate attacks based on performance impact. For example, to filter out slow-performing attack objects:</p> <ul style="list-style-type: none"> • None—No filter is applied. • Low—Add low-performance impact attack objects that are vulnerable to an attack. The performance impact of signatures is Low1 to Low3 where the application identification is faster. • Medium—Add medium-performance impact attack objects that are vulnerable to an attack. The performance impact of signatures is Medium4 to Medium6 where the application identification is normal. • High—Add high-performance impact attack objects that are vulnerable to an attack. The performance impact of signatures is High7 to High9 where the application identification is slow.

Table 151: Create IPS Signature Settings (Continued)

Setting	Guideline
Add Signature	<p>You can add one or more signature attack objects that use a stateful attack signature (a pattern that always exists within a specific section of the attack) to detect known attacks.</p> <p>NOTE: For a customized IPS signature, you must add at least one signature attack object or anomaly.</p> <ul style="list-style-type: none"> • To add a signature attack object: <ul style="list-style-type: none"> a. Click the add (+) icon. The Add Signature page opens. b. Complete the configuration according to the guidelines in Table 152 on page 368. c. Click OK. The previous page opens and the signature attack object is displayed in the table. • To modify a signature attack object: <ul style="list-style-type: none"> a. Select an attack object and click the edit (pencil) icon. The Edit Signature page opens. b. Modify the fields. See Table 152 on page 368. c. Click OK. Your modifications are saved and the previous page opens. • To delete a signature attack object: <ul style="list-style-type: none"> a. Select an attack object and click the delete (trash can) icon. A popup appears asking you to confirm the delete operation.

Table 151: Create IPS Signature Settings *(Continued)*

Setting	Guideline
	<p data-bbox="894 359 1029 386">b. Click Yes.</p> <p data-bbox="927 422 1409 485">The signature attack object is deleted and the previous page opens.</p>

Table 151: Create IPS Signature Settings (Continued)

Setting	Guideline
Add Anomaly	<p>Select an option to detect abnormal or ambiguous messages within a connection according to the set of rules for the particular protocol being used.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • The Add Anomaly field is displayed only if you select Service in the Binding field. • For a customized IPS signature, you must add at least one signature attack object or anomaly. <p>You can add, modify, or delete anomaly attack objects:</p> <ul style="list-style-type: none"> • To add an anomaly: <ul style="list-style-type: none"> a. Click the add (+) icon. <p>The Add Anomaly page opens.</p> b. Complete the configuration according to the guidelines in Table 153 on page 369. c. Click OK. <p>The previous page opens and the anomaly is displayed in the table.</p> • To modify an anomaly: <ul style="list-style-type: none"> a. Select an anomaly, and click the edit (pencil) icon. <p>The Edit Anomaly page opens.</p> b. Modify the fields as needed. See Table 153 on page 369. c. Click OK. <p>Your modifications are saved and the previous page opens.</p> • To delete an anomaly:

Table 151: Create IPS Signature Settings (Continued)

Setting	Guideline
	<p>a. Select an anomaly and click the delete (trash can) icon.</p> <p>A popup opens asking you to confirm the delete operation.</p> <p>b. Click Yes.</p> <p>The signature anomaly is deleted and the previous page opens.</p>

Table 152: Add Signature Settings

Setting	Guideline
Signature No.	<p>Displays the system-generated signature number.</p> <p>You cannot modify this field.</p>
Context	<p>Select the attack context, which defines the location of the signature where IPS must look for the attack in a specific Application Layer protocol.</p>
Direction	<p>Select the connection direction of the attack:</p> <ul style="list-style-type: none"> • Any—Detects the attack for traffic in either direction. • Client to Server—Detects the attack only in the client to server traffic. • Server to Client—Detects the attack only in the server to client traffic.

Table 152: Add Signature Settings (Continued)

Setting	Guideline
Pattern	<p>Enter the signature pattern (in Juniper Networks proprietary regular expression syntax) of the attack to detect.</p> <p>An attack pattern can be a segment of code, a URL, or a value in a packet header and the signature pattern is the syntactical expression that represents the attack pattern.</p> <p>For example, use <code>\[<character-set>\]</code> for case-insensitive matches.</p>
Regex	<p>Enter a regular expression to define rules to match malicious or unwanted behavior over the network.</p> <p>For example, for the syntax <code>\[hello\]</code>, the expected pattern is hello, which is case sensitive. The example matches can be hElLo, HEllO, and heLLo.</p>
Negated	<p>Select this check box to exclude the specified pattern from being matched.</p> <p>When you negate a pattern, the attack is considered matched if the pattern defined in the attack does not match the specified pattern.</p>

Table 153: Add Anomaly Settings

Setting	Guideline
Anomaly No.	<p>Displays the system-generated anomaly number.</p> <p>You cannot modify this field.</p>
Anomaly	<p>Select the protocol (service) whose anomaly is being defined in the attack.</p>

Table 153: Add Anomaly Settings (Continued)

Setting	Guideline
Direction	<p>Select the connection direction of the attack:</p> <ul style="list-style-type: none"> • Any—Detects the attack for traffic in either direction. • Client to Server—Detects the attack only in the client to server traffic. • Server to Client—Detects the attack only in server to client traffic.

Create an IPS Signature Static Group

The signature database in Juniper Security Director Cloud contains predefined intrusion prevention system (IPS) signature static groups.

You can create customized IPS signature static groups from the Create IPS Signature Static Group page. You must have the tenant administrator role or a custom role assigned with the appropriate IPS tasks to create customized IPS signature static groups.

Static groups enable better manageability because you can group different types of signatures into one entity.

To create a customized IPS signature static group:

1. Select **SRX > Security Subscriptions > IPS > IPS Signatures**.

The IPS Signatures page opens.

2. Select **Create > Static Group**.

The Create IPS Signature Static Group page opens.

3. Complete the configuration according to the guidelines in [Table 154 on page 371](#).

NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **OK**.

The IPS Signatures page opens with a message that the static group was successfully created.

You can use the new IPS signature static group in an IPS rule or an exempt rule. You can then reference the IPS profile containing the rule in a firewall policy, which you can deploy on the device.

Table 154: Create IPS Signature Static Group Settings

Setting	Guideline
Name	<p>Enter a unique name for the IPS signature static group that is a string of maximum 127 characters without spaces.</p> <p>The string can contain alphanumeric characters and special characters, such as colons, hyphens, periods, and underscores.</p>
Description	<p>Enter a description of maximum 1024 characters for the IPS signature static group.</p>

Table 154: Create IPS Signature Static Group Settings (*Continued*)

Setting	Guideline
Group Members	<p>Add one or more IPS signatures, static groups, or dynamic groups as members of the new static group.</p> <p>NOTE: You must add at least one IPS signature, static group, or dynamic group to proceed.</p> <ul style="list-style-type: none"> • To add group members: <ul style="list-style-type: none"> a. Click the add (+) icon. <p>The Add IPS Signatures page opens displaying the existing predefined and customized IPS signatures, static groups, and dynamic groups in a table.</p> b. Select one or more group members by clicking the check boxes corresponding to the rows. c. Click OK. <p>The previous page opens and the selected group members are displayed in the table.</p> • To delete group members: <ul style="list-style-type: none"> a. Select the group members to delete, and click the delete (trash can) icon. <p>A warning message asking you to confirm the deletion is displayed.</p> b. Click Yes. <p>The group members are deleted.</p>

Create an IPS Signature Dynamic Group

The signature database in Juniper Security Director Cloud contains predefined intrusion prevention system (IPS) signature dynamic groups.

You can create customized IPS signature dynamic groups based on a specific filter criteria from the Create IPS Signature Dynamic Group page. You must have the tenant administrator role or a custom role with the appropriate IPS tasks to create customized IPS signature dynamic groups.

The specified filter criteria are matched only to predefined or customized IPS signatures, and not to IPS static groups and dynamic groups. When a new signature database is used, the dynamic group membership is automatically updated based on the filter criteria for the group.

To create a customized IPS signature dynamic group:

1. Select **SRX > Security Subscriptions > IPS > IPS Signatures**.

The IPS Signatures page opens.

2. Select **Create > Dynamic Group**.

The Create IPS Signature Dynamic Group page opens.

3. Complete the configuration according to the guidelines in [Table 155 on page 373](#).

4. (Optional) Click **Preview Filtered Signatures** to check whether the signatures that match the dynamic group are consistent with the specified filter criteria.

The IPS Signatures page opens displaying the list of IPS signatures matching the filters.

If the signatures do not match, you can tweak the filter criteria. Click **Close** to go back to the previous page.

5. Click **OK**.

The IPS Signatures page opens with a message indicating that the dynamic group was successfully created.

You can use the new IPS signature dynamic group in an IPS rule or an exempt rule. You can then reference the IPS profile containing the rule in a firewall policy, which you can deploy on the device.

Table 155: Create IPS Signature Dynamic Group Settings

Setting	Guideline
Name	<p>Enter a unique name for the IPS signature dynamic group that is a string of maximum 255 characters without spaces.</p> <p>The string can contain alphanumeric characters and special characters, such as colons, hyphens, periods, and underscores.</p>

Table 155: Create IPS Signature Dynamic Group Settings (Continued)

Setting	Guideline
Filter Criteria	<p>Select one or more filters to define the attributes of IPS signatures that will be added to the new IPS signature dynamic group.</p> <p>Filters apply to existing signatures (already downloaded in the application) and to new signatures when the signatures are downloaded.</p> <p>IPS signatures that match any of the configured filters are included as part of the signature group.</p>
Severity	
Info	Enable this option to include IPS signatures with the Info severity level.
Warning	Enable this option to include IPS signatures with the Warning severity level.
Minor	Enable this option to include IPS signatures with the Minor severity level.
Major	Enable this option to include IPS signatures with the Major severity level.
Critical	Enable this option to include IPS signatures with the Critical severity level.
Service	

Table 155: Create IPS Signature Dynamic Group Settings (Continued)

Setting	Guideline
Service	<p>Select the services to filter IPS signatures that must be included as part of the dynamic group.</p> <p>Select one or more services listed in the Available column, and click the forward arrow to confirm your selection. The selected services are displayed in the Selected column.</p>
Category	
Category	<p>Select the categories to filter IPS signatures that must be included as part of the dynamic group.</p> <p>Select one or more categories listed in the Available column, and click the forward arrow to confirm your selection. The selected categories are displayed in the Selected column.</p>
Recommended	
Recommended	<p>This filter is based on attack objects that are recommended by Juniper Networks. Select one of the following:</p> <ul style="list-style-type: none"> • None—Do not use this filter. • Yes—Add predefined attacks recommended by Juniper Networks to the dynamic group. • No—Add predefined attacks that are not recommended by Juniper Networks to the dynamic group.
Direction	<p>Add IPS signatures to the dynamic group based on the traffic direction of the attacks.</p> <p>If you select more than one traffic direction (Any, Client-to-Server, and Server-to-Client), you must select a value in the Expression field.</p>

Table 155: Create IPS Signature Dynamic Group Settings (*Continued*)

Setting	Guideline
Any	<p>Select one of the following:</p> <ul style="list-style-type: none"> • None (default): Do not use this filter. • Yes: Include IPS signatures that track traffic from client to server or server to client. • No: Do not include IPS signatures that track traffic from client to server or server to client.
Client-to-Server	<p>Select one of the following:</p> <ul style="list-style-type: none"> • None (default): Do not use this filter. • Yes: Include IPS signatures that track traffic from client to server. • No: Do not include IPS signatures that track traffic from client to server.
Server-to-Client	<p>Select one of the following:.</p> <ul style="list-style-type: none"> • None (default): Do not use this filter. • Yes: Include IPS signatures that track traffic from server to client. • No: Do not include IPS signatures that track traffic from server to client.
Expression	<p>If you select more than one traffic directional filter, you must select how the signatures must be matched:</p> <ul style="list-style-type: none"> • None (default): Do not use this filter. • OR—Include signatures that match any of the specified traffic directions. • AND—Include signatures that match all of the specified traffic directions.

Table 155: Create IPS Signature Dynamic Group Settings (*Continued*)

Setting	Guideline
Performance Impact	
Unknown	Enable this option to include the IPS signatures with the Unknown performance impact.
Slow	Enable this option to include the IPS signatures with the Slow performance impact.
Normal	Enable this option to include the IPS signatures with the Normal performance impact.
Fast	Enable this option to include the IPS signatures with the Fast performance impact.
False Positives	
Unknown	Enable this option to include the IPS signatures with the Unknown match assurance.
Low	Enable this option to include the IPS signatures with the Low match assurance.
Medium	Enable this option to include the IPS signatures with the Medium match assurance.
High	Enable this option to include the IPS signatures with the High match assurance.
Age of Attack	The age of the attack in years to be used as a filter criteria to include IPS signatures as part of the dynamic group.

Table 155: Create IPS Signature Dynamic Group Settings (*Continued*)

Setting	Guideline
Greater Than	<p>Enter the age of attack in years to include the IPS signatures with the age of attack greater than the specified value as part of the dynamic group.</p> <p>The range is from 1 to 100 years.</p>
Less Than	<p>Enter the age of attack in years to include the IPS signatures with the age of attack less than the specified value as part of the dynamic group.</p> <p>The range is from 1 to 100 years.</p>
CVSS Score	<p>The Common Vulnerability Scoring System (CVSS) to be used as a filter criteria to include IPS signatures as part of the dynamic group.</p>
Greater Than	<p>Enter the CVSS score to include the IPS signatures with the score greater than the specified value as part of the dynamic group.</p> <p>The range is a decimal number between 0 and 10.</p>
Less Than	<p>Enter the CVSS score to include the IPS signatures with the score less than the specified value as part of the dynamic group.</p> <p>The range is a decimal number between 0 and 10.</p>
Other Filters	

Table 155: Create IPS Signature Dynamic Group Settings (*Continued*)

Setting	Guideline
Excluded	<p>Select one of the following:.</p> <ul style="list-style-type: none"> • None (default): Do not use this filter. • Yes: Include excluded attack objects as part of the dynamic group. • No: Do not include excluded attack objects as part of the dynamic group.
File Type	<p>Select the file type of the attack to be used as a filter criteria.</p> <p>For example, flash.</p>
Vulnerability Type	<p>Select the vulnerability type of the attack to be used as a filter criteria.</p> <p>For example, overflow.</p>
Type	<p>Use this filter to group attack objects by type (anomaly or signature).</p>
Signature	<p>Enable this option to add signatures based on stateful signature attack objects specified in the signature.</p> <p>A stateful attack signature is a pattern that always exists within a specific section of the attack. Stateful signature attack objects also include the protocol or service used to perpetrate the attack and the context in which the attack occurs.</p>
Protocol Anomaly	<p>Enable this option to add signatures of attacks that violate protocol specifications (RFCs and common RFC extensions).</p>
Vendor Description	

Table 155: Create IPS Signature Dynamic Group Settings (Continued)

Setting	Guideline
Product Type	Select this filter to include signatures belonging to the selected product type.
Vendor Name	Select this filter to include signatures belonging to the selected vendor.
Title	Select this filter to include signatures belonging to the selected product name. The product names are populated only when you select a product type and a vendor.

Edit, Clone, and Delete an IPS Signature

IN THIS SECTION

- [Edit an IPS Signature | 380](#)
- [Clone an IPS Signature | 381](#)
- [Delete IPS Signatures | 381](#)

You must have the tenant administrator role or a customized role assigned with the appropriate IPS tasks to modify customized IPS signatures.

Edit an IPS Signature

You can edit only customized IPS signatures and not predefined (system-generated) signatures.

To edit a customized IPS signature:

1. Select **SRX > Security Subscriptions > IPS > IPS Signatures**.

The IPS Signatures page opens.

2. Select a customized IPS signature, and click the edit (pencil) icon.

The Edit IPS Signature page opens.

3. Modify the IPS signature fields. See ["Create an IPS Signature" on page 358](#) .

NOTE: You cannot modify the name of the IPS signature.

4. Click **OK** to save your changes.

The IPS Signatures page opens with a message that the IPS signature was successfully updated.

If the IPS signature was used in an IPS rule or exempt rule that is deployed on the device through the firewall policy, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.

Clone an IPS Signature

Cloning enables you to easily create an IPS signature based on an existing one. You can clone predefined or customized IPS signatures and modify the parameters.

To clone an IPS signature:

1. Select **SRX > Security Subscriptions > IPS > IPS Signatures**.

The IPS Signatures page opens.

2. Select an IPS signature, and select **More > Clone**.

The Clone IPS Signature page opens.

3. Modify the IPS signature fields. See ["Create an IPS Signature" on page 358](#) .

4. Click **OK** to save your changes.

The IPS Signatures page opens with a message that the IPS signature was successfully created.

You can use the cloned IPS signature in an IPS rule or an exempt rule. You can then reference the IPS profile containing the rule in a firewall policy, which you can deploy on the device.

Delete IPS Signatures

NOTE: You can delete only customized (user-created) IPS signatures that are not used in an IPS or exempt rule. You cannot delete predefined (system-generated) IPS signatures.

To delete the customized IPS signatures:

1. Select **SRX > Security Subscriptions > IPS > IPS Signatures**.

The IPS Signatures page opens.

2. Select one or more customized IPS signatures, and click the delete (trash can) icon.

A warning message asking you to confirm the deletion is displayed.

3. Click **Yes**.

The IPS Signatures page opens with a message indicating the status of the delete operation.

Edit, Clone, and Delete an IPS Signature Static Group

IN THIS SECTION

- [Edit an IPS Signature Static Group | 382](#)
- [Clone an IPS Signature Static Group | 383](#)
- [Delete IPS Signature Static Groups | 383](#)

You must have the tenant administrator role or a customized role assigned with the appropriate IPS tasks to modify customized IPS signature static groups.

Edit an IPS Signature Static Group

You can edit only customized IPS signature static groups, and not predefined (system-generated) static groups.

To edit a customized IPS signature static group:

1. Select **SRX > Security Subscriptions > IPS > IPS Signatures**.

The IPS Signatures page opens.

2. Select a customized IPS signature static group, and click the edit (pencil) icon.

The Edit IPS Signature Static Group page opens.

3. Modify the IPS signature static group fields. See "[Create an IPS Signature Static Group](#)" on page 370 .

NOTE: You cannot modify the IPS signature static group name.

4. Click **OK** to save your changes.

The IPS Signatures page opens with a message that the IPS signature static group was successfully updated.

If the IPS signature static group was used in an IPS rule or exempt rule that is deployed on the device through the firewall policy, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.

Clone an IPS Signature Static Group

Cloning enables you to easily create an IPS signature static group based on an existing one. You can clone predefined or customized IPS signature static groups and modify the parameters.

To clone an IPS signature static group:

1. Select **SRX > Security Subscriptions > IPS > IPS Signatures**.

The IPS Signatures page opens.

2. Select an IPS signature static group, and select **More > Clone**.

The Clone IPS Signature Static Group page opens.

3. Modify the IPS signature static group fields. See "[Create an IPS Signature Static Group](#)" on page 370 .

4. Click **OK** to save your changes.

The IPS Signatures page opens with a message that the IPS signature static group was successfully created.

You can use the cloned IPS signature static group in an IPS rule or an exempt rule. You can then reference the IPS profile containing the rule in a firewall policy, which you can deploy on the device.

Delete IPS Signature Static Groups

NOTE: You can delete only customized (user-created) IPS signature static groups that are not used in an IPS or exempt rule. You cannot delete predefined (system-generated) IPS signature static groups.

To delete the customized IPS signature static groups:

1. Select **SRX > Security Subscriptions > IPS > IPS Signatures**.

The IPS Signatures page opens.

2. Select one or more customized IPS signature static groups, and click the delete (trash can) icon.

A warning message asking you to confirm the deletion is displayed.

3. Click **Yes**.

The IPS Signatures page opens with a message indicating the status of the delete operation.

Edit, Clone, and Delete an IPS Signature Dynamic Group

IN THIS SECTION

- [Edit an IPS Signature Dynamic Group | 384](#)
- [Clone IPS Signature Dynamic Groups | 385](#)
- [Delete IPS Signature Dynamic Groups | 385](#)

You must have the tenant administrator role or a customized role assigned with the appropriate IPS tasks to modify customized IPS signature dynamic groups.

Edit an IPS Signature Dynamic Group

You can edit only customized IPS signature dynamic groups, and not predefined (system-generated) dynamic groups.

To edit a customized IPS signature dynamic group:

1. Select **SRX > Security Subscriptions > IPS > IPS Signatures**.

The IPS Signatures page opens.

2. Select a customized IPS signature dynamic group, and click the edit (pencil) icon.

The Edit IPS Signature Dynamic Group page opens.

3. Modify the IPS signature dynamic group fields. See "[Create an IPS Signature Dynamic Group](#)" on [page 372](#).

NOTE: You cannot modify the IPS signature dynamic group name.

4. (Optional) Click **Preview Filtered Signatures** to check if the signatures that match the dynamic group are consistent with the specified filter criteria.

The IPS Signatures page opens displaying the list of IPS signatures matching the filters. If the signatures do not match, you can tweak the filter criteria. Click **Close** to go back to the previous page.

5. Click **OK** to save your changes.

The IPS Signatures page opens with a message indicating that the IPS signature dynamic group was successfully updated.

If the IPS signature dynamic group was used in an IPS rule or exempt rule that is deployed on the device through the firewall policy, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.

Clone IPS Signature Dynamic Groups

Cloning enables you to easily create an IPS signature dynamic group based on an existing one. You can clone predefined or customized IPS signature dynamic groups and modify the parameters.

To clone an IPS signature dynamic group:

1. Select **SRX > Security Subscriptions > IPS > IPS Signatures**.

The IPS Signatures page opens.

2. Select an IPS signature dynamic group, and select **More > Clone**.

The Clone IPS Signature Dynamic Group page opens.

3. Modify the IPS signature dynamic group fields. See ["Create an IPS Signature Dynamic Group" on page 372](#).

4. (Optional) Click **Preview Filtered Signatures** to check if the signatures that match the dynamic group are consistent with the specified filter criteria.

The IPS Signatures page opens displaying the list of IPS signatures matching the filters. If the signatures do not match, you can tweak the filter criteria. Click **Close** to go back to the previous page.

5. Click **OK** to save your changes.

The IPS Signatures page opens with a message that the IPS signature dynamic group was successfully created.

You can use the cloned IPS signature dynamic group in an IPS rule or an exempt rule. You can then reference the IPS profile containing the rule in a firewall policy, which you can deploy on the device.

Delete IPS Signature Dynamic Groups

NOTE: You can delete only customized (user-created) IPS signature dynamic groups that are not used in an IPS or exempt rule. You cannot delete predefined (system-generated) IPS signature dynamic groups.

To delete the customized IPS signature dynamic groups:

1. Select **SRX > Security Subscriptions > IPS > IPS Signatures**.

The IPS Signatures page opens.

2. Select one or more customized IPS signature dynamic groups, and click the delete (trash can) icon.

A warning message asking you to confirm the deletion is displayed.

3. Click **Yes**.

The IPS Signatures page opens with a message indicating the status of the delete operation.

Security Subscriptions-Content Security

IN THIS CHAPTER

- [Content Security Overview | 387](#)
- [Configure the Content Security Settings | 389](#)
- [About the Content Security Profiles Page | 391](#)
- [Create a Content Security Profile | 395](#)
- [Edit, Clone, and Delete a Content Security Profile | 399](#)
- [About the Web Filtering Profiles Page | 401](#)
- [Create a Web Filtering Profile | 405](#)
- [Edit, Clone, and Delete a Web Filtering Profile | 413](#)
- [About the Antivirus Profiles Page | 415](#)
- [Create an Antivirus Profile | 417](#)
- [Edit, Clone, and Delete an Antivirus Profile | 420](#)
- [About the Antispam Profiles Page | 422](#)
- [Create an Antispam Profile | 424](#)
- [Edit, Clone, and Delete an Antispam Profile | 426](#)
- [About the Content Filtering Profiles Page | 427](#)
- [Create a Content Filtering Profile | 430](#)
- [Edit, Clone, and Delete a Content Filtering Profile | 434](#)
- [About the Content Filtering Policy \(New\) Page | 435](#)
- [Create a Content Filtering Policy | 436](#)
- [Add Rules in a Content Filtering Policy | 437](#)
- [Edit a Content Filtering Policy | 438](#)
- [Clone a Content Filtering Policy | 438](#)
- [Edit a Content Filtering Policy Rule | 439](#)
- [Clone a Content Filtering Policy Rule | 439](#)

Content Security Overview

IN THIS SECTION

- [Content Security Licensing | 388](#)
- [Content Security Components | 388](#)

Content security is a term used to describe the consolidation of several security features to protect against multiple threat types. The advantage of content security is a streamlined installation and management of multiple security capabilities.

NOTE: In Junos CLI commands, we continue to use the legacy term UTM for content security.

The following security features are provided as part of the content security solution:

- **Antispam**—This feature examines transmitted messages to identify e-mail spam. E-mail spam consists of unwanted messages usually sent by commercial, malicious, or fraudulent entities. When the device detects an e-mail message deemed to be spam, it either drops the message or tags the message header or subject field with a preprogrammed string. The antispam feature uses a constantly updated Spamhaus Block List (SBL). Sophos updates and maintains the IP-based SBL.
- **Full file-based antivirus**—A virus is an executable code that infects or attaches itself to other executable code to reproduce itself. Some malicious viruses erase files or lock up systems. Other viruses merely infect files and overwhelm the target host or network with bogus data. The full file-based antivirus feature provides file-based scanning on specific *application layer* traffic, checking for viruses against a virus signature database. The antivirus feature collects the received data packets until it has reconstructed the original application content, such as an e-mail file attachment, and then scans this content.
- **Express antivirus**—Express antivirus scanning is offered as a less CPU-intensive alternative to the full file-based antivirus feature. The express antivirus feature is similar to the antivirus feature in that it scans specific application layer traffic for viruses against a virus signature database. However, unlike full antivirus, express antivirus does not reconstruct the original application content. Rather, it just sends (streams) the received data packets, as is, to the scan engine. With express antivirus, the virus scanning is executed by a hardware pattern-matching engine. This improves performance while scanning is occurring, but the level of security provided is lessened. Juniper Networks provides the scan engine.

- Content filtering—Content filtering blocks or permits certain types of traffic based on the MIME type, file extension, protocol command, and embedded object type.
- Web filtering—Web filtering enables you to manage Internet usage by preventing access to inappropriate Web content. The following types of Web filtering solutions are available:
 - Integrated Web filtering—Blocks or permits Web access after the device identifies the category for a URL either from user-defined categories or from a category server (Websense provides the SurfControl Content Portal Authority (CPA) server).
 - Redirect Web filtering—Intercepts HTTP requests and forwards the server URL to an external URL filtering server to determine whether to block or permit the requested Web access. Websense provides the URL filtering server.

Content Security Licensing

All content security components require licenses with the exception of content filtering, which uses the parameters defined in the content filtering profile. This is because Juniper Networks leverages third-party technology that is constantly updated to provide the most up-to-date inspection capabilities.

Content Security Components

Content security components include custom objects, feature profiles, and content security profiles that can be configured on SRX Series Firewalls. From a high level, feature profiles specify how a feature is configured and then applied to content security profiles, which in turn is applied to firewall policies, as shown in [Figure 12 on page 388](#).

Figure 12: Content Security Components



Content security profiles do not have their own seven-tuple rulebase; in a sense they inherit the rules from the firewall rule. The strength of the content security feature comes from URL filtering, where you can have a separate configuration for different users or user groups.

- Custom objects—Although SRX Series Firewalls support predefined feature profiles that can handle most typical use cases, there are some cases where you might need to define your own objects, specifically for URL filtering, antivirus filtering, and content filtering.

- **Feature profiles**—Feature profiles specify how components of each profile should function. You can configure multiple feature profiles that can be applied through different content security profiles to firewall rules.
- **Content security profiles**—content security profiles function as a logical container for individual feature profiles. Content security profiles are then applied to specific traffic flows based on the classification of rules in the firewall policy, thereby enabling you to define separate content security profiles per firewall rule to differentiate the enforcement per firewall rule. Essentially, the firewall rulebase acts as the match criteria, and the content security profile is the action to be applied.
- **Security policy**—You can choose predefined content security policies which consist of predefined feature profiles that can be applied to the firewall policy rules. The predefined content security policies are :
 - default-utm-policy
 - sophos-av-policy
 - je-wf-policy
 - sophos-je-av-wf-policy

Configure the Content Security Settings

Use the **Edit Content Security Settings** page to configure content security antispam, antivirus, and Web filtering settings for a tenant.

These settings are applicable to all the devices. The settings are pushed to all those devices where a firewall policy rule with content security enabled is applicable.

To configure content security settings:

1. Select **SRX > Security Subscriptions > Content Security > Content Security Settings**.

The Edit Content Security Settings page appears.

2. Complete the configuration according to the guidelines provided in [Table 156 on page 390](#).

3. Do one of the following:

- Click **Reset** to reset the settings to the previously saved configured.
- Click **OK** to save the settings.

The settings are saved and a confirmation message is displayed.

Table 156: Content Security Settings

Setting	Guideline
Antispam Settings	
Address Allowlist	<p>Select the URL pattern to be used as the antispam allowlist.</p> <p>Alternatively, click Create New URL Pattern to create a new URL pattern to use as a allowlist.</p> <p>The Create URL Patterns page appears.</p> <p>For more information, see "Create a URL Pattern" on page 921 for an explanation of the fields on this page.</p>
Address Blocklist	<p>Select the URL pattern to be used as the antispam blocklist.</p> <p>Alternatively, click Create New URL Pattern to create a new URL pattern to use as a blocklist.</p>
Antivirus Settings	
MIME Allowlist	Enter one or more MIME types (separated by commas) to exclude from antivirus scanning.
Exception MIME Allowlist	Enter one or more MIME types (separated by commas) that are to be excluded from the list of MIME types specified as part of the MIME allowlist. This list is a subset of the MIME types that you specified in the MIME allowlist. For example, if you specify video/ in the allowlist and video/x-shockwave-flash in the exception allowlist, all objects of MIME type video/ except MIME type video/x-shockwave-flash are excluded from antivirus scanning.
URL Allowlist	Select the list of URLs the antivirus settings can allow.
Web Filtering Settings	

Table 156: Content Security Settings (Continued)

Setting	Guideline
URL Allowlist	Select the list of URLs the Web filtering settings can allow; these URLs are excluded from Web filtering.
URL Blocklist	Select the list of URLs the Web filtering settings can block; these URLs are blocked from Web access.
Site Reputation Level	<p>Site reputation level is a rating system to define the following default security levels for a URL:</p> <ul style="list-style-type: none"> • Harmful • Suspicious • Fairly-safe • Moderately-safe • Very-safe <p>Drag the slider to change the default site reputation values. For example, to change the site reputation value for harmful URL (1-59), you can drag the slider to left or right to increase or decrease the default site reputation value.</p>

About the Content Security Profiles Page

IN THIS SECTION

- [Tasks You Can Perform | 392](#)
- [Field Descriptions | 392](#)

To access this page, select **SRX > Security Subscriptions > Content Security > Content Security Profiles**.

You can view and manage content security profiles using the Content Security Profiles page. Content security profiles enable you to consolidate several security features into one system to protect against multiple threat types.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a content security profile—See ["Create a Content Security Profile" on page 395](#) .
- Edit, clone, or delete a content security profile—See ["Edit, Clone, and Delete a Content Security Profile" on page 399](#) .
- View the details of a content security profile—Select the content security profile for which you want to view the details and from the More or right-click menu, select **Detailed View**. The Content Security Profile Details page appears. [Table 158 on page 393](#) describes the fields on this page.
- Clear the selected content security profiles—Click **Clear All Selections** to clear any content security profiles that you might have selected.
- Search for content security profiles using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.

Field Descriptions

[Table 157 on page 392](#) describes the fields on the Content Security Profiles page.

Table 157: Content Security Profiles Page Fields

Field	Description
Name	Name of the content security profile.
Antispam	Information about the antispam profile associated with the content security profile.
Antivirus	Information about the antivirus profiles associated with the content security profile.
Content Filtering	Information about the content filtering profiles associated with the content security profile.

Table 157: Content Security Profiles Page Fields *(Continued)*

Field	Description
Web Filtering	Information about the Web filtering profile associated with the content security profile. NOTE: To view Juniper NextGen categories, you must have Junos OS version 23.4R1 or later installed.
Description	Description of the content security profile.

Table 158: Content Security Profile Details Page Fields

Field	Description
General Information	
Name	Name of the content security profile.
Description	Description of the content security profile.
Traffic Options	
Connection Limit Per Client	Specify the connection limit per client. The default is 2000 and a value of 0 means that there is no connection limit.
Action When Connection Limit Is Reached	Action to be taken when the configured connection limit per client is reached.
Web Filtering Profile	
HTTP	Web filtering profile to be used for HTTP traffic.
Antivirus Profile	
HTTP	Antivirus profile to be used for HTTP traffic.

Table 158: Content Security Profile Details Page Fields (Continued)

Field	Description
FTP Upload	Antivirus profile to be used for FTP upload traffic.
FTP Download	Antivirus profile to be used for FTP download traffic.
IMAP	Antivirus profile to be used for IMAP traffic.
SMTP	Antivirus profile to be used for SMTP traffic.
POP3	Antivirus profile to be used for POP3 traffic.
Antispam Profile	
SMTP	Antispam profile to be used for SMTP traffic.
Content Filtering Profile	
HTTP	Content filtering profile to be used for HTTP traffic.
FTP Upload	Content filtering profile to be used for FTP upload traffic.
FTP Download	Content filtering profile to be used for FTP download traffic.
IMAP	Content filtering profile to be used for IMAP traffic.
SMTP	Content filtering profile to be used for SMTP traffic.
POP3	Content filtering profile to be used for POP3 traffic.

Create a Content Security Profile

Use the **Create Content Security Profiles** page to configure content security profiles. Content security consolidates several security features to protect against multiple threat types. The Create Content Security Profiles wizard provides step-by-step procedures to create a content security profile. You can configure antispam, antivirus, Web filtering, and content filtering profiles by launching the respective wizards from the wizard.

To create a content security profile:

1. Select **SRX > Security Subscriptions > Content Security > Content Security**.

The Content Security Profiles page appears.

2. Click the add icon (+) to create a new content security profile.

The Create Content Security Profiles wizard appears, displaying brief instructions about creating a content security profile.

3. Complete the configuration according to the guidelines provided in [Table 159 on page 395](#).

NOTE: Fields marked with * are mandatory.

4. Click **Finish**.

A content security profile is created. You are returned to the content security Profiles page where a confirmation message is displayed. After you create a content security profile, you can assign it to a firewall policy rule on the Security Policy page.

Table 159: Content Security Profile Settings

Setting	Guideline
General Information	
Name	Enter a unique name for the content security profile. The maximum length is 29 characters.
Description	Enter a description for the content security profile. The maximum length is 255 characters.

Table 159: Content Security Profile Settings (Continued)

Setting	Guideline
<p>Traffic Options</p> <p>NOTE: In an attempt to consume all available resources, a malicious user might generate a large amount of traffic all at once. To prevent such activity from succeeding, you can impose traffic options.</p>	
Connection Limit per Client	Specify the connection limit per client for client connections on the device. The default is 2000 and a value of 0 means that there is no connection limit.
Action when connection limit is reached	<p>Specify the action that must be taken when the connection limit is reached. The available actions are No action (default), Log and permit, and Block.</p> <p>Click Next to continue.</p>
<p>Web Filtering Profiles by Traffic Protocol</p>	
HTTP	<p>Select the Web filtering profile to be applied for HTTP traffic.</p> <p>NOTE: To select Juniper NextGen Web filtering profile, you must have Junos OS version 23.4R1 or later installed.</p> <p>Alternatively, click Create Another Profile to create a Web filtering profile. The Create Web Filtering Profiles wizard appears. See "Create a Web Filtering Profile" on page 405 for an explanation of the fields on this wizard.</p> <p>Click Back to go the preceding step or click Next to go to the next step.</p>
<p>Antivirus Profiles by Traffic Protocol</p>	

Table 159: Content Security Profile Settings (Continued)

Setting	Guideline
Apply to all protocols	<p>Click the toggle button to enable a single antivirus profile to all traffic protocols and then specify the profile in the Default Profile field.</p> <p>If you disable the toggle button, which is the default, you can specify antivirus profiles for each traffic type .</p>
Default Profile	<p>Select the antivirus profile to be applied to all traffic protocols.</p> <p>Click Back to go the preceding step or click Next to go to the next step.</p>
<p>NOTE: Click Create Another Profile to create an antivirus profile that you can then assign. The Create Antivirus Profiles wizard appears. See "Create an Antivirus Profile" on page 417 for an explanation of the fields on this wizard.</p>	
HTTP	<p>Select the antivirus profile to be applied to HTTP traffic.</p>
FTP Upload	<p>Select the antivirus profile to be applied to FTP upload traffic.</p>
FTP Download	<p>Select the antivirus profile to be applied to FTP download traffic.</p>
IMAP	<p>Select the antivirus profile to be applied to IMAP traffic.</p>
SMTP	<p>Select the antivirus profile to be applied to SMTP traffic.</p>

Table 159: Content Security Profile Settings (Continued)

Setting	Guideline
POP3	<p>Select the antivirus profile to be applied to POP3 traffic.</p> <p>Click Back to go the preceding step or click Next to go to the next step.</p>
Antispam Profiles by Traffic Protocol	
SMTP	<p>Select the antispam profile to be applied for SMTP traffic.</p> <p>Alternatively, click Create Another Profile to create an antispam profile. The Create Antispam Profiles wizard appears. See "Create an Antispam Profile" on page 424 for an explanation of the fields on this wizard.</p> <p>Click Back to go the preceding step or click Next to go to the next step.</p>
Content Filtering Profiles by Traffic Protocol	
Apply to all protocols	<p>Click the toggle button to apply a single content filtering profile to all traffic protocols and then specify the profile in the Default Profile field.</p> <p>If you disable this toggle button, which is the default, you can specify antivirus profiles for each traffic type.</p>
Default Profile	<p>Select the content filtering profile to be applied to all traffic protocols.</p> <p>Click Back to go the preceding step or click Next to go to the next step.</p>
<p>NOTE: Click Create Another Profile to create a content filtering profile that you can then assign. The Create Content Filtering Profiles wizard appears. See "Create a Content Filtering Profile" on page 430 for an explanation of the fields on this wizard.</p>	

Table 159: Content Security Profile Settings (Continued)

Setting	Guideline
HTTP	Select the content filtering profile to be applied to HTTP traffic.
FTP Upload	Select the content filtering profile to be applied to FTP upload traffic.
FTP Download	Select the content filtering profile to be applied to FTP download traffic.
IMAP	Select the content filtering profile to be applied to IMAP traffic.
SMTP	Select the content filtering profile to be applied to SMTP traffic.
POP3	Select the content filtering profile to be applied to POP3 traffic. Click Back to go the preceding step.
Content Filtering (New)	
Content Filtering Profile	Select the content filtering policy to be applied for devices running Junos OS Release 21.4 or later.

Edit, Clone, and Delete a Content Security Profile

IN THIS SECTION

- [Edit a Content Security Profile | 400](#)
- [Clone a Content Security Profile | 400](#)

You can edit, clone, and delete content security profiles from the **Content Security Profiles** page. This topic has the following sections:

Edit a Content Security Profile

To modify the parameters configured for a content security profile:

NOTE: You cannot modify the default profiles already present in the system.

1. Select **SRX > Security Subscriptions > Content Security > Content Security Profiles**.

The Content Security Profiles page appears, displaying the existing content security profiles.

2. Select the custom content security profile that you want to edit and click the pencil icon.

The Edit Content Security Profiles page appears, displaying the same fields that are presented when you create a content security profile.

3. Modify the content security profile fields as needed.

4. Click **OK** to save your changes.

You are taken to the Content Security Profiles page. A confirmation message appears indicating the status of the edit operation.

Clone a Content Security Profile

Cloning enables you to easily create a new content security profile based on an existing one.

To clone a content security profile:

1. Select **SRX > Security Subscriptions > Content Security > Content Security Profiles**.

The Content Security Profiles page appears, displaying the existing content security profiles.

2. Select the custom content security profile that you want to clone and then select **More > Clone**.

The Clone Content Security Profiles page appears, displaying the same fields that are presented when you create a content security profile.

3. Modify the content security profile fields as needed.

4. Click **OK** to save your changes.

You are taken to the Content Security Profiles page. A confirmation message appears, indicating the status of the clone operation.

Delete a Content Security Profile

NOTE: Before deleting a content security profile, ensure that the profile is not used in a firewall policy rule. If you try to delete a profile that is used in a firewall policy rule, an error message is displayed.

To delete one or more content security profiles:

1. Select **SRX > Security Subscriptions > Content Security > Content Security Profiles**.
The Content Security Profiles page appears, displaying the existing content security profiles.
2. Select one or more custom content security profiles that you want to delete and click the delete icon.
An alert message appears, asking you to confirm the delete operation.
3. Click **Yes** to delete the selected content security profiles.
A confirmation message appears, indicating the status of the delete operation.

About the Web Filtering Profiles Page

IN THIS SECTION

- [Tasks You Can Perform | 402](#)
- [Field Descriptions | 403](#)

To access this page, select **SRX > Security Subscriptions > Content Security > Web Filtering Profiles** in Customer Portal.

Use the Web Filtering Profiles page to view and manage Web filtering profiles. Web filtering profiles enable you to manage Internet usage by preventing access to inappropriate Web content over HTTP. [Table 160 on page 402](#) lists the Web filtering solutions that are supported and the license requirements.

Table 160: Web Filtering Solutions Supported

Type	Description	License Requirement
Integrated Web Filtering	Blocks or permits Web access after the device identifies the category for a URL, either from user-defined categories or from a category server (SurfControl Content Portal Authority provided by Websense).	A separately licensed subscription service.
Redirect Web Filtering	Intercepts HTTP requests and forwards the server URL to an external URL filtering server to determine whether to block or permit the requested Web access. Websense provides the URL filtering server.	Does not require a license.
Juniper Local Web Filtering	Intercepts every HTTP request in a TCP connection. In this case, the decision making is done on the device after it looks up a URL to determine whether it is in the allowlist or blocklist based on its user-defined category.	Does not require a license or a remote category server.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a Web filtering profile—See ["Create a Web Filtering Profile" on page 405](#) .
- Edit, clone, or delete a Web filtering profile—See ["Edit, Clone, and Delete a Web Filtering Profile" on page 413](#) .
- View the details of a Web filtering profile—Select the Web filtering profile for which you want to view the details and from the More, select **Detailed View**. The Web Filtering Profile Details page appears. [Table 162 on page 403](#) describes the fields on this page.
- Clear the selected Web filtering profiles—Click **Clear All Selections** to clear any Web filtering profiles that you might have selected.

- Search for Web filtering profiles using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.

Field Descriptions

Table 161 on page 403 describes the fields on the Web Filtering Profiles page.

Table 161: Web Filtering Profiles Page Fields

Field	Description
Name	Name of the Web filtering profile.
Profile Type	Type of engine used for the profile: Juniper-Enhanced, Local, Websense Redirect, or Juniper NextGen. NOTE: To use the Juniper NextGen profile type, you must have Junos OS version 23.4R1 or later installed.
Default Action	Default action taken when the specified connection limit per client is reached.
Timeout	Timeout value to wait for a response from the Websense server.
Description	Description of the Web filtering profile.

Table 162: Web Filtering Profile Details Page Fields

Field	Description
General Information	
Name	Name of the Web filtering profile.
Description	Description of the Web filtering profile.

Table 162: Web Filtering Profile Details Page Fields (Continued)

Field	Description
Engine Type	<p>Type of engine used for the profile: Juniper-Enhanced, Local, Websense Redirect, or Juniper NextGen.</p> <p>NOTE: To view the Juniper NextGen engine type, you must have Junos OS version 23.4R1 or later installed.</p>
Timeout	Timeout value to wait for a response from the Websense server.
Custom Block Message/ URL	Redirect URL address or a custom message when HTTP requests are blocked.
Custom Quarantine Message	Custom message to indicate if the access is allowed or denied to the URL.
Fallback Options	
Default Action	Action taken for URL categories with no assigned action and for uncategorized URLs. This action is taken only if no reputation action is assigned.
Global Reputation Actions	<p>Actions taken for the following site reputations:</p> <ul style="list-style-type: none"> • Very Safe • Moderately Safe • Fairly Safe • Suspicious • Harmful <p>NOTE: The site reputation score is not applicable for Juniper NextGen Web filtering.</p>

Table 162: Web Filtering Profile Details Page Fields (Continued)

Field	Description
URL Categories	URL categories associated with the Web filtering profile.

Create a Web Filtering Profile

Web filtering profiles enable you to manage Internet usage by preventing access to inappropriate Web content over HTTP.

To create a Web filtering profile:

1. Select **SRX > Security Subscriptions > Content Security > Web Filtering Profiles**.

The Web Filtering Profiles page appears.

2. Click the add icon (+) to create a new Web filtering profile.

The Create Web Filtering Profiles wizard appears, displaying brief instructions about creating a Web filtering profile.

3. Click **Next** to navigate to the next page.

4. Complete the configuration according to the guidelines provided in [Table 163 on page 405](#).

NOTE: Fields marked with * are mandatory.

5. Click **Finish**.

A Web filtering profile is created, which you can associate with a content security profile. You are returned to the Web Filtering Profiles page where a confirmation message is displayed.

Table 163: Creating Web Filtering Profiles Settings

Setting	Guideline
General Information	

Table 163: Creating Web Filtering Profiles Settings *(Continued)*

Setting	Guideline
Name	Enter a unique name for the Web filtering profile. The maximum length is 29 characters.
Description	Enter a description for the Web filtering profile. The maximum length is 255 characters.
Timeout	Enter a timeout (in seconds) to wait for a response from the Websense server. The default is 15 seconds and the maximum is 1800 seconds.
Engine Type	<p>Select an engine type for Web filtering:</p> <ul style="list-style-type: none"> • (Default) Juniper Enhanced—Content Security-enhanced Web filtering. • Juniper NextGen—Intercepts the HTTP and HTTPS traffic and sends URL information or the destination IP address to the Juniper NextGen Web Filtering (NGWF) Cloud. The NGWF Cloud categorizes the URL and provides site reputation information. Based on this information, SRX Series Firewall takes action on the traffic. <p>NOTE: To use this option, you must have Junos OS version 23.4R1 or later installed.</p> <ul style="list-style-type: none"> • Websense Redirect—Redirect Web filtering profile. • Local—Allows you to define custom URL categories, which can be included in blocklists and allowlists that are evaluated on the device.

Table 163: Creating Web Filtering Profiles Settings *(Continued)*

Setting	Guideline
Safe Search	<p>Click the toggle button to enable (default) or disable the safe search. Safe search ensures that embedded objects, such as images on the URLs received from the search engines, are safe and that undesirable content is not returned to the client.</p> <p>NOTE: This option is available only for the Juniper Enhanced engine type. Safe search redirect supports only HTTP and you cannot extract the URL for HTTPS. Therefore, it is not possible to generate a redirect response for HTTPS search URLs.</p>
Custom Block Message/URL	<p>Specify the redirect URL or a custom message to be sent when HTTP requests are blocked. The maximum length is 1024 characters.</p> <p>NOTE: If a message begins with http: or https:, the message is considered a block URL. Messages that begin with values other than http: or https: are considered custom block messages.</p> <p>Click Back to go the preceding step or click Next to go to the next step.</p>

Table 163: Creating Web Filtering Profiles Settings *(Continued)*

Setting	Guideline
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. The maximum length is 512 characters.</p> <p>The quarantine message contains the following information:</p> <ul style="list-style-type: none"> • URL name • Quarantine name • Category (if available) • Site reputation (if available) <p>For example, if you set the action for Enhanced_Search_Engines_and_Portals to quarantine, and you try to access www.search.yahoo.com, the quarantine message is as follows: ***The requested webpage is blocked by your organization's access policy***.</p> <p>Click Back to go the preceding step or click Next to go to the next step.</p>
Account	Specify the user account associated with the Websense Web filtering profile.
Server	Specify the hostname or an IP address for the Websense server.
Port	<p>Specify the port number to use to communicate with the Websense server. The default port value is 15968.</p> <p>Click Back to go the preceding step or click Next to go to the next step.</p>

Table 163: Creating Web Filtering Profiles Settings (*Continued*)

Setting	Guideline
Sockets	Enter the number of sockets used for communication between the client and the server. The default value is 8.
<p>URL Categories</p> <p>NOTE: To select Juniper NextGen URL categories, you must have Junos OS version 23.4R1 or later installed.</p>	
Deny Action List	<p>Click the Add URL Categories button to specify a list of URL categories that must be denied access.</p> <p>The Select URL Categories page appears. Complete the configuration according to the guidelines provided in Table 164 on page 412 .</p> <p>The list of URL categories selected is displayed in a text box.</p>
Log & Permit Action List	<p>Specify a list of URL categories that are logged and then permitted.</p> <p>The Select URL Categories page appears. Complete the configuration according to the guidelines provided in Table 164 on page 412 .</p> <p>The list of URL categories selected is displayed in a text box.</p>
Permit Action List	<p>Specify a list of URL categories that should be permitted access.</p> <p>The Select URL Categories page appears. Complete the configuration according to the guidelines provided in Table 164 on page 412 .</p> <p>The list of URL categories selected is displayed in a text box.</p>

Table 163: Creating Web Filtering Profiles Settings *(Continued)*

Setting	Guideline
Quarantine Action List	<p>Specify a list of URL categories that should be quarantined.</p> <p>The Select URL Categories page appears. Complete the configuration according to the guidelines provided in Table 164 on page 412 .</p> <p>The list of URL categories selected is displayed in a text box.</p> <p>Click Back to go the preceding step or click Next to go to the next step.</p>
Fallback Options	

Table 163: Creating Web Filtering Profiles Settings *(Continued)*

Setting	Guideline
Global Reputation Actions	<p>Enhanced Web filtering intercepts HTTP and HTTPS requests and sends the HTTP URL or the HTTPS source IP to the Websense ThreatSeeker Cloud (TSC). The TSC categorizes the URL into one of the predefined categories and provides the site reputation information to the device. The device determines if it can permit or block the request based on the information provided by the TSC.</p> <p>By default, the URLs are processed using their reputation score if there is no category available. Click the toggle button to disable global reputation actions or select the action that you want to take for the uncategorized URLs based on their reputation score:</p> <ul style="list-style-type: none"> • Very Safe—Permit, log and permit, block, or quarantine a request if a site reputation value is 90 through 100. By default, Permit is selected. • Moderately Safe—Permit, log and permit, block, or quarantine a request if a site reputation of 80 through 89 is returned. By default, Log and Permit is selected. • Fairly Safe—Permit, log and permit, block or quarantine a request if a site-reputation of 70 through 79 is returned. By default, Log and Permit is selected. • Suspicious—Permit, log and permit, block, or quarantine a request if a site reputation of 60 through 69 is returned. By default, Quarantine is selected. • Harmful—Permit, log and permit, block, or quarantine a request if a site reputation of zero through 59 is returned. By default, Block is selected. <p>NOTE: The site reputation score for each level can be modified as per user requirements under Content Security Settings menu. For more information, see</p>

Table 163: Creating Web Filtering Profiles Settings *(Continued)*

Setting	Guideline
	<p>"Configure the Content Security Settings" on page 389 .</p> <p>The site reputation score is not applicable for Juniper NextGen Web filtering.</p>
Default Action	Choose the actions for URL categories with no assigned action and for uncategorized URLs. This is used only if no reputation action is assigned.
Fallback Actions	
Default	Select Log and Permit or Block (a default action) when an error occurs.
Server connectivity	Select Log and Permit or Block when the ThreatSeeker Websense Cloud servers are unreachable.
Timeout	Select Log and Permit or Block when a timeout occurs for requests to ThreatSeeker Cloud.
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.

Table 164: Select URL Categories Settings

Setting	Guideline
Show	<p>Choose which URL categories for selection: All categories, Custom URL categories, or Juniper NextGen URL categories.</p> <p>The Available column of the URL Categories field displays URL categories based on your selection.</p>

Table 164: Select URL Categories Settings (Continued)

Setting	Guideline
URL Categories	<p>Select one or more URL categories in the Available column and click the forward arrow to confirm your selection. The selected URL categories are displayed in the Selected column.</p> <p>Alternatively, click Create New URL Category to create a URL category and assign it to the URL category. The Create URL Categories page appears; for more information, see "Create a URL Category" on page 928 .</p> <p>Click OK to confirm your selection. You are returned to the Create Web Filtering Profiles page.</p>

Edit, Clone, and Delete a Web Filtering Profile

IN THIS SECTION

- [Edit a Web Filtering Profile | 413](#)
- [Clone a Web Filtering Profile | 414](#)
- [Delete a Web Filtering Profile | 414](#)

You can edit, clone, and delete Web filtering profiles from the Web Filtering Profiles page. This topic has the following sections:

Edit a Web Filtering Profile

To modify the parameters configured for a Web filtering profile:

NOTE: You cannot modify the default profiles already present in the system.

1. Select **SRX > Security Subscriptions > Content Security > Web Filtering Profiles**.

The Web Filtering Profiles page appears, displaying the existing Web filtering profiles.

2. Select the custom Web filtering profile that you want to edit and click the pencil icon.

The Edit Web Filtering Profiles page appears, displaying the same fields that are presented when you create a Web filtering profile.

3. Modify the Web filtering profile fields as needed.
4. Click **OK** to save your changes.

You are taken to the Web Filtering Profiles page. A confirmation message appears, indicating the status of the edit operation.

Clone a Web Filtering Profile

Cloning enables you to easily create a new Web filtering profile based on an existing one.

To clone a Web filtering profile:

1. Select **SRX > Security Subscriptions > Content Security > Web Filtering Profiles**.

The Web Filtering Profiles page appears, displaying the existing Web filtering profiles.

2. Select the Web filtering profile that you want to clone and then select **More > Clone**.

The Clone Web Filtering Profiles page appears, displaying the same fields that are presented when you create a Web filtering profile.

3. Modify the Web filtering profile fields as needed.
4. Click **OK** to save your changes.

You are taken to the Web Filtering Profiles page. A confirmation message appears, indicating the status of the clone operation.

Delete a Web Filtering Profile

Before deleting a Web filtering profile, ensure that the profile is not used in a content security profile that is, in turn, used in a firewall policy rule. If you try to delete a Web filtering profile that is used in a firewall policy rule, an error message is displayed.

To delete one or more Web filtering profiles:

1. Select **SRX > Security Subscriptions > Content Security > Web Filtering Profiles**.

The Web Filtering Profiles page appears, displaying the existing Web filtering profiles.

2. Select one or more custom Web filtering profiles that you want to delete and click the delete icon.

An alert message appears, asking you to confirm the delete operation.

3. Click **Yes** to delete the selected Web filtering profiles.

A confirmation message appears, indicating the status of the delete operation.

About the Antivirus Profiles Page

IN THIS SECTION

- [Tasks You Can Perform | 415](#)
- [Field Descriptions | 415](#)

To access this page, select **SRX > Security Subscriptions > Content Security > Antivirus Profiles**.

Use the Antivirus Profiles page to view and manage antivirus profiles. Antivirus profiles enable you to inspect files transmitted over several protocols (HTTP, FTP upload and download, IMAP, SMTP, and POP3) to determine whether the files exchanged are known malicious files, similar to how desktop antivirus software scans files for the same purpose.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create an antivirus profile—See "[Create an Antivirus Profile](#)" on page 417 .
- Edit, clone, or delete an antivirus profile—See "[Edit, Clone, and Delete an Antivirus Profile](#)" on page 420 .
- View the details of an antivirus profile—Select the antivirus profile for which you want to view the details and from the More or right-click menu, select **Detailed View**. The Antivirus Profile Details page appears. [Table 166 on page 416](#) describes the fields on this page.
- Clear the selected antivirus profiles—Click **Clear All Selections** to clear any antivirus profiles that you might have selected.
- Search for antivirus profiles by using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.

Field Descriptions

[Table 165 on page 416](#) describes the fields on the Antivirus Profiles page.

Table 165: Antivirus Profiles Page Fields

Field	Description
Name	Name of the antivirus profile.
Profile Type	Type of engine used for the profile.
Content Size Limit	Content size limit, in kilobytes, refers to accumulated TCP payload size.
Trickling Timeout	Number of seconds to wait for a response from the server.
Description	Description of the antivirus profile.

Table 166: Antivirus Profiles Details Page Fields

Field	Description
General Information	
Name	Name of the antivirus profile.
Description	Description of the antivirus profile.
Engine Type	Type of engine used for the profile.
Scan Options	
Content Size Limit	Content size limit, in kilobytes, refers to accumulated TCP payload size.
Fallback Options	

Table 166: Antivirus Profiles Details Page Fields (Continued)

Field	Description
Default Action	Displays the default fallback action taken when the antivirus system encounters errors.
Content Size	Displays the actions taken if the content size exceeds a set limit.
Engine Error	Displays the action taken when an engine error occurs.

Create an Antivirus Profile

Use the Create Antivirus Profiles page to configure antivirus profiles. The *antivirus* profile defines the content to scan for any malware and the action to be taken when malware is detected. After you create a profile, you can assign it to content security profiles.

To create an antivirus profile:

1. Select **SRX > Security Subscriptions > Content Security > Antivirus Profiles**.

The Antivirus Profiles page appears.

2. Click the add icon (+) to create a new antivirus profile.

The Create Antivirus Profiles wizard appears, displaying brief instructions about creating an antivirus profile.

3. Click **Next** to navigate to the next page.

4. Complete the configuration according to the guidelines provided in [Table 167 on page 418](#).

NOTE: Fields marked with * are mandatory.

5. Click **Finish**.

A summary page is displayed. 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 settings and create the profile.

A message indicating the status of the create operation is displayed.

7. Click **Close**.

You are returned to the Antivirus Profiles page.

Table 167: Antivirus Profile Settings

Setting	Guideline
General Information	
Name	Enter a unique name for the antivirus profile. The maximum length is 29 characters.
Description	Enter a description for the antivirus profile. The maximum length is 255 characters.
Engine Type	<p>Displays the engine type used for scanning. Currently, Sophos is the only antivirus engine supported.</p> <p>Sophos antivirus is an in-the-cloud antivirus solution. The virus and malware database is located on external servers maintained by Sophos (Sophos Extensible List) servers, thus there is no need to download and maintain large pattern databases on the Juniper Networks device.</p>
Fallback Options	

Table 167: Antivirus Profile Settings (Continued)

Setting	Guideline
	<p>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.</p> <p>Specify the fallback options to use when there is a failure, or select the default action if no specific options are to be configured:</p> <ul style="list-style-type: none"> • Content Size—Select an option to specify whether the content should be blocked (default) or logged and permitted if the content size exceeds the previously defined limit. • Content Size Limit—Enter the content size limit in kilobytes (KB) based on which action is taken. The range is 20 through 40,000 KB. The content size limit check occurs before the scan request is sent. The content size refers to accumulated TCP payload size. • Engine Error—Select the action to take (Block [default] or Log and Permit) when an engine error occurs. <p>The term <i>engine error</i> refers all engine errors, including engine not ready, timeout, too many requests, password protected, corrupt file, decompress layer, and out of resources.</p> • Default Action—Select the default action (Block [default] or Log and Permit) to take when an error occurs.
Notification Options	

Table 167: Antivirus Profile Settings (Continued)

Setting	Guideline
	<p>Use the notification options to configure a method of notifying the user when a fallback occurs or a virus is detected:</p> <ul style="list-style-type: none"> • Fallback Deny—Select this option to notify mail senders that their messages were blocked. • Fallback Non-Deny—Select this option to warn mail recipients that they received unblocked messages despite problems. • Virus Detected—Select this option to notify mail recipients that their messages were blocked.

Edit, Clone, and Delete an Antivirus Profile

IN THIS SECTION

- [Edit an Antivirus Profile | 420](#)
- [Clone an Antivirus Profile | 421](#)
- [Delete an Antivirus Profile | 421](#)

You can edit, clone, and delete antivirus profiles from the Antivirus Profiles page. This topic has the following sections:

Edit an Antivirus Profile

To modify the parameters configured for an antivirus profile:

NOTE: You cannot modify the default profiles already present in the system.

1. Select **Security Subscriptions > Content Security > Antivirus Profiles**.

The Antivirus Profiles page appears, displaying the existing antivirus profiles.

2. Select the custom antivirus profile that you want to edit and then select the pencil icon.

The Edit Antivirus Profiles page appears, displaying the same fields that are presented when you create an antivirus profile.

3. Modify the antivirus profile fields as needed.
4. Click **OK** to save your changes.

You are taken to the Antivirus Profiles page. A confirmation message appears, indicating the status of the edit operation.

Clone an Antivirus Profile

Cloning enables you to easily create a new antivirus profile based on an existing one.

To clone an antivirus profile:

1. Select **Security Subscriptions > Content Security > Antivirus Profiles**.

The Antivirus Profiles page appears, displaying the existing antivirus profiles.

2. Select the antivirus profile that you want to clone and then select **More > Clone**.

The Clone Antivirus Profiles page appears, displaying the same fields that are presented when you create an antivirus profile.

3. Modify the antivirus profile fields as needed.
4. Click **OK** to save your changes.

You are taken to the Antivirus Profiles page. A confirmation message appears, indicating the status of the clone operation.

Delete an Antivirus Profile

Before deleting an antivirus profile, ensure that the profile is not used in a content security profile that is, in turn, used in a firewall policy rule. If you try to delete an antivirus profile that is used in a firewall policy rule, an error message is displayed.

To delete one or more antivirus profiles:

1. Select **SRX > Security Subscriptions > Content Security > Antivirus Profiles** in Customer Portal.

The Antivirus Profiles page appears, displaying the existing antivirus profiles.

2. Select one or more custom antivirus profiles that you want to delete and then select the delete icon.

An alert message appears, asking you to confirm the delete operation.

3. Click **Yes** to delete the selected antivirus profiles.

A confirmation message appears, indicating the status of the delete operation.

About the Antispam Profiles Page

IN THIS SECTION

- [Tasks You Can Perform | 422](#)
- [Field Descriptions | 422](#)

To access this page, select **Security Subscriptions > Content Security > Antispam Profiles** in Customer Portal.

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 ["Create an Antispam Profile" on page 424](#) .
- Edit, clone, or delete an antispam profile—See ["Edit, Clone, and Delete an Antispam Profile" on page 426](#) .
- View the details of an antispam profile—Select the antispam profile for which you want to view the details and from the More or right-click menu, select **Detailed View**. The Antispam Profile Details page appears. [Table 169 on page 423](#) describes the fields on this page.
- Clear the selected antispam profiles—Click **Clear All Selections** to clear any antispam profiles that you might have selected.
- Search for antispam profiles using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.

Field Descriptions

[Table 168 on page 423](#) describes the fields on the Antispam Profiles page.

Table 168: Antispam Profiles Page Fields

Field	Description
Name	Name of the antispam profile.
Blacklist	Indicates whether server-based spam filtering or local spam filtering is used.
Action	Action to be taken when spam is detected.
Custom Tag	Custom-defined tag that identifies an e-mail message as spam.
Description	Description of the antispam profile.

Table 169: Antispam Profile Details Page Fields

Field	Description
Name	Name of the antispam profile.
Description	Description of the antispam profile.
Sophos Blacklist	Indicates whether Sophos Blacklist is enabled (server-based filtering) or disabled (local filtering).
Default Action	Action to be taken when spam is detected.
Custom Tag	Custom-defined tag that identifies an e-mail message as spam.

Create an Antispam Profile

Use the Create Antispam Profiles page to configure *antispam* profiles.

E-mail spam consists of unwanted e-mail messages usually sent by commercial, malicious, or fraudulent entities. When the device detects an e-mail message deemed to be spam, it either blocks the message or tags the message header or subject field with a preprogrammed string. Antispam filtering allows you to use a third-party server-based spam block list (SBL) and to optionally create your own local allowlists (benign) and blocklists (malicious) for filtering against e-mail messages.

NOTE: Sophos updates and maintains the IP-based SBL. Antispam is a separately licensed subscription service.

After you create an antispam profile, you can assign it to content security profiles.

To create an antispam profile:

1. Select **SRX > Security Subscriptions > Content Security > Antispam Profiles**.

The Antispam Profiles page appears.

2. Click the add icon (+) to create a new antispam profile.

The Create Antispam Profiles page appears, displaying brief instructions about creating an antispam profile.

3. Complete the configuration according to the guidelines provided in [Table 170 on page 424](#).

Fields marked with * are mandatory.

4. Click **OK** save the settings and create the profile.

A message indicating the status of the create operation is displayed. You are returned to the Antispam Profiles page.

Table 170: Antispam Profile Settings

Setting	Guideline
General Information	
Name	Enter a unique name for the antispam profile. The maximum length is 29 characters.

Table 170: Antispam Profile Settings (Continued)

Setting	Guideline
Description	Enter a description for the antispam profile. The maximum length is 255 characters.
Sophos Blacklist	<p>Use this toggle button to enable server-based spam filtering. If the toggle button is disabled, which is the default, local spam filtering is used.</p> <p>Server-based antispam filtering requires Internet connectivity with the spam block list (SBL) server. Domain Name Service (DNS) is required to access the SBL server. The firewall performs SBL lookups through the DNS protocol.</p> <p>NOTE: Server-based spam filtering supports only IP-based spam block list blacklist lookup. Sophos updates and maintains the IP-based spam block list. Server-based antispam filtering is a separately licensed subscription service.</p>
Action	
Default Action	<p>Select the action to be taken when spam is detected:</p> <ul style="list-style-type: none"> • Tag Email Subject Line • Tag SMTP Header • Block Email • None
Custom Tag	Enter a custom string for identifying a message as spam. The maximum length is 512 characters and the default is ***SPAM*** .

Edit, Clone, and Delete an Antispam Profile

IN THIS SECTION

- [Edit an Antispam Profile | 426](#)
- [Clone an Antispam Profile | 426](#)
- [Delete an Antispam Profile | 427](#)

You can edit, clone, and delete antispam profiles from the Antispam Profiles page. This topic has the following sections:

Edit an Antispam Profile

To modify the parameters configured for an antispam profile:

NOTE: You cannot modify the default profiles already present in the system.

1. Select **SRX > Security Subscriptions > Content Security > Antispam Profiles**.
The Antispam Profiles page appears, displaying the existing antispam profiles.
2. Select the custom antispam profile that you want to edit and click the pencil icon.
The Edit Antispam Profiles page appears, displaying the same fields that are presented when you create an antispam profile.
3. Modify the antispam profile fields as needed.
4. Click **OK** to save your changes.
You are taken to the Antispam Profiles page. A confirmation message appears, indicating the status of the edit operation.

Clone an Antispam Profile

Cloning enables you to easily create a new antispam profile based on an existing one.

To clone an antispam profile:

1. Select **SRX > Security Subscriptions > Content Security > Antispam Profiles**.
The Antispam Profiles page appears displaying the existing antispam profiles.
2. Select the custom antispam profile that you want to clone and then select **More > Clone**.

The Clone Antispam Profiles page appears, displaying the same fields that are presented when you create an antispam profile.

3. Modify the antispam profile fields as needed.
4. Click **OK**

You are taken to the Antispam Profiles page. A confirmation message appears, indicating the status of the clone operation.

Delete an Antispam Profile

Before deleting an antispam profile, ensure that the profile is not used in a content security profile that is, in turn, used in a firewall policy rule. If you try to delete an antispam profile that is used in a firewall policy rule, an error message is displayed.

To delete one or more antispam profiles:

1. Select **SRX > Security Subscriptions > Content Security > Antispam Profiles**.

The Antispam Profiles page appears, displaying the existing antispam profiles.

2. Select one or more custom antispam profiles that you want to delete and click the delete icon.

An alert message appears, asking you to confirm the delete operation.

3. Click **Yes** to delete the selected antispam profiles.

A confirmation message appears, indicating the status of the delete operation.

About the Content Filtering Profiles Page

IN THIS SECTION

- [Tasks You Can Perform | 428](#)
- [Field Descriptions | 428](#)

To access this page, select **SRX > Security Subscriptions > Content Security > Content Filtering Profiles** in Customer Portal.

Use the Content Filtering Profiles page to view and manage content filtering profiles for devices running Junos OS Releases earlier than 21.4.

NOTE: To filter content and manage the traffic on devices running Junos OS Release 21.4 or later, go to the ["Content Filtering Policy \(New\)" on page 435](#) page.

Content filtering profiles enable you to block or permit certain types of traffic over several protocols (HTTP, FTP upload and download, IMAP, SMTP, and POP3) 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:

- Create a content filtering profile—See ["Create a Content Filtering Profile" on page 430](#) .
- Edit, clone, or delete a content filtering profile—See ["Edit, Clone, and Delete a Content Filtering Profile" on page 434](#) .
- View the details of a content filtering profile—Select the content filtering profile for which you want to view the details and from the More or right-click menu, select **Detailed View**. The Content Filtering Profile Details page appears. [Table 172 on page 429](#) describes the fields on this page.
- Clear the selected content filtering profiles—Click **Clear All Selections** to clear any content filtering profiles that you might have selected.
- Search for content filtering profiles by using keywords—Click the search icon, enter the search term in the text box, and press Enter. The search results are displayed on the same page.

Field Descriptions

[Table 171 on page 428](#) describes the fields on the Content Filtering Profiles page.

Table 171: Content Filtering Profiles Page Fields

Field	Description
Name	Name of the content filtering profile.
Permit Command List	List of protocol commands permitted by the content filtering profile.

Table 171: Content Filtering Profiles Page Fields *(Continued)*

Field	Description
Block Command List	List of protocol commands blocked by the content filtering profile.
Notification Type	Type of notification that is sent when content is blocked.
Description	Description of the content filtering profile.

Table 172: Content Filtering Profiles Details Page Fields

Field	Description
General Information	
Name	Name of the content filtering profile.
Description	Description of the content filtering profile.
Notification Options	
Notify Mail Sender	Specifies whether the option to notify the e-mail sender is enabled or disabled.
Notification Type	Type of notification that is sent when content is blocked.
Protocol Commands	
Command Block List	List of protocol commands permitted by the content filtering profile.

Table 172: Content Filtering Profiles Details Page Fields (Continued)

Field	Description
Command Permit List	List of protocol commands blocked by the content filtering profile.
Content Types	
Block Content Types	List of harmful content types to be blocked.
File Extensions	
Extension Block List	File extensions to be blocked.
MIME	
MIME Block List	List of MIME types to be blocked.
MIME Permit List	List of MIME types to be permitted.

Create a Content Filtering Profile

Use the Create Content Filtering Profiles page to configure content filtering profiles. Content filtering blocks or permits certain types of traffic based on the MIME type, file extension, and protocol command. The content filter controls file transfers across the device by checking traffic against configured filter lists. [Table 173 on page 431](#) displays the types of content filters that you can configure as part of a content filtering profile.

NOTE: The content filtering profile evaluates traffic before all other content security profiles. Therefore, if traffic meets criteria configured in the content filter, the content filter acts first upon this traffic.

Table 173: Supported Content Filter Types

Type	Description
Protocol Command Block and Permit Lists	<p>Different protocols use different commands to communicate between servers and clients. By blocking or allowing certain commands, traffic can be controlled on the protocol command level. The block or permit command lists are intended to be used in combination, with the permit list acting as an exception list to the block list.</p> <p>NOTE: If a protocol command appears on both the permit list and the block list, the command is permitted.</p>
Extension Block List	<p>It is recommended to use file extensions to block or allow file transfers, because the name of a file is available during the transfers. All protocols support the use of the extension block list.</p>
MIME pattern filter	<p>MIME patterns are used to identify the type of traffic in HTTP and MAIL protocols. There are two lists of MIME patterns that are used by the content filter to determine the action to be taken. The MIME Block List contains a list of MIME type traffic that is to be blocked. The MIME Permit List contains MIME patterns that permitted by the content filter and are generally subsets of items on the block list.</p> <p>NOTE: The MIME permit list has a higher priority than the block list.</p>

To create a content filtering profile:

1. Select **SRX > Security Subscriptions > Content Security > Content Filtering Profiles**.

The Content Filtering Profiles page appears.

2. Click the add icon (+) to create a new content filtering profile.

The Create Content Filtering Profiles wizard appears, displaying brief instructions about creating a content filtering profile.

3. Click **Next** to navigate to the next page.

4. Complete the configuration according to the guidelines provided in [Table 174 on page 432](#).

Fields marked with * are mandatory.

5. Click **Finish**.

A summary page is displayed. Review the settings and if you need to make any modifications click the **Edit** link or the **Back** button.

6. Click **OK** save the settings and create the profile.

A message indicating the status of the create operation is displayed.

7. Click **Close**.

You are returned to the Content Filtering Profiles page.

Table 174: Content Filtering Profile Settings

Setting	Guideline
General Information	
Name	Enter a unique name for the content filtering profile. The maximum length is 29 characters.
Description	Enter a description for the content filtering profile. The maximum length is 255 characters.
Notification Options	
Notify Mail Sender	Click this toggle button to enable notification when a content filter is matched. Notifications are disabled by default.
Notification Type	Select the type of notification to send: <ul style="list-style-type: none"> • None—Do not send notifications. • Protocol—Send a protocol-specific notification. With these notifications, a protocol-specific error code might be sent. • Message—Send a generic notification.
Custom Notification Message	Enter a custom notification message. The maximum length is 512 characters.

Table 174: Content Filtering Profile Settings (*Continued*)

Setting	Guideline
Protocol Commands	
Command Block List	<p>Enter the protocol commands to be blocked for the HTTP, FTP, SMTP, IMAP, and POP3 protocols. Use commas to separate each command.</p> <p>Protocol commands allow you to control traffic at the protocol-command level.</p>
Command Permit List	<p>Enter specific commands to be permitted for the HTTP, FTP, SMTP, IMAP, and POP3 protocols. Use commas to separate each command.</p>
Block Content Type	<p>Use the content filter to block other types of harmful files that the MIME type or the file extension cannot control. Select from the following types of content blocking (supported only for HTTP):</p> <ul style="list-style-type: none"> • Active X • Windows executables (.exe) • HTTP cookie • Java applet • ZIP files
Extension Block List	<p>Use a file extension list to define a set of file extensions to block over HTTP, FTP, SMTP, IMAP, and POP3.</p> <p>Enter file extensions to block separated by commas. For example, exe, pdf, js, and so on.</p>
MIME Block List	<p>Enter the MIME types you want to block over HTTP, FTP, SMTP, IMAP, and POP3 connections. Use commas to separate each MIME type.</p>

Table 174: Content Filtering Profile Settings (Continued)

Setting	Guideline
MIME Permit List	Enter the MIME types you want to permit over HTTP, FTP, SMTP, IMAP, and POP3 connections. Use commas to separate each MIME type.

Edit, Clone, and Delete a Content Filtering Profile

IN THIS SECTION

- [Edit a Content Filtering Profile | 434](#)
- [Clone a Content Filtering Profile | 435](#)
- [Delete a Content Filtering Profile | 435](#)

You can edit, clone, and delete content filtering profiles from the Content Filtering Profiles page. This topic has the following sections:

Edit a Content Filtering Profile

To modify the parameters configured for a content filtering profile:

NOTE: You cannot modify the default profiles already present in the system.

1. Select **SRX > Security Subscriptions > Content Security > Content Filtering Profiles**.
The Content Filtering Profiles page appears, displaying the existing content filtering profiles.
2. Select the custom content filtering profile that you want to edit and click the pencil icon.
The Edit Content Filtering Profiles page appears, displaying the same fields that are presented when you create a content filtering profile.
3. Modify the content filtering profile fields as needed.
4. Click **OK** to save your changes.

You are taken to the Content Filtering Profiles page. A confirmation message appears, indicating the status of the edit operation.

Clone a Content Filtering Profile

Cloning enables you to easily create a new content filtering profile based on an existing one.

To clone a content filtering profile:

1. Select **SRX > Security Subscriptions > Content Security > Content Filtering Profiles**.

The Content Filtering Profiles page appears, displaying the existing content filtering profiles.

2. Select the content filtering profile that you want to clone and then select **More > Clone**.

The Clone Content Filtering Profiles page appears, displaying the same fields that are presented when you create a content filtering profile.

3. Modify the content filtering profile fields as needed.

4. Click **OK** to save your changes.

You are taken to the Content Filtering Profiles page. A confirmation message appears, indicating the status of the clone operation.

Delete a Content Filtering Profile

Before deleting a content filtering profile, ensure that the profile is not used in a content security profile that is, in turn, used in a firewall policy rule. If you try to delete a content filtering profile that is used in a firewall policy rule, an error message is displayed.

To delete one or more content filtering profiles:

1. Select **SRX > Security Subscriptions > Content Security > Content Filtering Profiles**.

The Content Filtering Profiles page appears, displaying the existing content filtering profiles.

2. Select one or more custom content filtering profiles that you want to delete and click the delete icon.

An alert message appears, asking you to confirm the delete operation.

3. Click **Yes** to delete the selected content filtering profiles.

A confirmation message appears, indicating the status of the delete operation.

About the Content Filtering Policy (New) Page

A content filtering policy enable you to filter content and manage the traffic on devices running Junos OS Release 21.4 or later. The policy filters the content based on the file extension and traffic direction.

NOTE: To filter content and manage traffic on devices running Junos OS Releases earlier than 21.4, go to the ["Content Filtering Profiles" on page 427](#) page.

After you create a content filter policy, you must assign it to a content security profile, then assign it to a security policy that will be deployed on the device.

The **Content Filtering Policy (New)** page enables you to create, edit, delete, and clone content filtering policies. It displays the policy name, policy description, and the number of rules in a policy.

To access the **Content Filtering Policy (New)** page, go to **SRX > Security Subscriptions > Content Security > Content Filtering Policies (New)**.

Create a Content Filtering Policy

Before You Begin

Ensure that the device is running Junos OS Release 21.4 or later.

About The Task

A content filtering policy enable you to filter content and manage the traffic on devices based on the file extension and traffic direction.

To create a content filter policy:

1. Go to **SRX > Security Subscriptions > Content Security > Content Filtering Policies (New)**.
The **Content Filtering Policy (New)** page is displayed.
2. Click the + icon above the table.
The **Create Content Filtering Policy** page is displayed.
3. Enter a unique policy name with alphanumeric characters, dashes, or underscores. The name must be within 255 characters and must not contain spaces.
4. Enter a policy description within 255 characters.
5. Click **OK**.
The policy is created and displayed on the **Content Filtering Policy (New)** page.

What's Next

["Add Rules in a Content Filtering Policy" on page 437](#)

Add Rules in a Content Filtering Policy

Before You Begin

"[Create a Content Filtering Policy](#)" on page 436 .

About The Task

After you create a content filtering policy, you can add rule(s) to the policy to define the filtering criteria. You can configure Juniper Security Director Cloud to filter the traffic based on file types and direction.

To add a rule in a content filtering policy:

1. Go to **SRX > Security Subscriptions > Content Security > Content Filtering Policies (New)**. The **Content Filtering Policy (New)** page is displayed.
2. In the **Rules** column, click **Add Rules** beside the policy in which you want to add rule(s).

NOTE: If rule(s) already exists for the policy, the number of rules in the policy are displayed in the **Rules** column.

The policy overview page is displayed.

3. Click the + icon.
4. Enter an alphanumeric name within 29 characters for the rule. The name can contain colons, periods, slashes, dashes and underscores.
5. Select the rule group to which you want to associate the rule. You can also click **Create Rule Group** to create a new rule group.
6. Select the direction of the traffic to be inspected.
7. In the **File Types** column, click the + icon, select the file types that must be filtered, and then click **OK**.
8. In the **Action** column, select the action that must be taken on the filtered file types.
 - **No Action**-No action is required.
 - **Block**-Block and drop the connection
 - **Close Client**-Close the client connection
 - **Close Server**-Close the server connection
 - **Close Client And Server**-Close the client and the server connection
9. In the **Options** column, perform the following steps:
 - Enable the **Event logs** toggle switch to enable logging for the filter.

- Enable the **End user notification** toggle switch to notify users when content is blocked. You can also configure a custom notification message within 512 characters.

NOTE: The **End user notification** toggle switch is enabled only if you select **Block** in the **Action** column.

10. Click the tick icon.

The rule is created and is nested under the rule group in the policy overview page. You can create multiple rules under the same rule group or different rule groups.

What's Next

1. Assign the content filtering policy to a content security profile. See "[Create a Content Security Profile](#)" on page 395 .
2. Select the profile when you add or edit the required security policy rule. See "[Add a Security Policy Rule](#)" on page 307 .

Edit a Content Filtering Policy

To edit a content filter policy:

1. Go to **SRX > Security Subscriptions > Content Security > Content Filtering Policies (New)**.
The **Content Filtering Policy (New)** page is displayed.
2. Select the policy that you want to edit and click the pencil icon above the table.
The **Edit Content Filtering Policy** page is displayed.
3. Modify the required details and click **OK**.

What's Next

Redeploy the SRX policy that is associated with the content filtering policy. See "[Deploy Security Policies](#)" on page 325 .

Clone a Content Filtering Policy

To clone a content filter policy:

1. Go to **SRX > Security Subscriptions > Content Security > Content Filtering Policies (New)**.
The **Content Filtering Policy (New)** page is displayed.
2. Select the policy that you want to clone, click **More**, and then click **Clone**.
The **Clone Content Filtering Policy** page is displayed.
3. Modify the required details and click **OK**.

NOTE: The policy name is suffixed with `_copy_1`.

The policy is cloned and displayed on the **Content Filtering Policy (New)** page.

Edit a Content Filtering Policy Rule

To edit a content filtering policy rule:

1. Go to **SRX > Security Subscriptions > Content Security > Content Filtering Policies (New)**.
The **Content Filtering Policy (New)** page is displayed.
2. Click the policy name to which the rule that you want to modify is added.
The policy overview page is displayed.
3. Expand the rule group to which the rule is assigned.
4. Select the required rule and click the pencil icon.
5. Modify the required fields and click the tick icon.

What's Next

Redeploy the SRX policy that is associated with the content filtering policy. See "[Deploy Security Policies](#)" on page 325 .

Clone a Content Filtering Policy Rule

1. Go to **SRX > Security Subscriptions > Content Security > Content Filtering Policies (New)**.
The **Content Filtering Policy (New)** page is displayed.
2. Click the policy name to which the rule that you want to modify is added.
The policy overview page is displayed.
3. Expand the rule group to which the rule is assigned.
4. Select the rule that you want to clone, click **More**, and then click **Clone**.
The rule is cloned and displayed.

NOTE: The rule name is suffixed with `_clone_1`.

5. Modify the required fields and click the tick icon.
The rule is created and nested under the corresponding rule group.

Security Subscriptions-Decrypt Profiles

IN THIS CHAPTER

- [Decrypt Profiles Overview | 440](#)
- [About the Decrypt Profiles Page | 447](#)
- [Create a Decrypt Profile | 449](#)
- [Edit, Clone, and Delete a Decrypt Profile | 457](#)

Decrypt Profiles Overview

IN THIS SECTION

- [Supported Ciphers in Proxy Mode | 442](#)
- [Server Authentication | 444](#)
- [Root CA | 445](#)
- [Trusted CA List | 445](#)
- [Session Resumption | 445](#)
- [SSL Proxy Logs | 445](#)

Secure Sockets Layer (*SSL*) is an application-level protocol that provides encryption technology for the Internet. *SSL*, also called *Transport Layer Security* (*TLS*), ensures the secure transmission of data between a client and a server through a combination of privacy, authentication, confidentiality, and data integrity. *SSL* relies on certificates and private–public key exchange pairs for this level of security.

Server authentication guards against fraudulent transmissions by enabling a Web browser to validate the identity of a Web server. Confidentiality mechanisms ensure that communications are private. *SSL* enforces confidentiality by encrypting data to prevent unauthorized users from eavesdropping on

electronic communications. Finally, message integrity ensures that the contents of a communication have not been tampered with.

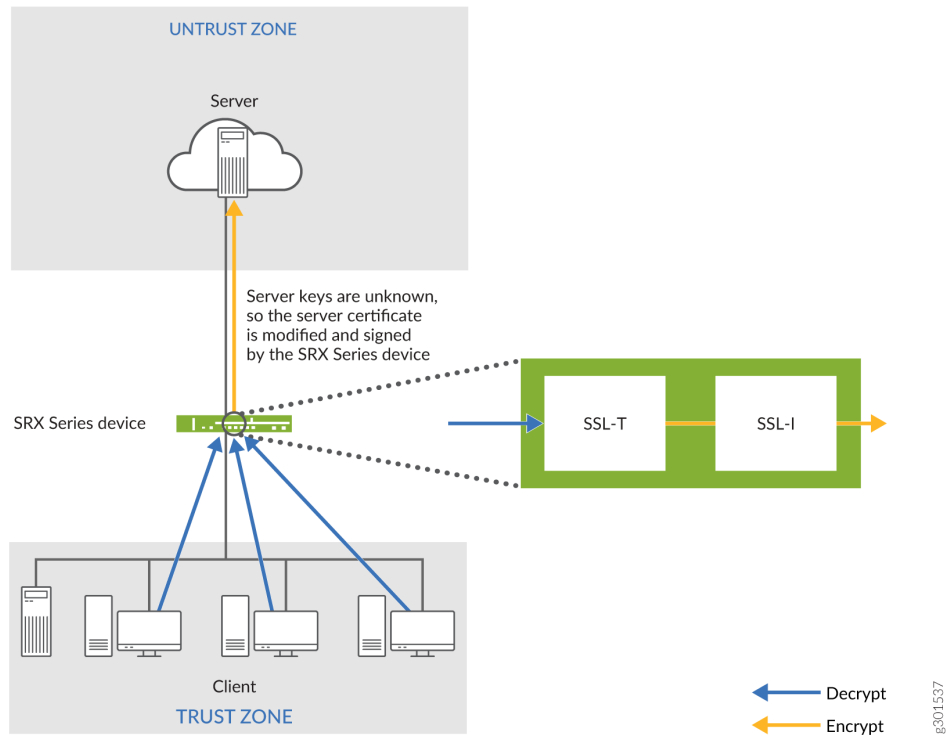
SSL proxy performs SSL encryption and decryption between the client and the server, but neither the server nor the client can detect its presence. SSL proxy ensures that it has the keys to encrypt and decrypt the payload:

- For the server, SSL proxy acts as a client—SSL proxy generates the shared pre-master key, it determines the keys to encrypt and decrypt.
- For the client, SSL proxy acts as a server—SSL proxy first authenticates the original server and replaces the public key in the original server certificate with a key that is known to it. It then generates a new certificate by replacing the original issuer of the certificate with its own identity and signs this new certificate with its own public key (provided as a part of the proxy profile configuration). When the client accepts such a certificate, it sends a shared pre-master key encrypted with the public key on the certificate. Because SSL proxy replaced the original key with its own key, it is able to receive the shared pre-master key. Decryption and encryption take place in each direction (client and server), and the keys are different for both encryption and decryption.

[Figure 13 on page 442](#) shows how SSL proxy works on an encrypted payload. SSL proxy uses the following services:

- SSL-T-SSL terminator on the client side.
- SSL-I-SSL initiator on the server side.

Figure 13: SSL Proxy on an Encrypted Payload



This topic has the following sections:

Supported Ciphers in Proxy Mode

An SSL cipher comprises encryption ciphers, authentication method, and compression. [Table 175 on page 442](#) displays a list of supported ciphers. NULL ciphers are excluded.

The following SSL protocols are supported:

- SSLv3
- TLS1

Table 175: Supported Ciphers in Proxy Mode

SSL Cipher	Key Exchange Algorithm	Data Encryption	Message Integrity
RSA_WITH_RC4_128_MD5	RSA key exchange	128-bit RC4	MD5 hash

Table 175: Supported Ciphers in Proxy Mode (Continued)

SSL Cipher	Key Exchange Algorithm	Data Encryption	Message Integrity
RSA_WITH_RC4_128_SHA	RSA key exchange	128-bit RC4	Secure Hash Algorithm (SHA) hash
RSA_WITH_DES_CBC_SHA	RSA key exchange	DES CBC	SHA hash
RSA_WITH_3DES_EDE_CBC_SHA	RSA key exchange	3DES EDE/CBC	SHA hash
RSA_WITH_AES_128_CBC_SHA	RSA key exchange	128-bit AES/CBC	SHA hash
RSA_WITH_AES_256_CBC_SHA	RSA key exchange	256-bit AES/CBC	SHA hash
RSA_EXPORT_WITH_RC4_40_MD5	RSA-export	40-bit RC4	MD5 hash
RSA_EXPORT_WITH_DES40_CBC_SHA	RSA-export	40-bit DES/CBC	SHA hash
RSA_EXPORT1024_WITH_DES_CBC_SHA	RSA 1024 bit export	DES/CBC	SHA hash
RSA_EXPORT1024_WITH_RC4_56_MD5	RSA 1024 bit export	56-bit RC4	MD5 hash
RSA_EXPORT1024_WITH_RC4_56_SHA	RSA 1024 bit export	56-bit RC4	SHA hash
RSA-WITH-AES-256-GCM-SHA384	RSA key exchange	256-bit AES/GCM	SHA384 hash

Table 175: Supported Ciphers in Proxy Mode (Continued)

SSL Cipher	Key Exchange Algorithm	Data Encryption	Message Integrity
RSA-WITH-AES-256-CBC-SHA256	RSA key exchange	256-bit AES/CBC	SHA256 hash
RSA-WITH-AES-128-GCM-SHA256	RSA key exchange	128-bit AES/GCM	SHA256 hash
RSA-WITH-AES-128-CBC-SHA256	RSA key exchange	128-bit AES/CBC	SHA256 hash

Server Authentication

Implicit trust between the client and the device (because the client accepts the certificate generated by the device) is an important aspect of SSL proxy. It is extremely important that server authentication is not compromised; however, in reality, self-signed certificates and certificates with anomalies are in abundance. Anomalies can include expired certificates, instances of common name not matching a domain name, and so forth.

You can specify that the SSL proxy should ignore server authentication completely. In this case, SSL proxy ignores errors encountered during the server certificate verification process (such as CA signature verification failure, self-signed certificates, and certificate expiry).

You can specify whether the SSL proxy should ignore server authentication errors or not during the creation of an SSL proxy profile.

- If you specify that server authentication errors should *not* be ignored, the following scenarios occur:
 - If authentication succeeds, a new certificate is generated by replacing the keys and changing the issuer name to the issuer name that is configured in the root CA certificate in the proxy profile.
 - If authentication fails, the connection is dropped.
- If you specify that server authentication errors should be ignored, the following scenarios occur:

NOTE: We do not recommend that you configure 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.

- If the certificate is self-signed, a new certificate is generated by replacing the keys only. The issuer name is not changed. This ensures that the client browser displays a warning that the certificate is not valid.
- If the certificate has expired or if the common name does not match the domain name, a new certificate is generated by replacing the keys and changing the issuer name to SSL-PROXY: DUMMY_CERT:GENERATED DUE TO SRVR AUTH FAILURE. This ensures that the client browser displays a warning that the certificate is not valid.

Root CA

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.

Trusted CA List

SSL proxy ensures secure transmission of data between a client and a server. Before establishing a secure connection, SSL 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.

Session Resumption

An SSL session refers to the set of parameters and encryption keys that are created when a full handshake is performed. A connection is the conversation or active data transfer that occurs within the session. The computational overhead of a complete SSL handshake and generation of primary keys is considerable. In short-lived sessions, the time taken for the SSL handshake can be more than the time for data transfer. To improve throughput and still maintain an appropriate level of security, SSL session resumption provides a mechanism for caching sessions. This way, session information, such as the pre-master secret key and agreed-upon ciphers, can be cached for both the client and the server. A session ID identifies the cached information. In subsequent connections, both parties agree to use the session ID to retrieve the information rather than create pre-master secret key. Session resumption shortens the *handshake* process and accelerates SSL transactions.

SSL Proxy Logs

When logging is enabled in an decrypt profile, the SSL proxy can generate the messages shown in [Table 176 on page 446](#) .

Table 176: SSL Proxy Logs

Log Type	Description
All	All logs are generated.
Warning	Logs used for reporting warnings.
Info	Logs used for reporting general information.
Error	Logs used for reporting errors.
Session Whitelisted	Logs generated when a session is allowed.
Session Allowed	Logs generated when a session is processed by SSL proxy even after encountering some minor errors.
Session Dropped	Logs generated when a session is dropped by SSL proxy.

All logs contain similar information; the message field contains the reason for the log generation. One of three prefixes shown in [Table 177 on page 446](#) identifies the source of the message. Other fields are descriptively labeled.

Table 177: SSL Proxy Log Prefixes

Prefix	Description
system	Logs generated because of errors related to the device or an action taken as part of the decrypt profile. Most logs fall into this category.
openssl error	Logs generated during the <i>handshake</i> process if an error is detected by the openssl library.

Table 177: SSL Proxy Log Prefixes (*Continued*)

Prefix	Description
certificate error	Logs generated during the handshake process if an error is detected in the certificate (X.509 related errors).

About the Decrypt Profiles Page

IN THIS SECTION

- [Tasks You Can Perform | 447](#)
- [Widget Descriptions | 447](#)

To access this page, click **Security Subscriptions > Decrypt > Decrypt Profiles**. Use the Decrypt Profiles page to view and to manage decrypt profiles.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create an decrypt profile—See ["Create a Decrypt Profile" on page 449](#) .
- Edit, clone, or delete an decrypt profile—See ["Edit, Clone, and Delete a Decrypt Profile" on page 457](#) .
- View the details of an decrypt profile—Select the decrypt profile for which you want to view the details and from the More or right-click menu, select **Detailed View**. The View decrypt profile Details page appears. [Table 179 on page 448](#) describes the fields on this page.
- Search for decrypt profiles using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results appear on the same page.

Widget Descriptions

[Table 178 on page 448](#) describes the fields on the decrypt Profiles page.

Table 178: Fields on the Decrypt Profiles Page

Field	Description
Name	Name of the decrypt profile.
Preferred Cipher	Preferred cipher associated with the profile.
Custom Ciphers	The set of ciphers, if the preferred cipher is Custom , which the SSH server uses to perform the encryption and the decryption functions.
Exempted Address	Addresses that are exempted from decrypt processing.
Description	Description of the decrypt profile.
Root Certificate	Root certificate associated with the decrypt profile.

Table 179: View Decrypt Profile Details Page Fields

Field	Description
General Information	
Name	Name of the decrypt profile.
Description	Description of the decrypt profile.
Preferred Cipher	Preferred cipher associated with the proxy profile.
Custom Ciphers	The set of ciphers, if the preferred cipher is Custom , which the SSH server uses to perform the encryption and the decryption functions.
Flow Trace Enabled	Indicates whether flow tracing is enabled or disabled.

Table 179: View Decrypt Profile Details Page Fields (*Continued*)

Field	Description
Certificates	Displays the root certificate and the trusted certificate authorities associated with the root certificate.
Exempted Address	Addresses that are exempted from decrypt processing.
Exempted URL Categories	URL categories that are exempted from decrypt processing.
Actions	
Ignore	Indicates whether server authentication failure is ignored (Enabled) or not (Disabled).
Session Resumption	Indicates whether session information is cached to enable session resumption (Enabled) or not (Disabled).
Logging	If logging is enabled, indicates the type of events that are logged.
Renegotiation	Indicates the type of renegotiation required for a change in SSL parameters after creating a session and establishing the SSL tunnel transport.

Create a Decrypt Profile

Use this page to configure decrypt profiles. decrypt profile is enabled as an application service within a security policy.

To create an decrypt profile:

NOTE: Ensure that you have a root certificate imported for the tenant before you create an decrypt profile. You can import SSL certificates (root and trusted) from the Certificates page (**Administration > Certificates**) and associate the certificates with decrypt profiles.

1. Select Security Subscriptions > Decrypt.

The decrypt profiles page appears.

2. Click the add icon (+) to create an decrypt profile.

The Create Decrypt Profiles page appears.

3. Complete the configuration according to the guidelines provided in [Table 180 on page 450](#) .

Fields marked with an asterisk (*) are mandatory.

4. Click OK.

An decrypt profile is created. You are returned to the decrypt Profiles page where a confirmation message is displayed.

Table 180: Decrypt Profile Settings

Setting	Guideline
General Information	
Name	Enter a unique name for the profile, which is string of alphanumeric characters and some special characters (- _). No spaces are allowed and the maximum length is 63 characters.
Description	Enter a description for the profile. The maximum length is 255 characters.

Table 180: Decrypt Profile Settings (Continued)

Setting	Guideline
Preferred Cipher	<p>Select a preferred cipher. Preferred ciphers enable you to define an SSL cipher that can be used with acceptable key strength. You can select from the following categories:</p> <ul style="list-style-type: none">• None (Default)—Do not specify a preferred cipher.• 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 a custom cipher suite.

Table 180: Decrypt Profile Settings (Continued)

Setting	Guideline
Custom Ciphers	<p>If you specified Custom as the preferred cipher, you can define a custom cipher list by selecting ciphers.</p> <p>Select the set of ciphers that the SSH server can use to perform encryption and decryption functions.</p> <p>The available custom ciphers are:</p> <ul style="list-style-type: none"> • rsa-with-RC4-128-md5—RSA, 128- bit RC4, MD5 hash • rsa-with-RC4-128-sha—RSA, 128-bit RC4, SHA hash • rsa-with-des-cbc-sha—RSA, DES/CBC, SHA hash • rsa-with-3DES-edc-cbc-sha—RSA, 3DES EDE/ CBC, SHA hash • rsa-with-aes-128-cbc-sha—RSA, 128-bit AES/ CBC, SHA hash • rsa-with-aes-256-cbc-sha—RSA, 256 bit AES/ CBC, SHA hash • rsa-export-with-rc4-40-md5—RSA-export, 40 bit RC4, MD5 hash • rsa-export-with-des40-cbc-sha—RSA-export, 40 bit DES/CBC, SHA hash • rsa-export1024-with-des-cbc-sha—RSA 1024 bit export, DES/CBC, SHA hash • rsa-export1024-with-rc4-56-md5—RSA 1024 bit export, 56 bit RC4, MD5 hash • rsa-export1024-with-rc4-56-sha—RSA 1024 bit export, 56 bit RC4, SHA hash • rsa-with-aes-256-gcm-sha384—RSA, 256 bit AES/GCM, SHA384 hash

Table 180: Decrypt Profile Settings (Continued)

Setting	Guideline
	<ul style="list-style-type: none"> • rsa-with-aes-256-cbc-sha256—RSA, 256 bit AES/CBC, SHA256 hash • rsa-with-aes-128-gcm-sha256—RSA, 128 bit AES/GCM, SHA256 hash • rsa-with-aes-128-cbc-sha256—RSA, 256 bit AES/CBC, SHA256 hash • ecdhe-rsa-with-aes-256-gcm-sha384—ECDHE, RSA, 256 bit AES/GCM, SHA384 hash • ecdhe-rsa-with-aes-256-cbc-sha384—ECDHE, RSA, 256 bit AES/CBC, SHA384 hash • ecdhe-rsa-with-aes-256-cbc-sha—ECDHE, RSA, 256 bit AES/CBC, SHA hash • ecdhe-rsa-with-aes-3des-ede-cbc-sha—ECDHE, RSA, 3DES, EDE/CBC, SHA hash • ecdhe-rsa-with-aes-128-gcm-sha256—ECDHE, RSA, 128 bit AES/GCM, SHA256 hash • ecdhe-rsa-with-aes-128-cbc-sha256—ECDHE, RSA, 128 bit AES/CBC, SHA256 hash • ecdhe-rsa-with-aes-128-cbc-sha—ECDHE, RSA, 128 bit AES/CBC, SHA hash
Flow Trace	Move this toggle button to enable flow tracing for troubleshooting the policy-related issues.
Root Certificate	<p>Select or add a <i>root certificate</i>. In a public key infrastructure (PKI) hierarchy, the root certificate authority (CA) is at the top of the trust path.</p> <p>NOTE: To select the root certificate from the device, you must ensure that at least one trusted certificate is installed on the device.</p>

Table 180: Decrypt Profile Settings (Continued)

Setting	Guideline
Trusted Certificate Authorities	<p>Choose whether you want to add all trusted certificates present on the device (All) or select specific trusted certificates. Before establishing a secure connection, the decrypt checks CA certificates to verify signatures on server certificates.</p> <p>NOTE:</p> <ul style="list-style-type: none">• Specifying that all trusted certificates should be used means that all trusted certificates on a particular device (site) are used during SSL policy deployment.• If you specify that all trusted certificates should be used in an decrypt profile, you must ensure that at least one trusted certificate is installed on the device.

Table 180: Decrypt Profile Settings (Continued)

Setting	Guideline
Exempted Addresses	<p>Exempted addresses include addresses that you want to exempt from undergoing decrypt processing.</p> <p>To specify exempted addressees, select one or more addresses in the Available column and click the forward arrow to confirm your selection. The selected addresses are then displayed in the Selected column. These addresses are used to create allowlists that bypass decrypt processing.</p> <p>Because SSL encryption and decryption are complicated and expensive procedures, network administrators can selectively bypass decrypt processing for some sessions.</p> <p>Such sessions typically 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> <p>NOTE: You can also add addresses by clicking Add Address. The Create Addresses page appears. See "Create Addresses or Address Groups" on page 863.</p>
Exempted URL Categories	<p>Select the previously defined URL categories to create allowlists that bypass decrypt processing. The selected URL categories are exempted during SSL inspection.</p> <p>NOTE: To select Juniper NextGen categories, you must have Junos OS version 23.4R1 or later installed.</p>
Actions	

Table 180: Decrypt Profile Settings (Continued)

Setting	Guideline
Server Auth Failure	<p>Select this check box to ignore errors encountered during the server certificate verification process (such as CA signature verification failure, self-signed certificates, and certificate expiry). This check box is cleared by default.</p> <p>We do not recommend this option for authentication, because configuring it results in websites not being authenticated at all. However, you can use this option to effectively identify the root cause for dropped SSL sessions.</p>
Session Resumption	<p>Select this check box to disable session resumption. This check box is cleared by default.</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 one or more events to be logged. You can choose to log all events, warnings, general information, errors, or different sessions (allowed, dropped, or ignored). Logging is disabled by default.</p>

Table 180: Decrypt Profile Settings (Continued)

Setting	Guideline
Renegotiation	<p>Select one of the following options if a change in SSL parameters requires renegotiation:</p> <ul style="list-style-type: none"> • None (default)—Indicates that renegotiation is not required. • Allow—Allow secure and nonsecure renegotiation. • Allow Secure—Allow secure negotiation only. • Drop—Drop session on renegotiation request. <p>After a session is created and SSL tunnel transport has been established, a change in SSL parameters requires renegotiation. decrypt supports both secure (RFC 5746) and nonsecure (TLS v1.0 and SSL v3) 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.

Edit, Clone, and Delete a Decrypt Profile

IN THIS SECTION

- [Edit a Decrypt Profile | 458](#)
- [Clone an Decrypt Profile | 458](#)
- [Delete a Decrypt Profile | 458](#)

You can edit, clone, and delete decrypt profiles from the decrypt Profiles page.

Edit a Decrypt Profile

To modify the parameters configured for an decrypt profile:

1. Select **Security Subscriptions > Decrypt**.

The Decrypt Profiles page appears, displaying the existing decrypt profiles.

2. Select the decrypt profile that you want to edit and then click the edit icon (pencil).

The Edit decrypt profile page appears showing the same fields that are presented when you create an decrypt profile.

3. Modify the decrypt profile fields as needed.

4. Click **OK** to save your changes.

The modified decrypt Profiles page appears.

Clone an Decrypt Profile

Cloning enables you to easily decrypt profile based on an existing one.

To clone an decrypt profile:

1. Select **Security Subscriptions > Decrypt**.

The decrypt Profiles page appears displaying the existing decrypt profiles.

2. Select the decrypt profile that you want to clone and then select **More > Clone**. Alternatively, right-click a profile and select **Clone**.

The Clone decrypt profile page appears, showing the same fields when you create an decrypt profile.

3. Modify the decrypt profile fields as needed.

4. Click **OK** to save your changes.

Decrypt Profiles page appears. A confirmation message appears, indicating the status of the clone operation.

Delete a Decrypt Profile

1. Select **Security Subscriptions > Decrypt**.

The decrypt Profiles page appears, displaying the existing decrypt profiles.

2. Select one or more decrypt profiles that you want to delete and then click the delete icon.

An alert message appears asking you to confirm the delete operation.

3. Click **Yes** to delete the selected decrypt profiles.

A confirmation message appears indicating the status of the delete operation.

Security Subscriptions-SecIntel

IN THIS CHAPTER

- [Security Intelligence Overview | 459](#)
- [SecIntel Profiles Overview | 461](#)
- [About SecIntel Profiles Page | 462](#)
- [Create Command and Control Profile | 463](#)
- [Create DNS Profile | 466](#)
- [Create Infected Hosts Profile | 468](#)
- [Edit, Clone, and Delete SecIntel Profile | 470](#)
- [About SecIntel Profile Groups Page | 472](#)
- [Create SecIntel Profile Group | 473](#)
- [Edit, Clone, and Delete SecIntel Profile Group | 475](#)
- [Associate a SecIntel Profile Group to a Security Policy | 476](#)

Security Intelligence Overview

Juniper Networks Security Intelligence (SecIntel) is a security framework that protects against evolving security threats by employing cloud-based security information. SecIntel provides carefully curated and verified threat intelligence from industry-leading threat feeds from ATP Cloud to Juniper Security Director Cloud.

You can create SecIntel profiles for the SRX Series Firewalls in Juniper Security Director Cloud. SecIntel profiles enable you to block malicious and unwanted traffic such as Command and Control (C&C) communications, compromised IP address or IP subnet, and domains connected to malicious activity.

You can create a SecIntel profile group by using combination of C&C, DNS, and infected-host profiles. After you create a SecIntel profile group, you can assign the profile group to a security policy. When an infected host on the cloud network tries to initiate contact with a possible command and control (C&C) server on the Internet, the SRX Series Firewall eliminates such threats based on the deployed security policy.

Figure 14: SecIntel Profile Group

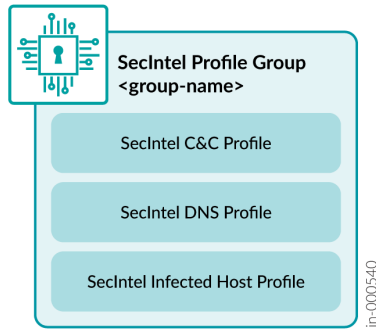
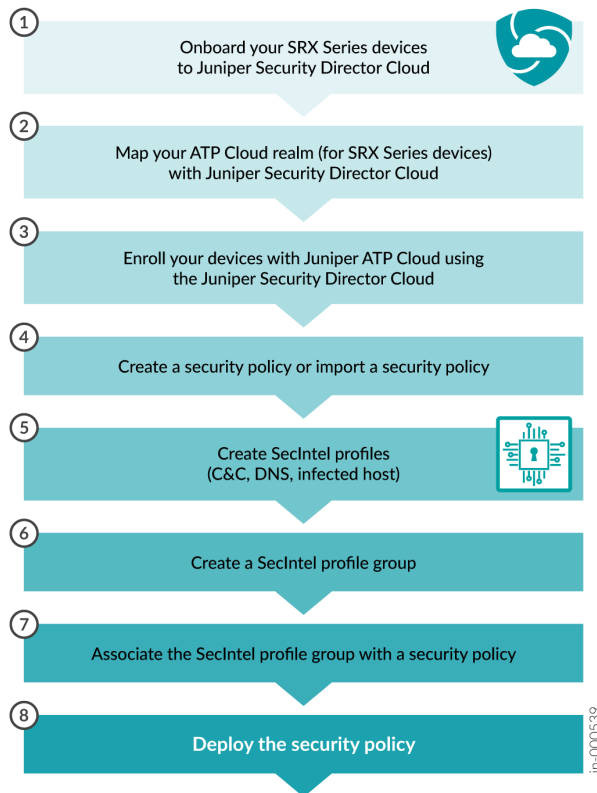


Figure 15 on page 460 shows the high-level steps for SecIntel configurations.

Figure 15: Juniper Security Director Cloud Workflow with SecIntel Configuration



SecIntel offers the following benefits:

- Detect and block known malicious IP addresses and DNS requests.
- Quarantine the compromised internal hosts.
- Identify the connected devices that are at risk.
- Shut down attacks before they start.
- Protect users (including subscribers), applications, and infrastructure from compromise.
- Turn connectivity layers into security layers without additional infrastructure.

RELATED DOCUMENTATION

[Add Devices to Juniper Security Director Cloud | 222](#)

[Map an Existing ATP Realm to Juniper Security Director Cloud | 1060](#)

[Add a Security Policy | 290](#)

[Import Security Policies | 298](#)

[Create Command and Control Profile | 463](#)

[Create DNS Profile | 466](#)

[Create Infected Hosts Profile | 468](#)

[Create SecIntel Profile Group | 473](#)

[Associate a SecIntel Profile Group to a Security Policy | 476](#)

[Deploy Security Policies | 325](#)

[SecIntel Feeds Overview](#)

[SecIntel on SRX Series Firewalls](#)

SecIntel Profiles Overview

You can create SecIntel profiles for the SRX Series Firewalls in Juniper Security Director Cloud. Secintel profiles enable you to block malicious and unwanted traffic such as Command and Control (C&C) communications, compromised IP address or IP subnet, and domains connected to malicious activity.

The following SecIntel profiles are supported:

- **SecIntel (C&C) Profile:** Provides information on C&C servers that have attempted to contact and compromise hosts on your network. A C&C server is a centralized computer that issues commands to botnets of compromised networks of computers and receives reports back from them.

- **SecIntel DNS Profile:** Includes feeds and threat score to list the domains that are known to be connected to malicious activity.
- **SecIntel Infected Host Profile:** Includes feeds and threat score to list the IP address or IP subnet of the compromised host. Infected hosts indicate local devices that are potentially compromised because they appear to be part of a C&C network or exhibit other symptoms.

Configure SecIntel profiles to work with security intelligence feeds, such as C&C, DNS, and infected hosts. The SecIntel process downloads the SecIntel feeds and parses from the feed connector or ATP Cloud feed server. Anything that matches these scores is considered malware or an infected host.

RELATED DOCUMENTATION

[About SecIntel Profiles Page | 462](#)

[About SecIntel Profile Groups Page | 472](#)

About SecIntel Profiles Page

IN THIS SECTION

- [Tasks You Can Perform | 462](#)
- [Field Description | 463](#)

To access this page, select **SRX > Security Subscriptions > SecIntel > Profiles**.

Use the SecIntel Profiles page to manage Command & Control (C&C), DNS, and Infected Hosts profile.

Tasks You Can Perform

You can perform the following tasks from this page:

- View the list of C&C, DNS, and infected hosts profiles. Click **View by** list and select Command & Control, DNS, or Infected Hosts profile.
- Create a command and control profile—See "[Create Command and Control Profile](#)" on page 463 .
- Create a DNS profile—See "[Create DNS Profile](#)" on page 466 .

- Create an infected hosts profile—See ["Create Infected Hosts Profile" on page 468](#) .
- Edit, clone, or delete SecIntel profile—See ["Edit, Clone, and Delete SecIntel Profile" on page 470](#)
- Associate a SecIntel profile to a security policy—See ["Add a Security Policy Rule" on page 307](#)
- Show or hide columns in the SecIntel 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.
- Reset Preference—Reset the displayed columns to the default set of columns for each tab in the table.

Hover over the More Options (vertical ellipsis) and select **Reset Preference**.

Field Description

[Table 181 on page 463](#) describes the fields on the SecIntel Profiles page.

Table 181: Fields on the SecIntel Profiles Page

Field	Description
Name	Displays the SecIntel profile name.
Type	Displays if the SecIntel profile is a C&C, a DNS, or an infected hosts profile.
Block action	Displays the notification action taken with the block action. For example, Close session, Drop packet, and Sinkhole.
Description	Displays the description of the SecIntel profile.

Create Command and Control Profile

Create a Command and Control (C&C) profile to provide information on C&C servers that have attempted to contact and compromise hosts on your network. A C&C server is a centralized computer that issues commands to botnets of compromised networks of computers and receives reports back from them.

To create a C&C profile:

1. Click **SRX > Security Subscriptions > SecIntel > Profiles**.
The SecIntel Profiles page opens.
2. Select **Create > Command & Control**.
The Create Command & Control Profile page appears.
3. Complete the configuration according to the guidelines provided in .
4. Click **OK** to save the changes. To discard your changes, click **Cancel**.
After creating a C&C profile, you can associate it with the SecIntel profile groups.

Table 182: Fields on the Create Command & Control Profile page

Field	Action
Name	Enter a name for the C&C profile. The name must be a unique string of alphanumeric and special characters; 63-character maximum. Special characters < and > are not allowed.
Description	Enter a description for the C&C profile.
Default action for all feeds	Drag the slider to change the action to be taken for all the feed types. Actions are Permit (1 - 4), Log (5-6), and Block (7 - 10). Log will have the permit action and also logs the event.

Table 182: Fields on the Create Command & Control Profile page (*Continued*)

Field	Action
Specific action for feeds	<p>Do the following:</p> <ol style="list-style-type: none"> a. Click + to define feeds and threat score for the C&C profile. The Add Feeds window appears. b. Enter the following details: <ol style="list-style-type: none"> i. Feeds—Select one or more feeds that are known command and control for botnets from the Available column and move it to the Selected column. ii. Threat score—Drag the slider to change the action to be taken based on the threat score. c. Click OK.
Block action	<p>Select one of the following block actions from the list:</p> <ul style="list-style-type: none"> • Close session—Device sends a TCP RST packet to the client and server and the session is dropped immediately. • Drop Packets—Device silently drops the session’s packet and the session eventually times out.
Close session options	<p>Select one of the following options from the list: None, Redirect URL, or Redirect message.</p>
Redirect URL	<p>Enter a remote file URL to redirect users when connections are closed.</p>
Redirect message	<p>Enter a custom message to send to the users when connections are closed.</p>

RELATED DOCUMENTATION

[SecIntel Profiles Overview | 461](#)

[About SecIntel Profiles Page | 462](#)

[Create SecIntel Profile Group | 473](#)

Create DNS Profile

Create a DNS profile to configure feeds and threat score to list the domains that are known to be connected to malicious activity.

To create a DNS profile:

1. Click **SRX > Security Subscriptions > SecIntel > Profiles**.
The SecIntel Profiles page appears.
2. Select **Create > DNS**.
The Create DNS Profile page appears.
3. Complete the configuration according to the guidelines provided in [Table 183 on page 466](#).
4. Click **OK** to save the changes. To discard your changes, click **Cancel**.

Once you create the DNS profile, you can associate it with the SecIntel profile groups.

Table 183: Fields on the Create DNS Profile Page

Field	Action
Name	Enter a name for the DNS profile. The name must be a unique string of alphanumeric and special characters; 63-character maximum. Special characters such as < and > are not allowed.
Description	Enter a description for the DNS profile.
Default action for all feeds	Drag the slider to change the action to be taken for all the feed types. Actions are Permit (1 - 4), Log (5-6), and Block (7 - 10). Log will have the permit action and also logs the event.

Table 183: Fields on the Create DNS Profile Page (Continued)

Field	Action
Specific action for feeds	<p>Do the following:</p> <ol style="list-style-type: none"> a. Click + to define feeds and threat score to the DNS profile. The Add Feeds window appears. b. Enter the following details: <ol style="list-style-type: none"> i. Feeds—Select one or more feeds from the Available column and move it to the Selected column to associate with the DNS profile. ii. Threat score—Drag the slider to change the action to be taken based on the threat score. c. Click OK.
Block action	<p>Select one of the following block actions from the list:</p> <ul style="list-style-type: none"> • Drop Packets—Device silently drops the session's packet and the session eventually times out. • Sinkhole—DNS sinkhole action for malicious DNS queries. DNS Sinkhole feature enables you to block DNS requests for the disallowed domains by resolving the domains to a sinkhole server or by rejecting the DNS requests.

RELATED DOCUMENTATION

[SecIntel Profiles Overview | 461](#)

[About SecIntel Profiles Page | 462](#)

[Create SecIntel Profile Group | 473](#)

Create Infected Hosts Profile

Infected hosts indicate local devices that are potentially compromised because they appear to be part of a C&C network or exhibit other symptoms. Create an Infected Hosts profile to configure feeds and threat score to list the IP address or IP subnet of the compromised host.

To create an Infected Host profile:

1. Click **SRX > Security Subscriptions > SecIntel > Profiles**.
The SecIntel Profiles page appears.
2. Select **Create > Infected Hosts**.
The Create Infected Hosts Profile page appears.
3. Complete the configuration according to the guidelines provided in [Table 184 on page 468](#).
4. Click **OK** to save the changes. To discard your changes, click **Cancel**.

Once you create the Infected Hosts profile, you can associate it with the SecIntel profile groups.

Table 184: Fields on the Create Infected Hosts Profile Page

Field	Action
Name	Enter a name for the Infected Hosts profile. The name must be a unique string of alphanumeric and special characters; 63-character maximum. Special characters such as < and > are not allowed.
Description	Enter a description for the Infected Hosts profile.
Default action for all feeds	Drag the slider to change the action to be taken for all the feed types. Actions are Permit (1 - 4), Log (5-6), and Block (7 - 10). Log will have the permit action and also logs the event.

Table 184: Fields on the Create Infected Hosts Profile Page (*Continued*)

Field	Action
Specific action for feeds	<p>Do the following:</p> <ol style="list-style-type: none"> a. Click + to define feeds and threat score to the Infected Hosts profile. The Add Feeds window appears. b. Enter the following details: <ol style="list-style-type: none"> i. Feeds—Select one or more feeds from the Available column and move it to the Selected column to associate with the Infected Hosts profile. ii. Threat score—Drag the slider to change the action to be taken based on the threat score. c. Click OK.
Block action	<p>Select one of the following block actions from the list:</p> <ul style="list-style-type: none"> • Drop Packets—Device silently drops the session's packet and the session eventually times out. • Close session—Device sends a TCP RST packet to the client and server and the session is dropped immediately.
Close session options	<p>Select one of the following options from the list: None, Redirect URL, or Redirect message.</p>
Redirect URL	<p>Enter a remote file URL to redirect users when connections are closed.</p>
Redirect message	<p>Enter a custom message to send to the users when connections are closed.</p>

RELATED DOCUMENTATION

- [SecIntel Profiles Overview | 461](#)

- [Add a Security Policy Rule | 307](#)

- [View Policy Version Details | 301](#)

- [Configure Global Options | 315](#)

- [Configure Default Rule Option | 318](#)

Edit, Clone, and Delete SecIntel Profile

IN THIS SECTION

- [Edit a SecIntel Profile | 470](#)
- [Clone a SecIntel Profile | 471](#)
- [Delete a SecIntel Profile | 471](#)

Edit a SecIntel Profile

To edit a SecIntel profile:

1. Click **SRX > Security Subscriptions > SecIntel > Profiles**.
The SecIntel Profiles page appears.
2. Select a profile, and click the edit (pencil) icon.
The Edit Profile page appears.
3. Modify the profile fields by following the guidelines provided in "[Create Command and Control Profile](#)" on page 463 , "[Create DNS Profile](#)" on page 466 , or "[Create Infected Hosts Profile](#)" on page 468 .
4. Click **OK** to save your changes.
The SecIntel Profiles page opens with a message that the profile was successfully updated.

If the SecIntel profile is referenced in a firewall policy intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.

Clone a SecIntel Profile

Cloning enables you to easily create a new SecIntel profile based on an existing one. You can clone a SecIntel profile and modify the parameters.

To clone a SecIntel profile:

1. Click **SRX > Security Subscriptions > SecIntel > Profiles**.

The SecIntel Profiles page appears.

2. Select a profile and select **More > Clone**.

The Clone Profile page appears.

3. Modify the profile fields by following the guidelines provided in "[Create Command and Control Profile](#)" on page 463 , "[Create DNS Profile](#)" on page 466 , or "[Create Infected Hosts Profile](#)" on page 468 .

4. Click **OK** to save your changes.

The SecIntel Profiles page opens with a message that the IPS profile was successfully created.

Delete a SecIntel Profile

To delete a SecIntel profile:

1. Click **SRX > Security Subscriptions > SecIntel > Profiles**.

The SecIntel Profiles page appears.

2. Select one or more SecIntel profiles, and click the delete (trash can) icon.

A warning message asking you to confirm the deletion is displayed.

3. Click **Yes** to proceed with the deletion.

The SecIntel Profiles page opens with a message indicating the status of the delete operation.

SEE ALSO

[SecIntel Profiles Overview | 461](#)

[About SecIntel Profiles Page | 462](#)

About SecIntel Profile Groups Page

IN THIS SECTION

- [Tasks You Can Perform | 472](#)
- [Field Description | 472](#)

To access this page, select **SRX > Security Subscriptions > SecIntel > Profile Groups**.

Configure a SecIntel profile group to add SecIntel profiles, such as C&C, DNS, and infected hosts. Once created, you can assign this group to the security policy.

Use the SecIntel Profiles page to manage SecIntel profile groups.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a SecIntel profile group—See ["Create SecIntel Profile Group" on page 473](#) .
- Edit, clone, or delete SecIntel profile group—See ["Edit, Clone, and Delete SecIntel Profile Group" on page 475](#) .
- Associate a SecIntel profile group to a security policy—See ["Associate a SecIntel Profile Group to a Security Policy" on page 476](#)
- Show or hide columns in the SecIntel 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.
- Reset Preference—Reset the displayed columns to the default set of columns for each tab in the table.

Hover over the More Options (vertical ellipsis) and select **Reset Preference**.

Field Description

The following table describes the fields on the SecIntel Profiles page.

Table 185: Fields on the SecIntel Profile Groups Page

Field	Description
Name	Displays the SecIntel profile group name.
Command & Control	Displays the C&C profile that you have associated with the SecIntel profile group.
DNS	Displays the DNS profile that you have associated with the SecIntel profile group.
Infected Hosts	Displays the infected hosts profile that you have associated with the SecIntel profile group.
Description	Displays the description of the SecIntel profile group.

Create SecIntel Profile Group

Create a SecIntel profile group with SecIntel profiles, such as C&C, DNS, and infected hosts. Once created, you can assign this group to the security policy.

To create a SecIntel profile group:

1. Click **SRX > Security Subscriptions > SecIntel > Profile Groups**.
The SecIntel Profile Groups page appears.
2. Click **+** on the upper-right corner of the SecIntel Profile Groups page.
The Create SecIntel Profile Groups page appears.
3. Complete the configuration according to the guidelines provided in [Table 186 on page 474](#).
4. Click **OK** to save the changes. To discard your changes, click **Cancel**.
Once you create the SecIntel profile group, you can associate it with the security policies.

Table 186: Fields on the Create SecIntel Profile Groups Page

Field	Action
Name	<p>Enter a name for the SecIntel profile group.</p> <p>The name must be a unique string of alphanumeric, special characters and 64-character maximum. Special characters such as <code>& ()] ? " # < ></code> are not allowed.</p>
Description	<p>Enter description for the SecIntel profile group.</p>
Command & Control	<p>Select a C&C profile from the list to associate with the SecIntel profile group.</p> <p>Click Create New to create a new C&C profile inline. For more information on a new C&C profile, see "Create Command and Control Profile" on page 463 .</p>
DNS	<p>Select a DNS profile from the list to associate with the SecIntel profile group.</p> <p>Click Create New to create a new DNS profile inline. For more information on a new DNS profile, see "Create DNS Profile" on page 466 .</p>
Infected Hosts	<p>Select the infected hosts profile from the list to associate with the SecIntel profile group.</p> <p>Click Create New to create a new infected hosts profile inline. For more information on a new infected hosts profile, see "Create Infected Hosts Profile" on page 468 .</p>

Edit, Clone, and Delete SecIntel Profile Group

IN THIS SECTION

- [Edit a SecIntel Profile Group | 475](#)
- [Clone a SecIntel Profile Group | 475](#)
- [Delete a SecIntel Profile Group | 476](#)

Edit a SecIntel Profile Group

To edit a SecIntel profile group:

1. Click **SRX > Security Subscriptions > SecIntel > Profile Groups**.

The SecIntel Profile Groups page appears.

2. Select a profile group, and click the edit (pencil) icon.

The Edit SecIntel Profile Group page appears.

3. Modify the profile fields. See "[Create SecIntel Profile Group](#)" on page 473 .

4. Click **OK** to save your changes.

The SecIntel Profile Groups page opens with a message that the profile was successfully updated.

If the SecIntel profile group is referenced in a firewall policy intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.

Clone a SecIntel Profile Group

Cloning enables you to easily create a SecIntel profile group based on an existing one. You can clone a SecIntel profile group and modify the parameters.

To clone a SecIntel profile group:

1. Click **SRX > Security Subscriptions > SecIntel > Profile Groups**.

The SecIntel Profile Groups page appears.

2. Select a SecIntel profile group and select **More > Clone**.

The Create SecIntel Profile Group page appears.

3. Modify the profile fields. See "[Create SecIntel Profile Group](#)" on page 473 .

4. Click **OK** to save your changes.

The SecIntel Profile Groups page opens with a message that the IPS profile was successfully created.

Delete a SecIntel Profile Group

To delete a SecIntel profile group:

1. Click **SRX > Security Subscriptions > SecIntel > Profile Groups**.

The SecIntel Profile Groups page appears.

2. Select one or more SecIntel profile groups, and click the delete (trash can) icon.

A warning message asks you to confirm the deletion.

3. Click **Yes** to proceed with the deletion.

The SecIntel Profile Groups page opens with a message indicating the status of the delete operation.

Associate a SecIntel Profile Group to a Security Policy

SecIntel profile group are used to add SecIntel profiles, such as C&C, DNS, and infected hosts.

To associate a SecIntel profile group to a security policy:

1. Select **SRX>Security Policy>SRX Policy**.

The Security Policies page appears.

2. Click the security policy to which you want to associate the SecIntel profile group.

The security policy rules are displayed in the Security Policy page.

3. Click the pencil icon that appears on the right side of the rule.

The **Security Policy** page displays the same options as that appear when you create a new security policy rule.

4. Under **Security Subscriptions** enable the **SecIntel** toggle.

5. Optional: If there is no default SecIntel profile group configured, you can configure it using the **Customize** option or set the default profile using Global options. See "[Configure Global Options](#)" on [page 315](#) for more details.

6. Click the check mark icon ✓ to save the changes.

A confirmation message is displayed.

7. Deploy the modified security policy. See "[Deploy Security Policies](#)" on [page 325](#)

Security Subscriptions-Anti-Malware

IN THIS CHAPTER

- [Anti-Malware Overview | 477](#)
- [About the Anti-Malware Page | 479](#)
- [Create an Anti-Malware Profile | 481](#)
- [Edit, Clone, and Delete an Anti-Malware Profile | 486](#)

Anti-Malware Overview

IN THIS SECTION

- [Benefits of Anti-malware | 478](#)

Malicious files, such as ransomware and adware, are becoming more common through multiple attack vectors. These threats compromise network endpoints, exposing them to data theft, including credentials and personally identifiable information (PII). Detecting and blocking malware and unwanted files on the network before they reach an endpoint is critical for protecting users, applications, and infrastructure from attacks.

Juniper Networks Anti-malware is a security framework that protects against evolving security threats by employing cloud-based security information. You can create anti-malware profiles for the SRX Series Firewalls in Juniper Security Director Cloud. Anti-malware profiles let you define which files to send to the cloud for inspection and the action to be taken when malware is detected.

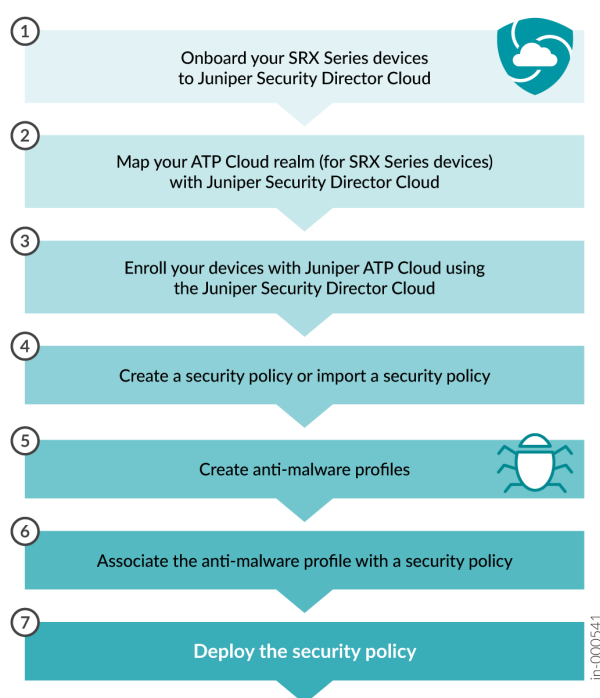
After you create an anti-malware profile, you can assign the profile to a security policy. When an infected host on the cloud network tries to initiate contact, the SRX Series Firewall uses Juniper Advanced Threat Prevention Cloud's (ATP Cloud) intelligence to remediate malicious content using security policies. If configured, security policies block the content before it is delivered to the destination address.

For more information on how to:

- Analyze and detect malwares using Juniper ATP Cloud, see [How is Malware Analyzed and Detected?](#).
- Enroll your SRX Series Firewall with Juniper ATP Cloud, see [Enrolling an SRX Series Firewall With Juniper Advanced Threat Prevention Cloud](#).

Figure 16 on page 478 shows the high-level steps for anti-malware configuration using Juniper Security Director Cloud.

Figure 16: Juniper Security Director Cloud Workflow with Anti-malware Configuration



Benefits of Anti-malware

- Detect and block known malicious downloadable files and email attachments using protocols (for example, HTTPs, SMB, IMAP, and SMTP).
- Quarantine the compromised internal hosts.
- Identify the connected devices that are at risk.
- Shut down attacks before they start.

- Protect users (including subscribers), applications, and infrastructure from compromise.

RELATED DOCUMENTATION

[About the Anti-Malware Page | 479](#)

[Create an Anti-Malware Profile | 481](#)

[Edit, Clone, and Delete an Anti-Malware Profile | 486](#)

About the Anti-Malware Page

IN THIS SECTION

- [Tasks You Can Perform | 479](#)
- [Field Descriptions | 480](#)

To access this page, select **SRX > Security Subscriptions > Anti-malware**.

You can create anti-malware profiles for the SRX Series Firewalls in Juniper Security Director Cloud. SRX Series Firewalls use intelligence provided by Juniper Advanced Threat Prevention Cloud (Juniper ATP Cloud) to remediate malicious content using security policies. The anti-malware profile defines the content to scan for any malware and the action to be taken when malware is detected. Juniper ATP Cloud uses a pipeline approach to analyzing and detecting malware. If an analysis reveals that the file is malware, it is not necessary to continue the pipeline to further examine the malware. If configured, security policies block the content before it is delivered to the destination address.

Tasks You Can Perform

- Create an anti-malware profile. See "[Create an Anti-Malware Profile](#)" on page 481 .
- Associate anti-malware profiles with security policies. To do this:
 1. Click **Security Policies** under the Anti-malware page title to directly navigate to the Security Policies page.
 2. Click + to add a new rule or click the pencil icon to edit a rule.
 3. Click + for Security Subscriptions and select an anti-malware profile from the Anti-malware list.

NOTE: You can add or edit any security subscriptions only if you select Action as **Permit**.

- Edit, clone, and delete an anti-malware profile. See "[Edit, Clone, and Delete an Anti-Malware Profile](#)" on page 486 .
- View the details of an anti-malware profile. To do this, select the anti-malware profile for which you want to view the details and then select **More > Detail**.
- Clear the selected anti-malware profiles. To do this, select **More > Clear all selections**.
- Show or hide columns in the Anti-malware table. To do this, use the Show Hide Columns icon in the upper-right corner of the page, and select the options to show or clear to hide options on the page.
- Reset Preference—Reset the displayed columns to the default set of columns for each tab in the table.
- Hover over the vertical ellipsis (three vertical dots) and select **Reset Preference**.

Field Descriptions

[Table 187 on page 480](#) describes the fields on the Anti-malware page.

Table 187: Fields on the Anti-malware Page

Field	Description
Name	Displays the anti-malware profile name.
Verdict threshold	Displays the threshold value to determine when a file is considered malware.
Protocols	Displays whether the protocol is HTTP, IMAP, SMB, or SMTP. Mouse over the protocol name to view the configuration details of inspection profile, action, and logs.
Logs	Displays whether the additional logs configured are files under verdict threshold, Allowlist or Blocklist.

RELATED DOCUMENTATION

| [Anti-Malware Overview](#) | 477

Create an Anti-Malware Profile

Configure the anti-malware profiles for SRX Series Firewall. The profile lets you define which files to send to the cloud for inspection and the action to be taken when malware is detected.

To create an anti-malware profile:

1. Select **SRX > Security Subscriptions > Anti-malware**.
The Anti-malware page opens.
2. Click **+** on the upper-right corner of the Anti-malware page.
The Create Anti-malware Profile page opens.
3. Complete the configuration according to the guidelines provided in [Table 188 on page 481](#) .
4. Click **OK** to save the changes. To discard your changes, click **Cancel**.

Table 188: Fields on the Create Anti-malware Profile Page

Field	Description
Name	Enter a name for the anti-malware profile. The name must be a unique string of alphanumeric, special characters and 64 characters maximum. Special characters such as & ()] ? " # are not allowed.
Verdict threshold	Select a threshold value from the list. The threshold value determines when a file is considered malware. If the cloud service returns a file verdict equal to or higher than the configured threshold, then that file is considered as malware.
Protocols	

Table 188: Fields on the Create Anti-malware Profile Page (Continued)

Field	Description
HTTP	<p>Enable this option to inspect advanced anti-malware (AAMW) files downloaded by hosts through HTTP protocol. The AAMW files are then submitted to Juniper ATP Cloud for malware screening.</p> <p>Once you enable this option, configure the following:</p> <ul style="list-style-type: none"> • Action (known verdict)—Select Permit or Block action from the list based on the detected malware. • Action (unknown verdict)—Select Permit or Block action from the list based on the detected malware having a verdict of “unknown.” • Notification—Select one of the following options to permit or block actions based on detected malware: <ul style="list-style-type: none"> • Redirect URL—Enter HTTP URL redirection for a customized client notification based on detected malware with the block action. • Redirect message—Enter the message for a customized client notification based on detected malware with the block action. <p>Range: 1 through 1023</p> • File name—Click Browse to upload a customized file to which users will be directed. The files must be in .php, .html, or .py format and the files will be stored in / jail/var/tmp. • Inspection profile—Select a Juniper ATP Cloud profile name from the list. The Juniper ATP Cloud profile defines the types of files to scan. <p>To view the default and other inspection profiles on the SRX device, your device must be enrolled with Juniper ATP Cloud.</p>

Table 188: Fields on the Create Anti-malware Profile Page (*Continued*)

Field	Description
	<ul style="list-style-type: none"> • Logs—Enable this option to add the event to the log file.
IMAP	<p>Enable this option to inspect and manage email attachments sent over IMAP email management.</p> <p>Once you enable this option, configure the following:</p> <ul style="list-style-type: none"> • Inspection profile—Select a Juniper Advanced Threat Prevention (ATP) Cloud profile name from the list. The ATP Cloud profile defines the types of files to scan. <p>To view the default and other inspection profiles on the SRX device, your device must be enrolled with Juniper ATP Cloud.</p> <ul style="list-style-type: none"> • Logs—Enable this option to add the event to the log file.
SMB	<p>Enable this option to inspect files downloaded by hosts through Server Message Block (SMB) protocol. SMB protocol enables applications or users to access files and other resources on a remote server.</p> <p>Once you enable this option, configure the following:</p> <ul style="list-style-type: none"> • Action—Select Permit or Block action from the list based on the downloaded files. • Inspection profile—Select a Juniper Advanced Threat Prevention (ATP) Cloud profile name from the list. The ATP Cloud profile defines the types of files to scan. <p>To view the default and other inspection profiles on the SRX device, your device must be enrolled with Juniper ATP Cloud.</p> <ul style="list-style-type: none"> • Logs—Enable this option to add the event to the log file.

Table 188: Fields on the Create Anti-malware Profile Page (*Continued*)

Field	Description
SMTP	<p>Enable this option to inspect and manage email attachments sent over SMTP email management.</p> <p>Once you enable this option, configure the following:</p> <ul style="list-style-type: none"> • Inspection profile—Select a Juniper Advanced Threat Prevention (ATP) Cloud profile name from the list. The ATP Cloud profile defines the types of files to scan. <p>To view the default and other inspection profiles on the SRX device, your device must be enrolled with Juniper ATP Cloud.</p> <ul style="list-style-type: none"> • Logs—Enable this option to add the event to the log file.
Fallback Actions	
Global fallback action	Select None , Permit , or Block action from the list to permit or block the file regardless of its threat level.
Logs	Enable this option to add the event to the log file.

Table 188: Fields on the Create Anti-malware Profile Page (Continued)

Field	Description
Specific Fallback Configurations	<ul style="list-style-type: none"> • Invalid content size: <ul style="list-style-type: none"> • Select None, Permit, or Block action from the list if the content size exceeds the supported range (32 MB). • Logs—Enable this option to add the event to the log file. • Out of resource action <ul style="list-style-type: none"> • Select None, Permit, or Block action from the list if the service is out of resources. • Logs—Enable this option to add the event to the log file. • Service not ready action <ul style="list-style-type: none"> • Select None, Permit, or Block action from the list if the service is not yet ready. • Logs—Enable this option to add the event to the log file. • Submission timeout action <ul style="list-style-type: none"> • Select None, Permit, or Block action from the list if the submission is timed out. • Logs—Enable this option to add the event to the log file. • Unknown file action: <ul style="list-style-type: none"> • Select None, Permit, or Block action from the list if the file type is unknown. • Logs—Enable this option to add the event to the log file. • Verdict timeout action

Table 188: Fields on the Create Anti-malware Profile Page (*Continued*)

Field	Description
	<ul style="list-style-type: none"> • Select None, Permit, or Block action from the list if the verdict response is timed out. • Logs—Enable this option to add the event to the log file.
Additional Logging	
Files under verdict threshold	Enable this option to create a system log entry when the file verdict number is less than the threshold.
Blocklist	Enable this option to create a system log entry when an attempt is made to access that are listed in the blocklist.
Allowlist	Enable this option to create a system log entry when an attempt is made to access that are listed in the allowlist.

RELATED DOCUMENTATION

[Anti-Malware Overview | 477](#)

[About the Anti-Malware Page | 479](#)

[Edit, Clone, and Delete an Anti-Malware Profile | 486](#)

Edit, Clone, and Delete an Anti-Malware Profile

IN THIS SECTION

● [Edit an Anti-Malware Profile | 487](#)

- [Clone an Anti-Malware Profile | 487](#)
- [Delete an Anti-Malware Profile | 488](#)

You can edit, clone, and delete anti-malware profiles from the Anti-malware page. This topic has the following sections:

Edit an Anti-Malware Profile

To edit an anti-malware profile:

1. Select **SRX > Security Subscriptions > Anti-malware**.

The Anti-malware page opens.

2. Select an existing anti-malware profile to edit, and click the pencil icon.

The Edit Anti-malware Profile page opens.

3. Edit the anti-malware profile fields.

4. Click **OK** to save your changes.

The Anti-malware page displays a confirmation message indicating the status of the edit operation.

Clone an Anti-Malware Profile

To clone an anti-malware profile:

1. Select **SRX > Security Subscriptions > Anti-malware**.

The Anti-malware page opens.

2. Select an existing anti-malware profile to clone then select **More > Clone**.

The Create Anti-malware Profile page opens displaying the same fields that are presented when you create an anti-malware profile.

3. Modify the anti-malware profile fields as needed.

4. Click **OK** to save your changes.

You are taken to the Anti-malware page. A confirmation message appears, indicating the status of the clone operation.

Delete an Anti-Malware Profile

To delete an anti-malware profile:

1. Select **SRX > Security Subscriptions > Anti-malware**.

The Anti-malware page opens.

2. Select an existing anti-malware profile to delete, and click the delete icon.

A message asking you to confirm the delete operation is displayed.

3. Click **Yes** to delete the anti-malware profile.

A confirmation message is displayed indicating the status of the delete operation.

RELATED DOCUMENTATION

[Anti-Malware Overview | 477](#)

[About the Anti-Malware Page | 479](#)

[Create an Anti-Malware Profile | 481](#)

Security Subscriptions-Secure Web Proxy

IN THIS CHAPTER

- [About the Secure Web Proxy Page | 489](#)
- [Create a Secure Web Proxy Profile | 491](#)
- [Edit a Secure Web Proxy Profile | 492](#)
- [Clone a Secure Web Proxy Profile | 492](#)
- [Delete a Secure Web Proxy Profile | 493](#)

About the Secure Web Proxy Page

IN THIS SECTION

- [Tasks You Can Perform | 490](#)
- [Field Descriptions | 490](#)

A secure Web proxy profile provides better quality of service for the selected application traffic by providing direct connections to a webserver. The **Secure Web Proxy** page enables you to create and manage secure Web proxy profiles for SRX Series firewalls and vSRX Virtual Firewall virtual firewalls running Junos OS Release 19.2R1 or later. A profile contains information about the list of applications that can bypass an external proxy server and connect to a webserver directly.

You can associate a secure Web proxy profile to a security policy rule for advanced security. So, if the traffic from the device matches with the rule, the traffic bypasses the proxy server and connects to the webserver directly. For information about creating a policy rule, see ["Add a Security Policy Rule" on page 307](#).



CAUTION: If you have configured unified policies (security policies with dynamic applications) on your SRX Series Firewall, the secure Web proxy feature may not function properly. If you have both standard and unified policies configured for the device, the traffic is first processed using the standard policy. If no match is found with the standard policy, only then the traffic is processed using the unified policy. For steps to configure a secure Web proxy profile along with a unified policy, see [KB35883](#).

For information about the benefits, limitations, and how secure Web proxy works on SRX Series Firewalls, see the [Application Security User Guide for Security Devices](#).

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a secure Web proxy profile—["Create a Secure Web Proxy Profile" on page 491](#) .
- Edit a secure Web proxy profile—["Edit a Secure Web Proxy Profile" on page 492](#) .
- Clone a secure Web proxy profile—["Clone a Secure Web Proxy Profile" on page 492](#) .
- Delete a secure Web proxy profile—["Delete a Secure Web Proxy Profile" on page 493](#) .

Field Descriptions

The following table describes the information displayed on the **Secure Web Proxy** page:

Table 189: Fields on the Secure Web Proxy page

Field	Description
Name	Displays the name of the secure Web proxy profile.
Drop on DNS Error	Displays the following statuses: <ul style="list-style-type: none"> • Enabled—if you selected the checkbox to end the session if the web server is unavailable. • Disabled—if you did not select the checkbox to end the session if the web server is unavailable.
Application Signatures	Displays names of the applications that can bypass a proxy server.

Table 189: Fields on the Secure Web Proxy page (Continued)

Field	Description
Proxy Address	Displays names of the proxy servers that can be bypassed by the applications.
Description	Displays the description of the secure Web proxy profile.

Create a Secure Web Proxy Profile

- Go to **SRX>Security Subscriptions>Secure Web Proxy**.
The **Secure Web Proxy** page is displayed.
- Click the **+** icon.
The **Create Secure Web Proxy** page is displayed.
- Enter a name and description for the profile.
The name must be an alphanumeric string within 63 characters. It can include special characters such as:
 - Colons
 - Periods
 - Slashes
 - Dashes
 - Underscores.
- Select the **If server unavailable, end session** checkbox to end the session if the webserver is not available.
- In the **Application signatures** section, click **+**, select the required applications, and then click **OK**. For information about application signatures, see ["About the Application Signatures Page" on page 898](#) .
The applications are displayed in the **Application signatures** section.
- In the **Proxy server** section, click **+** and perform the following steps:
 - Select the required proxy servers.
 - Optional: To add a new proxy server, click **+**, add the server details, and click the checkmark.
The name must be an alphanumeric string within 63 characters. It can include special characters such as:

- Colons
- Periods
- Slashes
- Dashes
- Underscores.

The IP address CIDR must be between 0 through 32. The port number must be between 1 through 65535.

c. Click **OK**.

The proxy servers are displayed in the **Proxy server** section.

7. Click **OK**.

A profile is created and displayed on the **Secure Web Proxy** page .

Edit a Secure Web Proxy Profile

1. Select the profile and click the edit icon.
The **Edit Secure Web Proxy** page is displayed.
2. Edit the required details and click **OK**.
The profile is updated and a success message is displayed.

Clone a Secure Web Proxy Profile

You can create a new secure Web proxy profile by cloning an existing profile.

1. Go to **SRX> Security Subscriptions> Secure Web Proxy**.
The **Secure Web Proxy** page is displayed.
2. Select the profile that you want to clone, click the **More** menu, and then click **Clone**.
The **Clone Secure Web Proxy** page is displayed.
3. Edit the required details and click **OK**.
A new profile is created and displayed on the **Secure Web Proxy** page.

Delete a Secure Web Proxy Profile

1. Select the profile and click the delete icon.
You are prompted to confirm if you want to delete the profile.
2. Click **Yes** to confirm.
The profile is deleted and a success message is displayed.

IPsec VPN

IN THIS CHAPTER

- [IPsec VPN Overview | 494](#)
- [Understanding IPsec VPN Modes | 497](#)
- [Understanding IPsec VPN Routing | 498](#)
- [Understanding IKE Authentication | 498](#)
- [IPsec VPN Main Page Fields | 499](#)
- [IPsec VPN Global Settings | 500](#)
- [Create a Policy-Based Site-to-Site VPN | 502](#)
- [Create a Route-Based Site-to-Site VPN | 511](#)
- [Create a Hub-and-Spoke \(Establishment All Peers\) VPN | 524](#)
- [Create a Hub-and-Spoke \(Establishment by Spokes\) VPN | 536](#)
- [Create a Hub-and-Spoke Auto Discovery VPN | 546](#)
- [Create a Remote Access VPN—Juniper Secure Connect | 557](#)
- [Importing IPsec VPNs | 569](#)
- [Deploy an IPsec VPN | 570](#)
- [Modify IPsec VPN Settings | 571](#)
- [Delete an IPsec VPN | 571](#)

IPsec VPN Overview

IN THIS SECTION

- [IPsec VPN Topologies | 496](#)

IPsec VPN provides a means to securely communicate with remote computers across a public WAN such as the Internet. A VPN connection can link two LANs using a site-to-site VPN or a remote dial-up user and a LAN. The traffic that flows between these two points passes through shared resources such as routers, switches, and other network equipment that comprise the public WAN. To secure VPN communication that passes through the WAN, you need to create an IPsec tunnel.

Juniper Security Director Cloud simplifies the management and deployment of IPsec VPNs. In general, VPN configurations are tedious and repetitive when deploying over a large number of SRX Series Firewalls. With Juniper Security Director Cloud, you can use VPN profiles to group common settings and apply the profiles to multiple VPN tunnel configurations across multiple SRX Series Firewalls. You can deploy site-to-site and hub-and-spoke VPNs. Juniper Security Director Cloud determines the necessary deployment scenarios and publishes the required configuration for all SRX Series Firewalls.

Juniper Security Director Cloud supports policy-based and route-based IPsec VPNs on SRX Series Firewalls. Policy-based VPNs are supported only in the site-to-site deployments, where you configure two endpoints. If you have two or more SRX Series Firewalls, then route-based VPNs offer more flexibility and scalability. To allow data to be securely transferred between a branch office and the corporate office, configure a policy-based or route-based IPsec VPN. For an enterprise-class deployment, configure a hub-and-spoke IPsec VPN.

Use route-based tunnel mode if:

- Participating gateways are Juniper Networks products.
- Either source or destination NAT must occur when traffic traverses the VPN.
- Dynamic routing protocols must be used for VPN routing.
- Primary and backup VPNs are required in the setup.

Use policy-based tunnel mode if:

- The remote VPN gateway is a non-Juniper Networks device.
- Access to the VPN must be restricted for specific application traffic.

When you create a policy-based or route-based IPsec VPN, a topology is displayed for a representation. You need to click the icons to configure the remote gateway.

NOTE:

- Juniper Security Director Cloud views each logical system as any other security device and takes ownership of the security configuration of the logical system. In Juniper Security Director Cloud, each logical system is managed as a unique security device.

- Juniper Security Director Cloud ensures that the tunnel interfaces are exclusively assigned to the individual logical systems of a device. No tunnel interface is assigned to more than one logical system of the same device.
- Juniper Security Director Cloud does not support VPN over Point-to-Point Protocol over Ethernet (PPPoE).

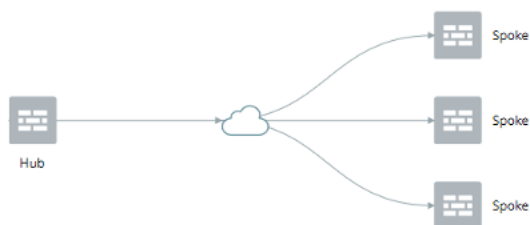
IPsec VPN Topologies

The following IPsec VPNs are supported:

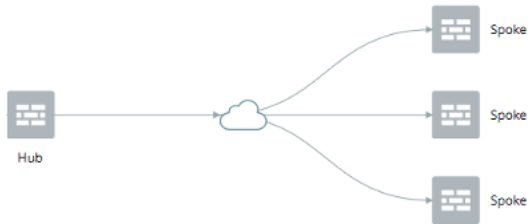
- Site-to-Site VPNs—Connects two sites in an organization together and allows secure communications between the sites.



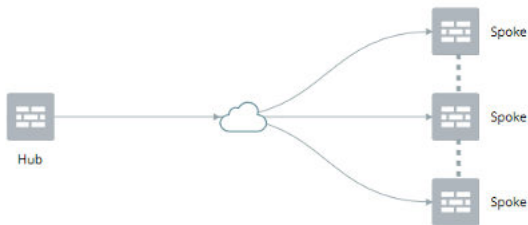
- Hub-and-Spoke (establishment all peers)—Connects branch offices to the corporate office in an enterprise network. You can also use this topology to connect spokes together by sending traffic through the hub.



- Hub-and-Spoke (establishment by spokes)—Auto-VPN supports an IPsec VPN aggregator called a hub that serves as a single termination point for multiple tunnels to remote sites called spokes. Auto-VPN allows network administrators to configure a hub for current and future spokes. No configuration changes are required on the hub when spoke devices are added or deleted, which allows administrators flexibility in managing large-scale network deployments.



- **Hub-and-Spoke (Auto Discovery VPN)**—Auto Discovery VPN (ADVPN) is a technology that allows the central hub to dynamically inform spokes about a better path for traffic between two spokes. When both spokes acknowledge the information from the hub, the spokes establish a shortcut tunnel and change the routing topology for the host to reach the other side without sending traffic through the hub.



- **Remote Access VPN (Juniper Secure Connect)**—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.



Understanding IPsec VPN Modes

The following two modes determine how traffic is exchanged in the VPN:

- **Tunnel Mode**—This mode encapsulates the original IP packet within another packet in the VPN tunnel. This is most commonly used when hosts within separate private networks want to communicate over a public network. Both VPN gateways establish the VPN tunnel to each other, and all traffic between the two gateways appears to be from the two gateways, with the original packet embedded within the exterior IPsec packet.

- **Transport Mode**—This mode does not encapsulate the original packet in a new packet like the tunnel mode. The transport mode sends the packet directly between the two hosts that have established the IPsec tunnel.

The Tunnel mode is the most common VPN mode on the Internet because it easily allows entire networks, particularly those with private address space, to communicate over public IP networks. The Transport mode is primarily used when encrypting traffic between two hosts to secure communication where IP address overlap is not an issue, such as between a host and a server on a private network.

Understanding IPsec VPN Routing

SRX Series Firewalls must know how to reach destination networks. This can be configured through the use of static routing or dynamic routing.

In Juniper Security Director Cloud, route-based VPNs support OSPF, RIP, and eBGP routing along with static routing. Static routing requires that administrators specify the list of host or network addresses at each site as part of the VPN.

For example, in a retail scenario, where thousands of spokes can be part of a VPN, the static routing approach generates a huge configuration at each device. Static routing requires administrators to manually configure each route, and problems might occur when the infrastructure changes or when the administrators do not have access to the addresses for the protected network. Keeping routes up-to-date manually also creates a tremendous overhead.

Understanding IKE Authentication

Internet Key Exchange negotiations only provide the ability to establish a secure channel over which two parties can communicate. You still need to define how they authenticate each other. This is where IKE authentication is used to ensure that the other party is authorized to establish the VPN.

The following IKE authentications are available:

- **Preshared key authentication**—The most common way to establish a VPN connection is to use preshared keys, which is essentially a password that is the same for both parties. This password must be exchanged in advance in an out-of-band mechanism, such as over the phone, through a verbal exchange, or through less secure mechanisms, even e-mail. The parties then authenticate each other by encrypting the preshared key with the peer's public key, which is obtained in the Diffie-Hellman exchange.

Preshared keys are commonly deployed for site-to-site IPsec VPNs, either within a single organization or between different organizations. To ensure that preshared keys are used in the most

secure fashion, a preshared key must consist of at least 8 characters with 12 or more characters recommended comprising a combination of letters, numbers, and non-alphanumeric characters, along with different cases for the letters. Preshared keys should not use a dictionary word.

- Certificate authentication—Certificate-based authentication is considered more secure than preshared key authentication because the certificate key cannot be compromised easily. Certificates are also more ideal in larger scale environments with numerous peer sites that should not all share a preshared key. Certificates are composed of a public and private key and can be signed by a primary certificate known as a certificate authority (CA). In this way, certificates can be checked to see if they are signed with a trusted CA.

IPsec VPN Main Page Fields

Use IPsec VPNs to secure your network traffic with encryption and authentication. The VPN tunnels are central components of networks which secure the data between different sites and remote users.

Table 190: IPsec VPN Main Page Fields

Field	Description
Name	The name of the IPsec VPN.
Description	The description of the IPsec VPN.
VPN Topology	The types of deployment topologies for IPsec VPN, such as site-to-site, hub-and-spoke, and remote access VPNs.
Profile Type	The type of VPN profile, such as Inline Profile or Shared Profile.
Profile Name	The name of the VPN profile. The security parameters are defined in this profile to establish the VPN connection between two sites.
Tunnel Mode	The tunnel mode, such as Route Based or Policy Based.
Configuration State	The configuration state of the IPsec VPN.

Table 190: IPsec VPN Main Page Fields (Continued)

Field	Description
Status	<p>Displays the publish state of the VPN configuration.</p> <p>You can verify your VPN configurations before updating the configuration to the device.</p> <ul style="list-style-type: none"> • Deploy pending—The VPN is created but not deployed. • Deploy scheduled—The deployment of the VPN is scheduled. • Deploy in-progress— The deployment of the VPN is in progress. • Deploy successful—The configuration is deployed to all the devices involved in the VPN. • Redeploy required—Modifications are made to the VPN configuration after it is deployed. • Deploy failed—The deployment of the VPN failed.
Created by	The email address of the user who created the IPsec VPN.

IPsec VPN Global Settings

The Global Settings page displays the default settings that apply to the devices in your remote access VPN topology. You can view or modify the VPN global configuration details.

1. Select **SRX > IPsec VPN > IPsec VPNs**.
The IPsec VPNs page opens.
2. Click **Global Settings**.
The Global Settings page opens.
3. Click the pencil icon to modify the global settings.
The Modify Global Settings page opens.

Table 191: Global Settings

Field	Description
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.
Remote Access VPN	
Default RAVPN	Select a remote IPsec VPN profile. This option is available when at least one Juniper Secure Connect VPN is created.
SSL VPN Tunnel tracking	Enable this option to track Encapsulated Security Payload (ESP) tunnels.
SSL VPN Profiles	Lists the SSL VPN profiles. NOTE: This option displays associated IPsec VPNs when at least one remote access VPN is created. To create a new SSL VPN profile: <ol style="list-style-type: none">1. Click Add. The Add SSL VPN Profile page opens.2. Enter the name for an SSL VPN profile.3. Enable Logging option to log SSL VPN events.4. Enter an SSL termination profile name.5. Select a server certificate from the list.6. Click OK. To edit an SSL VPN profile, select the profile to edit, and click the pencil icon. To delete an SSL VPN profile, select the profile to delete, and click the delete icon.

Create a Policy-Based Site-to-Site VPN

A site-to-site VPN allows secure communications between two sites in an organization.

Before You Begin

- Read the ["IPsec VPN Overview" on page 494](#) topic.
- Review the IPsec VPN main page for an understanding of your current data set. See ["IPsec VPN Main Page Fields" on page 499](#) for the field descriptions.
- Create addresses and address sets. See ["Create Addresses or Address Groups" on page 863](#) .
- Create VPN profiles. See ["Creating VPN Profiles" on page 576](#) .
- Define extranet devices. See ["Creating Extranet Devices" on page 587](#) .

To create a policy-based site-to-site VPN:

1. Select **SRX > IPsec VPN > IPsec VPNs**.

The IPsec VPNs page opens.

2. Click **Create > Policy Based - Site to Site**.

The Create Policy Based Site to Site VPN page opens.

3. Complete the VPN configuration parameters according to the guidelines provided in [Create Policy Based Site to Site VPN Page Settings on page 502](#) .

NOTE: Click **View VPN Profile Settings** to view or edit VPN profiles. If the VPN profile is inline, you can edit the configurations. If the profile is shared, you can only view the configurations.

The VPN connectivity changes from a gray line to blue in the topology to show that the configuration is complete.

4. Click **Save** to save the IPsec VPN configuration.

Table 192: Create Policy Based Site to Site VPN Page Settings

Settings	Guidelines
General	

Table 192: Create Policy Based Site to Site VPN Page Settings *(Continued)*

Settings	Guidelines
Name	<p>Enter a unique string of maximum 63 alphanumeric characters without spaces.</p> <p>The string can contain colons, periods, dashes, and underscores.</p>
Description	<p>Enter a description containing maximum 255 characters for the VPN.</p>
VPN profile	<p>Select a VPN profile from the drop-down list based on the deployment scenario.</p> <ul style="list-style-type: none"> • The Inline profile is applicable only to a particular IPsec VPN. To view and edit the details, click View VPN Profile Settings on the Create VPN page. • The Shared profile can be used by one or more IPsec VPNs. You can only view the details of the shared profiles. To view the details, click View VPN Profile Settings.

Table 192: Create Policy Based Site to Site VPN Page Settings *(Continued)*

Settings	Guidelines
Authentication method	<p>Select an authentication method from the list that the device uses to authenticate the source of IKE messages.</p> <ul style="list-style-type: none"> • Pre-shared based—Specifies that a pre-shared 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. • 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.
Max transmission unit	<p>Select the maximum transmission unit (MTU) in bytes.</p> <p>MTU defines the maximum size of an IP packet, including the IPsec overhead. You can specify the MTU value for the tunnel endpoint. The valid range is 68 to 9192 bytes, and the default value is 1500 bytes.</p>

Table 192: Create Policy Based Site to Site VPN Page Settings (*Continued*)

Settings	Guidelines
Pre-shared key	<p>Establish a VPN connection using pre-shared keys, which is essentially a password that is same for both parties. Pre-shared keys are commonly deployed for site-to-site IPsec VPNs, either within a single organization or between different organizations.</p> <p>Select the type of pre-shared key to use:</p> <ul style="list-style-type: none"> • Autogenerate—Automatically generate a unique key per tunnel. • Manual—Enter the key manually. By default, the manual key is masked. <p>Pre-shared keys are applicable only if the authentication method is pre-shared based.</p>
Devices	<p>Add devices as endpoints in the VPN. You can add maximum two devices.</p> <ol style="list-style-type: none"> 1. Click Add, and click one of the following: Device or Extranet device. The Add Device page opens. 2. Select the device and interface in the following fields: <ul style="list-style-type: none"> • Device—The devices list shows only physical systems. • External interface—Select the outgoing interface for IKE security associations (SAs). This interface is associated with a zone that acts as its carrier, providing firewall security for it. 3. Click OK.

Table 193: Add Device page settings

Settings	Guidelines
Device	Select a device.
External interface	Select the outgoing interface for IKE security associations (SAs). This interface is associated with a zone that acts as its carrier, providing firewall security for it.

Table 194: IKE and IPsec Settings

Settings	Guidelines
IKE Settings	
Authentication method	<p>Select an authentication method from the list that the device uses to authenticate the source of IKE messages.</p> <ul style="list-style-type: none"> • Pre-shared based—Specifies that a pre-shared 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. • 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.
IKE version	Select the V1 IKE version which is used to negotiate dynamic security associations (SAs) for IPsec.

Table 194: IKE and IPsec Settings (Continued)

Settings	Guidelines
Mode	<p>Select an IKE policy mode.</p> <ul style="list-style-type: none"> • Main—Uses 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. This mode provides identity protection. • Aggressive—Takes half the number of messages of main mode, has less negotiation power, and does not provide identity protection. <p>Mode is applicable when the IKE Version is V1.</p>
Encryption algorithm	<p>Select the appropriate encryption mechanism.</p>
Authentication algorithm	<p>Select an algorithm.</p> <p>The device uses this algorithm to verify the authenticity and integrity of a packet.</p>
Diffie Hellman group	<p>Select a group.</p> <p>Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process.</p>
Lifetime seconds	<p>Select a lifetime of an IKE security association (SA) in seconds.</p> <p>The valid range is from 180 to 86400 seconds.</p>
Dead peer detection	<p>Enable this option to permit the two gateways to determine if the peer gateway is up and responding to the Dead Peer Detection (DPD) messages that are negotiated during IPsec establishment.</p>

Table 194: IKE and IPsec Settings *(Continued)*

Settings	Guidelines
DPD mode	<p>Select a DPD Mode.</p> <ul style="list-style-type: none"> • Optimized: R-U-THERE messages are triggered if there is no incoming IKE or IPsec traffic within a configured interval after the device sends outgoing packets to the peer. This is the default mode. • Probe Idle Tunnel: R-U-THERE messages are triggered if there is no incoming or outgoing IKE or IPsec traffic within a configured interval. R-U-THERE messages are sent periodically to the peer until there is traffic activity. • Always-send: R-U-THERE messages are sent at configured intervals regardless of traffic activity between the peers.
DPD interval	<p>Select an interval in seconds to send dead peer detection messages.</p> <p>The default interval is 10 seconds with a valid range of 2 to 60 seconds.</p>
DPD threshold	<p>Select the failure DPD threshold value.</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 with a valid range of 1 to 5.</p>
Advanced Configuration	
General IKE ID	<p>Enable this option to accept peer IKE ID.</p> <p>This option is disabled by default. If General IKE ID is enabled, the IKE ID option is disabled automatically.</p>

Table 194: IKE and IPsec Settings *(Continued)*

Settings	Guidelines
IKE ID	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • None • Distinguished name • Hostname • IPv4 address • E-mail Address <p>IKE ID is applicable only when General IKE ID is disabled.</p>
NAT-T	<p>Enable Network Address Translation-Traversal (NAT-T) if the dynamic endpoint is behind a NAT device.</p>
Keep alive	<p>Select a period in seconds to keep the connection alive.</p> <p>NAT Keepalives are required to maintain the NAT translation during the connection between the VPN peers. The valid range is from 1 to 300 seconds.</p>
IPSec Settings	
Protocol	<p>Select the required protocol to establish the VPN.</p> <ul style="list-style-type: none"> • ESP—The Encapsulating Security Payload (ESP) protocol provides both encryption and authentication. • AH—The Authentication Header (AH) protocol provides data integrity and data authentication.
Encryption algorithm	<p>Select the encryption method.</p> <p>This option is applicable if the Protocol is ESP.</p>
Authentication algorithm	<p>Select an algorithm.</p> <p>The device uses these algorithms to verify the authenticity and integrity of a packet.</p>

Table 194: IKE and IPsec Settings (Continued)

Settings	Guidelines
Perfect forward secrecy	<p>Select Perfect Forward Secrecy (PFS) as the method that the device uses to generate the encryption key.</p> <p>The PFS generates each new encryption key independently from the previous key. The higher numbered groups provide more security but require more processing time.</p>
Establish tunnel	<p>Select an option to specify when IKE is activated.</p> <ul style="list-style-type: none"> • Immediately—IKE is activated immediately after VPN configuration changes are committed. • On-traffic—IKE is activated only when data traffic flows and must be negotiated with the peer gateway. This is the default behavior.
Advanced Configuration	
VPN monitor	<p>Enable this option to send Internet Control Message Protocol (ICMP) to determine if the VPN is up.</p>
Optimized	<p>Enable this option to optimize VPN monitoring and configure SRX Series Firewalls to send ICMP echo requests, also called pings, only when there is outgoing traffic and no incoming traffic from the configured peer through the VPN tunnel.</p> <p>If there is incoming traffic through the VPN tunnel, the SRX Series Firewalls considers the tunnel to be active and do not send pings to the peer.</p>
Anti replay	<p>Enable this option for the IPsec mechanism to protect against a VPN attack that uses a sequence of numbers that are built into the IPsec packet.</p> <p>IPsec does not accept a packet for which it has already seen the same sequence number. It checks the sequence numbers and enforces the check rather than just ignoring the sequence numbers.</p> <p>Disable this option if there is an error with the IPsec mechanism that results in out-of-order packets, preventing proper functionality.</p> <p>By default, Anti replay detection is enabled.</p>

Table 194: IKE and IPsec Settings (Continued)

Settings	Guidelines
Install interval	Select the maximum number of seconds to allow for the installation of a re-keyed outbound security association (SA) on the device.
Idle time	Select the appropriate idle time interval. The sessions and their corresponding translations typically time out after a certain period if no traffic is received.
DF bit	Select an option to process the Don't Fragment (DF) bit in IP messages. <ul style="list-style-type: none"> • Clear—Disable the DF bit from the IP messages. This is the default option. • Copy—Copy the DF bit to the IP messages. • Set—Enable the DF bit in the IP messages.
Copy outer DSCP	Enable this option to allow copying of the Differentiated Services Code Point (DSCP) field from the outer IP header encrypted packet to the inner IP header plain text message on the decryption path. The benefit in enabling this option is that after IPsec decryption, clear text packets can follow the inner class-of-service (CoS) rules.
Lifetime seconds	Select a lifetime of an IKE security association (SA) in seconds. The valid range is from 180 to 86,400 seconds.
Lifetime kilobytes	Select the lifetime of an IPsec security association (SA) in kilobytes. The range is from 64 to 4294967294 kilobytes.

Create a Route-Based Site-to-Site VPN

A site-to-site VPN allows secure communications between two sites in an organization.

Before You Begin

- Read the ["IPsec VPN Overview" on page 494](#) topic.
- Review the IPsec VPN main page to understand your current data set. See ["IPsec VPN Main Page Fields" on page 499](#) for the field descriptions.
- Create addresses and address sets. See ["Create Addresses or Address Groups" on page 863](#) .
- Create VPN profiles. See ["Creating VPN Profiles" on page 576](#) .
- Define extranet devices. See ["Creating Extranet Devices" on page 587](#) .

1. Select **SRX > IPsec VPN > IPsec VPNs**.

The IPsec VPNs page opens.

2. Click **Create > Site to Site**.

The Create Site to Site VPN page opens.

3. Complete the VPN configuration parameters according to the guidelines provided in [Table 195 on page 512](#) .

NOTE: Click **View VPN Profile Settings** to view or edit VPN profiles. If the VPN profile is inline, you can edit the configurations. If the profile is shared, you can only view the configurations.

The VPN connectivity changes from gray to blue line in the topology to show that the configuration is complete.

4. Click **Save** to save the IPsec VPN configuration.

Table 195: Create Site to Site VPN Page Settings

Settings	Guidelines
General	
Name	Enter a unique string of maximum 63 alphanumeric characters without spaces. The string can contain colons, periods, dashes, and underscores.
Description	Enter a description containing maximum 255 characters for the VPN.

Table 195: Create Site to Site VPN Page Settings (*Continued*)

Settings	Guidelines
Routing topology	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • Traffic selector (Auto route insertion)—A traffic selector is an agreement between IKE peers to permit traffic through a tunnel if the traffic matches a specified pair of local and remote addresses. • Static routing—Generates static routing based on the protected networks or zones per device. • OSPF-dynamic routing—Generates OSPF configuration. • RIP-dynamic routing—Generates RIP configuration. • eBGP-dynamic routing—Generates eBGP configuration. <p>The Routing topology is applicable only to route-based VPNs.</p>
VPN profile	<p>Select a VPN profile from the drop-down list based on the deployment scenario.</p> <ul style="list-style-type: none"> • The Inline profile is applicable only to a particular IPsec VPN. • The MainModeProfile is a predefined main mode profile with standard proposal set. • The AggressiveModeProfile is a predefined aggressive mode profile with standard proposal set. • The RSAProfile is a predefined profile for certificate based authentication (RSA SIGNATURE) with the Distinguished Name (DN) as IKE ID type. • The ADVPNProfile is a predefined profile fo ADVPN. <p>You can view and edit the details of the VPN profiles by clicking View VPN Profile settings on the Create VPN page.</p>

Table 195: Create Site to Site VPN Page Settings (Continued)

Settings	Guidelines
Authentication method	<p>Select an authentication method from the list that the device uses to authenticate the source of IKE messages.</p> <ul style="list-style-type: none"> • Pre-shared based—Specifies that a pre-shared 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. • 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.
Network IP	<p>Enter the IP address of the numbered tunnel interface.</p> <p>This is the subnet address from where the IP address is automatically assigned for tunnel interfaces.</p>
Max transmission unit	<p>Select the maximum transmission unit (MTU) in bytes.</p> <p>MTU defines the maximum size of an IP packet, including the IPsec overhead. You can specify the MTU value for the tunnel endpoint. The valid range is 68 to 9192 bytes, and the default value is 1500 bytes.</p>

Table 195: Create Site to Site VPN Page Settings (*Continued*)

Settings	Guidelines
Pre-shared key	<p>Establish a VPN connection using pre-shared keys, which is essentially a password that is same for both parties. Pre-shared keys are commonly deployed for site-to-site IPsec VPNs, either within a single organization or between different organizations.</p> <p>Select the type of pre-shared key to use:</p> <ul style="list-style-type: none"> • Autogenerate—Select if you want to automatically generate a unique key per tunnel. • Manual—Select to enter the key manually. By default, the manual key is masked. <p>Pre-shared keys are applicable only if the authentication method is pre-shared based.</p>
Devices	<p>Add devices as endpoints in the VPN. You can add maximum two devices.</p> <p>To add devices in route-based VPNs:</p> <ol style="list-style-type: none"> 1. Click Add, and click one of the following: Device or Extranet Device. <p>The Add Device page opens.</p> <ol style="list-style-type: none"> 2. Configure the device parameters as described in Table 196 on page 515 3. Click OK.

Table 196: Add Device page settings

Settings	Guidelines
Device	Select a device.
External interface	Select the outgoing interface for IKE security associations (SAs).

Table 196: Add Device page settings (*Continued*)

Settings	Guidelines
Tunnel zone	<p>Select the tunnel zone.</p> <p>Tunnel zones are logical areas of address spaces that can support dynamic IP (DIP) address pools for NAT applications to pre and post-encapsulated IPsec traffic. Tunnel zones also provide flexibility in combining tunnel interfaces with VPN tunnels.</p> <p>Tunnel zones are applicable only for route-based site-to-site VPN.</p>
Routing instance	<p>Select the required routing instance.</p> <p>Routing instances are applicable only for route-based site-to-site VPNs.</p>
Initiator/Recipient	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • Initiator • Recipient <p>This option is applicable when the VPN profile is Aggressive Mode profile.</p>
Certificate	<p>Select a certificate to authenticate the VPN initiator and recipient.</p> <p>Authentication certificates are applicable in one of the following scenarios:</p> <ul style="list-style-type: none"> • The VPN profile is RSA profile or ADVPN profile. • The authentication method is RSA-Signatures, DSA-Signatures, ECDSA-Signatures-256, or ECDSA-Signatures-384.
Trusted CA/Group	<p>Select the CA profile from the list to associate it with the local certificate.</p> <p>CA profiles are applicable in one of the following scenarios:</p> <ul style="list-style-type: none"> • The VPN profile is RSA profile, ADVPN profile, or default profile with any signature type. • The authentication method is RSA-Signatures, DSA-Signatures, ECDSA-Signatures-256, or ECDSA-Signatures-384.

Table 196: Add Device page settings (Continued)

Settings	Guidelines
Export	<p>Select the type of routes to export.</p> <ul style="list-style-type: none"> • Select the Static Routes check box to export static routes. <p>Juniper Security Director Cloud simplifies VPN address management by enabling administrators to export static routes to a remote site over a tunnel, allowing the static route networks to participate in the VPN.</p> <p>For eBGP Dynamic Routing, the Static Routes check box is selected by default.</p> <ul style="list-style-type: none"> • Select the RIP Routes check box to export RIP routes. <p>You can export RIP routes only when Routing Topology is OSPF Dynamic Routing.</p> <ul style="list-style-type: none"> • Select the OSPF Routes check box to export OSPF routes. <p>You can export OSPF routes only when Routing Topology is RIP-Dynamic Routing.</p> <p>If you select OSPF or RIP export, the OSPF or RIP routes outside the VPN network is imported into a VPN network through OSPF or RIP Dynamic routing protocols.</p>
OSPF area	<p>Select an OSPF area ID within the range of 0 to 4,294,967,295 where the tunnel interfaces of this VPN must be configured.</p> <p>The OSPF area ID is applicable when the routing topology is OSPF-Dynamic Routing in route-based site-to-site VPNs.</p>
Max retransmission time	<p>Select the retransmission timer to limit the number of times the RIP demand circuit re-sends update messages to an unresponsive peer.</p> <p>If the configured retransmission threshold is reached, routes from the next-hop router are marked as unreachable and the hold-down timer starts. You must configure a pair of RIP demand circuits for this timer to take effect. The retransmission range is from 5 to 180 seconds, and the default value is 50 seconds.</p> <p>This option is applicable only when the routing topology is RIP-Dynamic Routing in route-based site-to-site VPN.</p>

Table 196: Add Device page settings (Continued)

Settings	Guidelines
AS number	<p>Select a unique number to assign to the autonomous system (AS).</p> <p>The AS number identifies an autonomous system and enables the system to exchange exterior routing information with other neighboring autonomous systems. The valid range is from 0 to 4294967294.</p> <p>The AS number is applicable only when the routing topology is e-BGP Dynamic Routing in route-based site-to-site VPN.</p>
Protected networks	<p>Configure the addresses or the interface type for the selected device to protect one area of the network from the other.</p> <p>When a dynamic routing protocol is selected, the interface option is displayed. You can also create addresses by clicking the + sign.</p> <p>This option is applicable only for route-based site-to-site VPNs.</p>

Table 197: IKE and IPsec Settings

Settings	Guidelines
IKE Settings	

Table 197: IKE and IPsec Settings (Continued)

Settings	Guidelines
Authentication method	<p>Select an authentication method from the list that the device uses to authenticate the source of IKE messages.</p> <ul style="list-style-type: none"> • Pre-shared based—Specifies that a pre-shared 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. • 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.
IKE version	<p>Select the required IKE version, either V1 or V2, that is used to negotiate dynamic security associations (SAs) for IPsec.</p> <p>By default, IKE V2 is used.</p>
Mode	<p>Select an IKE policy mode.</p> <ul style="list-style-type: none"> • Main—Uses 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. This mode provides identity protection. • Aggressive—Takes half the number of messages of main mode, has less negotiation power, and does not provide identity protection. <p>Mode is applicable when the IKE Version is V1.</p>
Encryption algorithm	<p>Select the appropriate encryption mechanism.</p>
Authentication algorithm	<p>Select an algorithm.</p> <p>The device uses this algorithm to verify the authenticity and integrity of a packet.</p>

Table 197: IKE and IPsec Settings (Continued)

Settings	Guidelines
Diffie Hellman group	<p>Select a group.</p> <p>Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process.</p>
Lifetime seconds	<p>Select a lifetime of an IKE security association (SA).</p> <p>The valid range is from 180 to 86400 seconds.</p>
Dead peer detection	<p>Enable this option to permit the two gateways to determine if the peer gateway is up and responding to the Dead Peer Detection (DPD) messages that are negotiated during IPsec establishment.</p>
DPD mode	<p>Select a DPD Mode.</p> <ul style="list-style-type: none"> • Optimized: R-U-THERE messages are triggered if there is no incoming IKE or IPsec traffic within a configured interval after the device sends outgoing packets to the peer. This is the default mode. • Probe Idle Tunnel: R-U-THERE messages are triggered if there is no incoming or outgoing IKE or IPsec traffic within a configured interval. R-U-THERE messages are sent periodically to the peer until there is traffic activity. • Always-send: R-U-THERE messages are sent at configured intervals regardless of traffic activity between the peers.
DPD interval	<p>Select an interval in seconds to send dead peer detection messages.</p> <p>The default interval is 10 seconds with a valid range of 2 to 60 seconds.</p>
DPD threshold	<p>Select the failure DPD threshold value.</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 with a valid range of 1 to 5.</p>
Advance Settings	

Table 197: IKE and IPsec Settings (Continued)

Settings	Guidelines
General IKE ID	<p>Enable this option to accept peer IKE ID.</p> <p>This option is disabled by default. If General IKE ID is enabled, the IKE ID option is disabled automatically.</p>
IKEv2 re authentication	<p>Select a reauthentication frequency.</p> <p>Reauthentication can be disabled by setting the reauthentication frequency to 0. The valid range is 0 to 100.</p>
IKEv2 re fragmentation support	<p>Enable this option to split a large IKEv2 message into a set of smaller ones so that there is no fragmentation at the IP level.</p>
IKEv2 re-fragment size	<p>Select the size of the packet at which messages are fragmented.</p> <p>By default, the size is 576 bytes for IPv4, and the valid range is 570 to 1320 bytes.</p>
IKE ID	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • None • Distinguished name • Hostname • IPv4 address • E-mail Address <p>IKE ID is applicable only when General IKE ID is disabled.</p>
NAT-T	<p>Enable Network Address Translation-Traversal (NAT-T) if the dynamic endpoint is behind a NAT device.</p>
Keep alive	<p>Select a period in seconds to keep the connection alive.</p> <p>NAT Keepalives are required to maintain the NAT translation during the connection between the VPN peers. The valid range is from 1 to 300 seconds.</p>

Table 197: IKE and IPsec Settings (*Continued*)

Settings	Guidelines
IPSec Settings	
Protocol	<p>Select the required protocol to establish the VPN.</p> <ul style="list-style-type: none"> • ESP—The Encapsulating Security Payload (ESP) protocol provides both encryption and authentication. • AH—The Authentication Header (AH) protocol provides data integrity and data authentication.
Encryption algorithm	<p>Select the encryption method.</p> <p>This option is applicable if the Protocol is ESP.</p>
Authentication algorithm	<p>Select an algorithm.</p> <p>The device uses these algorithms to verify the authenticity and integrity of a packet.</p>
Perfect forward secrecy	<p>Select Perfect Forward Secrecy (PFS) as the method that the device uses to generate the encryption key.</p> <p>The PFS generates each new encryption key independently from the previous key. The higher numbered groups provide more security but require more processing time.</p>
Establish tunnel	<p>Select an option to specify when IKE is activated.</p> <ul style="list-style-type: none"> • Immediately—IKE is activated immediately after VPN configuration changes are committed. • On-traffic—IKE is activated only when data traffic flows and must be negotiated with the peer gateway. This is the default behavior.
Advance Settings	
VPN monitor	<p>Enable this option to send Internet Control Message Protocol (ICMP) to determine if the VPN is up.</p>

Table 197: IKE and IPsec Settings (*Continued*)

Settings	Guidelines
Optimized	<p>Enable this option to optimize VPN monitoring and configure SRX Series Firewalls to send ICMP echo requests, also called pings, only when there is outgoing traffic and no incoming traffic from the configured peer through the VPN tunnel.</p> <p>If there is incoming traffic through the VPN tunnel, the SRX Series Firewalls considers the tunnel to be active and do not send pings to the peer.</p>
Anti replay	<p>Enable this option for the IPsec mechanism to protect against a VPN attack that uses a sequence of numbers that are built into the IPsec packet.</p> <p>IPsec does not accept a packet for which it has already seen the same sequence number. It checks the sequence numbers and enforces the check rather than just ignoring the sequence numbers.</p> <p>Disable this option if there is an error with the IPsec mechanism that results in out-of-order packets, preventing proper functionality.</p> <p>By default, Anti-Replay detection is enabled.</p>
Install interval	<p>Select the maximum number of seconds to allow for the installation of a re-keyed outbound security association (SA) on the device.</p>
Idle time	<p>Select the appropriate idle time interval.</p> <p>The sessions and their corresponding translations typically time out after a certain period if no traffic is received.</p>
DF bit	<p>Select an option to process the Don't Fragment (DF) bit in IP messages.</p> <ul style="list-style-type: none"> • Clear—Disable the DF bit from the IP messages. This is the default option. • Copy—Copy the DF bit to the IP messages. • Set—Enable the DF bit in the IP messages.

Table 197: IKE and IPsec Settings (Continued)

Settings	Guidelines
Copy outer DSCP	<p>Enable this option to allow copying of the Differentiated Services Code Point (DSCP) field from the outer IP header encrypted packet to the inner IP header plain text message on the decryption path.</p> <p>The benefit in enabling this option is that after IPsec decryption, clear text packets can follow the inner class-of-service (CoS) rules.</p>
Lifetime seconds	<p>Select a lifetime in seconds of an IKE security association (SA).</p> <p>The valid range is from 180 to 86,400 seconds.</p>
Lifetime kilobytes	<p>Select the lifetime in kilobytes of an IPsec security association (SA).</p> <p>The range is from 64 through 4294967294 kilobytes.</p>

Create a Hub-and-Spoke (Establishment All Peers) VPN

The hub-and-spoke (establishment all peers) VPN connects spokes together by sending traffic through the hub.

Before You Begin

- Read the ["IPsec VPN Overview" on page 494](#) topic.
- Review the IPsec VPN main page for an understanding of your current data set. See ["IPsec VPN Main Page Fields" on page 499](#) for the field descriptions.
- Create addresses and address sets. See ["Create Addresses or Address Groups" on page 863](#) .
- Create VPN profiles. See ["Creating VPN Profiles" on page 576](#)
- Define extranet devices. See ["Creating Extranet Devices" on page 587](#) .

1. Select **SRX > IPsec VPN > IPsec VPNs**.

The IPsec VPNs page opens.

2. Click **Create > Route Based - Hub and Spoke (Establishment All Peers)**.

The Create Hub-and-Spoke (Establishment All Peers) VPN page opens.

3. Complete the VPN configuration parameters according to the guidelines provided in [Table 198 on page 525](#) .

NOTE: Click **View IKE/IPsec Settings** to view or edit VPN profiles. If the VPN profile is default, you can edit the configurations. If the profile is shared, you can only view the configurations.

The VPN connectivity will change from gray to blue line in the topology to show that the configuration is complete. The topology displayed for hub-and-spoke is only a representation. You can configure maximum one hub.

4. Click **Save** to save the IPsec VPN configuration.

Table 198: Create Hub-and-Spoke (Establishment All Peers) VPN Page Settings

Settings	Guidelines
Name	<p>Enter a unique string of maximum 63 alphanumeric characters without spaces.</p> <p>The string can contain colons, periods, dashes, and underscores.</p>
Description	<p>Enter a description containing maximum 255 characters for the VPN.</p>

Table 198: Create Hub-and-Spoke (Establishment All Peers) VPN Page Settings (*Continued*)

Settings	Guidelines
Routing Topology	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • Traffic selector (Auto route insertion)—A traffic selector is an agreement between IKE peers to permit traffic through a tunnel if the traffic matches a specified pair of local and remote addresses. • Static routing—Generates static routing based on the protected networks or zones per device. • OSPF-dynamic routing—Generates OSPF configuration. • RIP-dynamic routing—Generates RIP configuration. • eBGP-dynamic routing—Generates eBGP configuration.
VPN Profile	<p>Select a VPN profile from the drop-down list based on the deployment scenario.</p> <ul style="list-style-type: none"> • The Inline profile is applicable only to a particular IPsec VPN. You can view and edit the details by clicking View IKE/IPsec settings on the Create VPN page. • The Shared profile can be used by one or more IPsec VPNs. You can only view the details of the shared profiles by clicking View IKE/IPsec settings.

Table 198: Create Hub-and-Spoke (Establishment All Peers) VPN Page Settings (Continued)

Settings	Guidelines
Authentication Method	<p>Select an authentication method from the list that the device uses to authenticate the source of IKE messages.</p> <ul style="list-style-type: none"> • Pre-shared based—Specifies that a pre-shared 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. • 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.
Max Transmission Unit	<p>Select the maximum transmission unit (MTU) in bytes.</p> <p>MTU defines the maximum size of an IP packet, including the IPsec overhead. You can specify the MTU value for the tunnel endpoint. The valid range is 68 to 9192 bytes, and the default value is 1500 bytes.</p>

Table 198: Create Hub-and-Spoke (Establishment All Peers) VPN Page Settings (Continued)

Settings	Guidelines
Pre-shared Key	<p>Establish a VPN connection using pre-shared keys, which is essentially a password that is same for both parties.</p> <p>Select the type of pre-shared key to use:</p> <ul style="list-style-type: none"> • Autogenerate—Select if you want to automatically generate a unique key per tunnel. When selected, the Generate Unique key per tunnel option is automatically enabled. If you disable Generate Unique key per tunnel option, Juniper Security Director Cloud generates a single key for all tunnels. • Manual—Select to enter the key manually. By default, the manual key is masked. <p>Pre-shared keys are applicable only if the authentication method is pre-shared based.</p>
Network IP	<p>Enter the IP address of the numbered tunnel interface.</p> <p>This is the subnet address from where the IP address is automatically assigned for tunnel interfaces.</p>
Number of Spoke Devices Per Tunnel Interface	<p>Select All or specify the number of spoke devices to share one tunnel interface on hub.</p>
Devices	<p>Add devices as endpoints in the VPN.</p> <p>To add devices in route-based VPNs:</p> <ol style="list-style-type: none"> a. Click Add, and click one of the following: Hub Device, Spoke Device, or Extranet Spoke Device. The Add Device page opens. b. Configure the device parameters as described in Table 199 on page 529 . c. Click OK.

Table 199: Add Device Page Settings

Settings	Guidelines
Device	Select a device.
External Interface	<p>Select the outgoing interface for IKE security associations (SAs).</p> <p>This interface is associated with a zone that acts as its carrier, providing firewall security for it.</p>
Tunnel Zone	<p>Select the tunnel zone.</p> <p>Tunnel zones are logical areas of address space that can support dynamic IP (DIP) address pools for NAT applications to pre- and post-encapsulated IPsec traffic. Tunnel zones also provide flexibility in combining tunnel interfaces with VPN tunnels.</p>
Metric	Specify the cost for an access route for the next hop.
Routing instance	Select the required routing instance.
Certificate	<p>Select a certificate to authenticate the virtual private network (VPN) initiator and recipient.</p> <p>This is applicable in one of the following scenarios:</p> <ul style="list-style-type: none"> • The VPN profile is RSA profile or ADVPN profile. • The authentication method is RSA-Signatures, DSA-Signatures, ECDSA-Signatures-256, or ECDSA-Signatures-384.
Trusted CA/Group	<p>Select the CA profile from the list to associate it with the local certificate.</p> <p>This is applicable in one of the following scenarios:</p> <ul style="list-style-type: none"> • The VPN profile is RSA profile or ADVPN profile. • The authentication method is RSA-Signatures, DSA-Signatures, ECDSA-Signatures-256, or ECDSA-Signatures-384.

Table 199: Add Device Page Settings (Continued)

Settings	Guidelines
Export	<p>Select the type of routes to export.</p> <ul style="list-style-type: none"> • Select the Static Routes check box to export static routes. <p>Juniper Security Director Cloud simplifies VPN address management by enabling the administrator to export static routes to a remote site over a tunnel, allowing the static route networks to participate in the VPN. However, only devices on the hub side can export static default routes to the device side. Devices at the spoke side cannot export static default routes over a tunnel.</p> <p>For eBGP Dynamic Routing, the Static Routes check box is selected by default.</p> <ul style="list-style-type: none"> • Select the RIP Routes check box to export RIP routes. <p>You can export RIP routes only when Routing Topology is OSPF Dynamic Routing.</p> <ul style="list-style-type: none"> • Select the OSPF Routes check box to export OSPF routes. <p>You can export OSPF routes only when Routing Topology is RIP-Dynamic Routing.</p> <p>If you select OSPF or RIP export, the OSPF or RIP routes outside the VPN network is imported into a VPN network through OSPF or RIP Dynamic routing protocols.</p>
OSPF Area	<p>Select an OSPF area ID within the range of 0 to 4,294,967,295 where the tunnel interfaces of this VPN must be configured.</p> <p>The OSPF area ID is applicable when the Routing Topology is OSPF-Dynamic Routing.</p>
Max Retransmission Time	<p>Select the retransmission timer to limit the number of times the RIP demand circuit re-sends update messages to an unresponsive peer.</p> <p>If the configured retransmission threshold is reached, routes from the next-hop router are marked as unreachable and the hold-down timer starts. You must configure a pair of RIP demand circuits for this timer to take effect.</p> <p>The retransmission range is from 5 to 180 seconds and the default value is 50 seconds.</p> <p>This option is applicable only when Routing Topology is RIP-Dynamic Routing.</p>

Table 199: Add Device Page Settings (Continued)

Settings	Guidelines
AS Number	<p>Select a unique number to assign to the autonomous system (AS).</p> <p>The AS number identifies an autonomous system and enables the system to exchange exterior routing information with other neighboring autonomous systems. The valid range is from 0 to 4294967295.</p> <p>The AS number is applicable only when Routing Topology is e-BGP Dynamic Routing.</p>
Protected Networks	<p>Configure the addresses or interface type for the selected device to protect one area of the network from the other.</p> <p>When a dynamic routing protocol is selected, the interface option is displayed.</p> <p>You can also create addresses by clicking Add New Address.</p>

Table 200: View IKE/IPsec Settings

Settings	Guidelines
IKE Settings	
IKE Version	<p>Select the required IKE version, either V1 or V2, that is used to negotiate dynamic security associations (SAs) for IPsec.</p> <p>By default, IKE V2 is used.</p>
Mode	<p>Select an IKE policy mode.</p> <ul style="list-style-type: none"> • Main—Uses 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. This mode also provides identity protection. • Aggressive—Takes half the number of messages of main mode, has less negotiation power, and does not provide identity protection. <p>Mode is applicable when the IKE Version is V1.</p>
Encryption Algorithm	Select the appropriate encryption mechanism.

Table 200: View IKE/IPsec Settings (Continued)

Settings	Guidelines
Authentication Algorithm	<p>Select an algorithm.</p> <p>The device uses this algorithm to verify the authenticity and integrity of a packet.</p>
Diffie Hellman group	<p>Select a group.</p> <p>Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process.</p>
Lifetime Seconds	<p>Select a lifetime of an IKE security association (SA).</p> <p>The valid range is from 180 to 86400 seconds.</p>
Dead Peer Detection	<p>Enable this option to permit the two gateways to determine if the peer gateway is up and responding to the Dead Peer Detection (DPD) messages that are negotiated during IPsec establishment.</p>
DPD Mode	<p>Select a DPD Mode.</p> <ul style="list-style-type: none"> • Optimized: R-U-THERE messages are triggered if there is no incoming IKE or IPsec traffic within a configured interval after the device sends outgoing packets to the peer. This is the default mode. • Probe Idle Tunnel: R-U-THERE messages are triggered if there is no incoming or outgoing IKE or IPsec traffic within a configured interval. R-U-THERE messages are sent periodically to the peer until there is traffic activity. • Always-send: R-U-THERE messages are sent at configured intervals regardless of traffic activity between the peers.
DPD Interval	<p>Select an interval in seconds to send dead peer detection messages.</p> <p>The default interval is 10 seconds with a valid range of 2 to 60 seconds.</p>
DPD Threshold	<p>Select the failure DPD threshold value.</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 with a valid range of 1 to 5.</p>

Table 200: View IKE/IPsec Settings (Continued)

Settings	Guidelines
Advance Settings	
General IKE ID	<p>Enable this option to accept peer IKE ID.</p> <p>This option is disabled by default. If General IKE ID is enabled, the IKE ID option is disabled automatically.</p>
IKEv2 Re Authentication	<p>Select a reauthentication frequency. Reauthentication can be disabled by setting the reauthentication frequency to 0.</p> <p>The valid range is from 0 to 100.</p>
IKEv2 Re Fragmentation Support	<p>Enable this option to split a large IKEv2 message into a set of smaller ones so that there is no fragmentation at the IP level.</p>
IKEv2 Re-fragment Size	<p>Select the size of the packet at which messages are fragmented.</p> <p>By default, the size is 576 bytes for IPv4, and the valid range is from 570 to 1320.</p>
IKE ID	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • None • Distinguished name • Hostname • IPv4 address • E-mail Address <p>IKE ID is applicable only when General IKE ID is disabled.</p>
NAT-T	<p>Enable Network Address Translation-Traversal (NAT-T) if the dynamic endpoint is behind a NAT device.</p>

Table 200: View IKE/IPsec Settings (Continued)

Settings	Guidelines
Keep Alive	<p>Select a period in seconds to keep the connection alive.</p> <p>NAT Keepalives are required to maintain the NAT translation during the connection between the VPN peers.</p> <p>The valid range is from 1 to 300 seconds.</p>
IPsec Settings	
Protocol	<p>Select the required protocol to establish the VPN.</p> <ul style="list-style-type: none"> • ESP—The Encapsulating Security Payload (ESP) protocol provides both encryption and authentication. • AH—The Authentication Header (AH) protocol provides data integrity and data authentication.
Encryption Algorithm	<p>Select the encryption method.</p> <p>This option is applicable if the Protocol is ESP.</p>
Authentication Algorithm	<p>Select an algorithm.</p> <p>The device uses these algorithms to verify the authenticity and integrity of a packet.</p>
Perfect Forward Secrecy	<p>Select Perfect Forward Secrecy (PFS) as the method that the device uses to generate the encryption key.</p> <p>The PFS generates each new encryption key independently from the previous key. The higher numbered groups provide more security but require more processing time.</p>
Establish Tunnel	<p>Select an option to specify when IKE is activated.</p> <ul style="list-style-type: none"> • Immediately—IKE is activated immediately after VPN configuration changes are committed. • On-traffic—IKE is activated only when data traffic flows and must be negotiated with the peer gateway. This is the default behavior.

Table 200: View IKE/IPsec Settings (*Continued*)

Settings	Guidelines
Advance Settings	
VPN Monitor	<p>Enable this option to send Internet Control Message Protocol (ICMP) to determine if the VPN is up.</p>
Optimized	<p>Enable this option to optimize VPN monitoring and configure SRX Series Firewalls to send ICMP echo requests, also called pings, only when there is outgoing traffic and no incoming traffic from the configured peer through the VPN tunnel.</p> <p>If there is incoming traffic through the VPN tunnel, the SRX Series Firewalls considers the tunnel to be active and do not send pings to the peer.</p>
Anti Replay	<p>Enable this option for the IPsec mechanism to protect against a VPN attack that uses a sequence of numbers that are built into the IPsec packet.</p> <p>IPsec does not accept a packet for which it has already seen the same sequence number. It checks the sequence numbers and enforces the check rather than just ignoring the sequence numbers.</p> <p>Disable this option if there is an error with the IPsec mechanism that results in out-of-order packets, preventing proper functionality.</p> <p>By default, Anti-Replay detection is enabled.</p>
Install interval	<p>Select the maximum number of seconds to allow for the installation of a re-keyed outbound security association (SA) on the device.</p>
Idle Time	<p>Select the appropriate idle time interval.</p> <p>The sessions and their corresponding translations typically time out after a certain period if no traffic is received.</p>
DF Bit	<p>Select an option to process the Don't Fragment (DF) bit in IP messages.</p> <ul style="list-style-type: none"> • Clear—Disable the DF bit from the IP messages. This is the default option. • Copy—Copy the DF bit to the IP messages. • Set—Enable the DF bit in the IP messages.

Table 200: View IKE/IPsec Settings (Continued)

Settings	Guidelines
Copy Outer DSCP	<p>Enable this option to allow copying of the Differentiated Services Code Point (DSCP) field from the outer IP header encrypted packet to the inner IP header plain text message on the decryption path.</p> <p>The benefit in enabling this feature is that after IPsec decryption, clear text packets can follow the inner class-of-service (CoS) rules.</p>
Lifetime Seconds	<p>Select a lifetime of an IKE security association (SA).</p> <p>The valid range is from 180 to 86400 seconds.</p>
Lifetime kilobytes	<p>Select the lifetime in kilobytes of an IPsec security association (SA).</p> <p>The valid range is from 64 to 4294967294 kilobytes.</p>

Create a Hub-and-Spoke (Establishment by Spokes) VPN

Auto-VPN allows you to configure a hub for current and future spokes. No configuration changes are required on the hub when spoke devices are added or deleted, which allows administrators flexibility in managing large-scale network deployments.

Before You Begin

- Read the ["IPsec VPN Overview" on page 494](#) topic.
- Review the IPsec VPN main page for an understanding of your current data set. See ["IPsec VPN Main Page Fields" on page 499](#) for the field descriptions.
- Create addresses and address sets. See ["Create Addresses or Address Groups" on page 863](#) .
- Create VPN profiles. See ["Creating VPN Profiles" on page 576](#) .

1. Select **SRX > IPsec VPN > IPsec VPNs**.

The IPsec VPNs page opens.

2. Click **Create > Route Based - Hub and Spoke (Establishment by Spokes)**.

The Create Hub-and-Spoke (Establishment by Spokes) VPN page opens.

3. Complete the VPN configuration parameters according to the guidelines provided in [Table 201 on page 537](#).

NOTE: Click **View IKE/IPsec Settings** to view or edit VPN profiles. If the VPN profile is default, you can edit the configurations. If the profile is shared, you can only view the configurations.

The VPN connectivity will change from gray to blue line in the topology to show that the configuration is complete. The topology displayed for hub-and-spoke is only a representation. You can configure maximum one hub.

4. Click **Save** to save the IPsec VPN configuration.

Table 201: Create Hub-and-Spoke (Establishment By Spokes) VPN Page Settings

Settings	Guidelines
Name	<p>Enter a unique string of maximum 63 alphanumeric characters without spaces.</p> <p>The string can contain colons, periods, dashes, and underscores.</p>
Description	<p>Enter a description containing maximum 255 characters for the VPN.</p>
Routing Topology	<p>Select OSPF-dynamic routing to generate the OSPF configuration.</p>
VPN Profile	<p>Select a VPN profile from the drop-down list based on the deployment scenario.</p> <ul style="list-style-type: none"> • The Inline profile is applicable only to a particular IPsec VPN. You can view and edit the details by clicking View IKE/IPsec settings on the Create VPN page. • The Shared profile can be used by one or more IPsec VPNs. You can only view the details of the shared profiles by clicking View IKE/IPsec settings.

Table 201: Create Hub-and-Spoke (Establishment By Spokes) VPN Page Settings (Continued)

Settings	Guidelines
Authentication Method	<p>Select an authentication method from the list that the device uses to authenticate the source of IKE messages.</p> <ul style="list-style-type: none"> • RSA-Signatures—Specifies that a public key algorithm, which supports encryption and digital signatures is used. • DSA-Signatures—Specifies that the Digital Signature Algorithm (DSA) is used. • ECDSA-Signatures-256—Specifies that the Elliptic Curve DSA (ECDSA) using the 256-bit elliptic curve secp256r1, as specified in the Federal Information Processing Standard (FIPS) Digital Signature Standard (DSS) 186-3, is used. • ECDSA-Signatures-384—Specifies that the ECDSA using the 384-bit elliptic curve secp384r1, as specified in the FIPS DSS 186-3, is used.
Max Transmission Unit	<p>Select the maximum transmission unit (MTU) in bytes.</p> <p>MTU defines the maximum size of an IP packet, including the IPsec overhead. You can specify the MTU value for the tunnel endpoint. The valid range is 68 to 9192 bytes, and the default value is 1500 bytes.</p>
Network IP	<p>Enter the IP address of the numbered tunnel interface.</p> <p>This is the subnet address from where the IP address is automatically assigned for tunnel interfaces.</p>

Table 201: Create Hub-and-Spoke (Establishment By Spokes) VPN Page Settings (Continued)

Settings	Guidelines
Devices	<p>Add devices as endpoints in the VPN.</p> <p>To add devices in route-based VPNs:</p> <ol style="list-style-type: none"> 1. Click Add, and click one of the following: Hub Device, Spoke Device, or Extranet Spoke Device. <p>The Add Device page opens.</p> <ol style="list-style-type: none"> 2. Configure the device parameters as described in Table 202 on page 539. 3. Click OK.

Table 202: Add Device Page Settings

Settings	Guidelines
Device	Select a device.
External Interface	<p>Select the outgoing interface for IKE security associations (SAs). \</p> <p>This interface is associated with a zone that acts as its carrier, providing firewall security for it.</p>
Tunnel Zone	<p>Select the tunnel zone.</p> <p>Tunnel zones are logical areas of address space that can support dynamic IP (DIP) address pools for NAT applications to pre- and post-encapsulated IPsec traffic. Tunnel zones also provide flexibility in combining tunnel interfaces with VPN tunnels.</p>
Metric	Specify the cost for an access route for the next hop.
Routing instance	Select the required routing instance.

Table 202: Add Device Page Settings (Continued)

Settings	Guidelines
Certificate	<p>Select a certificate to authenticate the virtual private network (VPN) initiator and recipient.</p> <p>This is applicable in one of the following scenarios:</p> <ul style="list-style-type: none"> • The VPN profile is RSA profile or ADVPN profile. • The authentication method is RSA-Signatures, DSA-Signatures, ECDSA-Signatures-256, or ECDSA-Signatures-384.
Trusted CA/ Group	<p>Select the CA profile from the list to associate it with the local certificate.</p> <p>This is applicable in one of the following scenarios:</p> <ul style="list-style-type: none"> • The VPN profile is RSA profile or ADVPN profile. • The authentication method is RSA-Signatures, DSA-Signatures, ECDSA-Signatures-256, or ECDSA-Signatures-384.
Export	<p>Select the type of routes to export.</p> <ul style="list-style-type: none"> • Select the Static Routes check box to export static routes. <p>Juniper Security Director Cloud simplifies VPN address management by enabling the administrator to export static routes to a remote site over a tunnel, allowing the static route networks to participate in the VPN. However, only devices on the hub side can export static default routes to the device side. Devices at the spoke side cannot export static default routes over a tunnel.</p> <p>For eBGP Dynamic Routing, the Static Routes check box is selected by default.</p> <ul style="list-style-type: none"> • Select the RIP Routes check box to export RIP routes. <p>You can export RIP routes only when Routing Topology is OSPF Dynamic Routing.</p> <ul style="list-style-type: none"> • Select the OSPF Routes check box to export OSPF routes. <p>You can export OSPF routes only when Routing Topology is RIP-Dynamic Routing.</p> <p>If you select OSPF or RIP export, the OSPF or RIP routes outside the VPN network is imported into a VPN network through OSPF or RIP Dynamic routing protocols.</p>

Table 202: Add Device Page Settings (Continued)

Settings	Guidelines
OSPF Area	<p>Select an OSPF area ID within the range of 0 to 4,294,967,295 where the tunnel interfaces of this VPN must be configured.</p> <p>The OSPF area ID is applicable when the Routing Topology is OSPF-Dynamic Routing.</p>
Protected Networks	<p>Configure the addresses or interface type for the selected device to protect one area of the network from the other.</p> <p>When a dynamic routing protocol is selected, the interface option is displayed.</p> <p>You can also create addresses by clicking Add New Address.</p>

Table 203: View IKE/IPsec Settings

Settings	Guidelines
IKE Settings	
IKE Version	<p>Select the required IKE version, either V1 or V2, that is used to negotiate dynamic security associations (SAs) for IPsec.</p> <p>By default, IKE V2 is used.</p>
Mode	<p>Select an IKE policy mode.</p> <ul style="list-style-type: none"> • Main—Uses 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. This mode also provides identity protection. • Aggressive—Takes half the number of messages of main mode, has less negotiation power, and does not provide identity protection. <p>Mode is applicable when the IKE Version is V1.</p>
Encryption Algorithm	Select the appropriate encryption mechanism.
Authentication Algorithm	<p>Select an algorithm.</p> <p>The device uses this algorithm to verify the authenticity and integrity of a packet.</p>

Table 203: View IKE/IPsec Settings (Continued)

Settings	Guidelines
Diffie Hellman group	<p>Select a group.</p> <p>Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process.</p>
Lifetime Seconds	<p>Select a lifetime of an IKE security association (SA).</p> <p>The valid range is from 180 to 86400 seconds.</p>
Dead Peer Detection	<p>Enable this option to permit the two gateways to determine if the peer gateway is up and responding to the Dead Peer Detection (DPD) messages that are negotiated during IPsec establishment.</p>
DPD Mode	<p>Select a DPD Mode.</p> <ul style="list-style-type: none"> • Optimized: R-U-THERE messages are triggered if there is no incoming IKE or IPsec traffic within a configured interval after the device sends outgoing packets to the peer. This is the default mode. • Probe Idle Tunnel: R-U-THERE messages are triggered if there is no incoming or outgoing IKE or IPsec traffic within a configured interval. R-U-THERE messages are sent periodically to the peer until there is traffic activity. • Always-send: R-U-THERE messages are sent at configured intervals regardless of traffic activity between the peers.
DPD Interval	<p>Select an interval in seconds to send dead peer detection messages.</p> <p>The default interval is 10 seconds with a valid range of 2 to 60 seconds.</p>
DPD Threshold	<p>Select the failure DPD threshold value.</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 with a valid range of 1 to 5.</p>
Advance Settings	

Table 203: View IKE/IPsec Settings (Continued)

Settings	Guidelines
General IKE ID	<p>Enable this option to accept peer IKE ID</p> <p>This option is disabled by default. If General IKE ID is enabled, the IKE ID option is disabled automatically.</p>
IKEv2 Re Authentication	<p>Select a reauthentication frequency. Reauthentication can be disabled by setting the reauthentication frequency to 0.</p> <p>The valid range is 0 to 100.</p>
IKEv2 Re Fragmentation Support	<p>Enable this option to split a large IKEv2 message into a set of smaller ones so that there is no fragmentation at the IP level.</p>
IKEv2 Re-fragment Size	<p>Select the size of the packet at which messages are fragmented.</p> <p>By default, the size is 576 bytes for IPv4, and the valid range is 570 to 1320.</p>
IKE ID	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • None • Distinguished name • Hostname • IPv4 address • E-mail Address <p>IKE ID is applicable only when General IKE ID is disabled.</p>
NAT-T	<p>Enable Network Address Translation-Traversal (NAT-T) if the dynamic endpoint is behind a NAT device.</p>

Table 203: View IKE/IPsec Settings (Continued)

Settings	Guidelines
Keep Alive	<p>Select a period in seconds to keep the connection alive.</p> <p>NAT Keepalives are required to maintain the NAT translation during the connection between the VPN peers.</p> <p>The valid range is from 1 to 300 seconds.</p>
IPsec Settings	
Protocol	<p>Select the required protocol to establish the VPN.</p> <ul style="list-style-type: none"> • ESP—The Encapsulating Security Payload (ESP) protocol provides both encryption and authentication. • AH—The Authentication Header (AH) protocol provides data integrity and data authentication.
Encryption Algorithm	<p>Select the encryption method.</p> <p>This is applicable if the Protocol is ESP.</p>
Authentication Algorithm	<p>Select an algorithm.</p> <p>The device uses these algorithms to verify the authenticity and integrity of a packet.</p>
Perfect Forward Secrecy	<p>Select Perfect Forward Secrecy (PFS) as the method that the device uses to generate the encryption key.</p> <p>The PFS generates each new encryption key independently from the previous key. The higher numbered groups provide more security but require more processing time.</p>
Establish Tunnel	<p>Select an option to specify when IKE is activated.</p> <ul style="list-style-type: none"> • Immediately—IKE is activated immediately after VPN configuration changes are committed. • On-traffic—IKE is activated only when data traffic flows and must be negotiated with the peer gateway. This is the default behavior.

Table 203: View IKE/IPsec Settings (Continued)

Settings	Guidelines
Advance Settings	
VPN Monitor	<p>Enable this option to send Internet Control Message Protocol (ICMP) to determine if the VPN is up.</p>
Optimized	<p>Enable this option to optimize VPN monitoring and configure SRX Series Firewalls to send ICMP echo requests, also called pings, only when there is outgoing traffic and no incoming traffic from the configured peer through the VPN tunnel.</p> <p>If there is incoming traffic through the VPN tunnel, the SRX Series Firewalls considers the tunnel to be active and do not send pings to the peer.</p>
Anti Replay	<p>Enable this option for the IPsec mechanism to protect against a VPN attack that uses a sequence of numbers that are built into the IPsec packet.</p> <p>IPsec does not accept a packet for which it has already seen the same sequence number. It checks the sequence numbers and enforces the check rather than just ignoring the sequence numbers.</p> <p>Disable this option if there is an error with the IPsec mechanism that results in out-of-order packets, preventing proper functionality.</p> <p>By default, Anti-Replay detection is enabled.</p>
Install interval	<p>Select the maximum number of seconds to allow for the installation of a re-keyed outbound security association (SA) on the device.</p>
Idle Time	<p>Select the appropriate idle time interval.</p> <p>The sessions and their corresponding translations typically time out after a certain period if no traffic is received.</p>
DF Bit	<p>Select an option to process the Don't Fragment (DF) bit in IP messages.</p> <ul style="list-style-type: none"> • Clear—Disable the DF bit from the IP messages. This is the default option. • Copy—Copy the DF bit to the IP messages. • Set—Enable the DF bit in the IP messages.

Table 203: View IKE/IPsec Settings (Continued)

Settings	Guidelines
Copy Outer DSCP	<p>Enable this option to allow copying of the Differentiated Services Code Point (DSCP) field from the outer IP header encrypted packet to the inner IP header plain text message on the decryption path.</p> <p>The benefit in enabling this feature is that after IPsec decryption, clear text packets can follow the inner class-of-service (CoS) rules.</p>
Lifetime Seconds	<p>Select a lifetime of an IKE security association (SA).</p> <p>The valid range is from 180 to 86400 seconds.</p>
Lifetime Kilobytes	<p>Select the lifetime in kilobytes of an IPsec security association (SA).</p> <p>The valid range is from 64 to 4294967294 kilobytes.</p>

Create a Hub-and-Spoke Auto Discovery VPN

The Auto-Discovery VPN (ADVPN) dynamically establishes VPN tunnels between spokes to avoid routing traffic through the hub.

Before You Begin

- Read the ["IPsec VPN Overview" on page 494](#) topic.
- Review the IPsec VPN main page for an understanding of your current data set. See ["IPsec VPN Main Page Fields" on page 499](#) for the field descriptions.
- Create addresses and address sets. See ["Create Addresses or Address Groups" on page 863](#)
- Create VPN profiles. See ["Creating VPN Profiles" on page 576](#) .

1. Select **SRX > IPsec VPN > IPsec VPNs**.

The IPsec VPNs page opens.

2. Click **Create > Route Based - Hub and Spoke (ADVPN - Auto Discovery VPN)**.

The Create Hub-and-Spoke (ADVPN - Auto Discovery VPN) page opens.

3. Complete the VPN configuration parameters according to the guidelines provided in [Table 201 on page 537](#) .

NOTE: Click **View IKE/IPsec Settings** to view or edit VPN profiles. If the VPN profile is default, you can edit the configurations. If the profile is shared, you can only view the configurations.

The VPN connectivity will change from gray to blue line in the topology to show that the configuration is complete. The topology displayed for hub-and-spoke is only a representation. You can configure any number of hubs and spokes.

4. Click **Save** to save the IPsec VPN configuration.

Table 204: Create Hub-and-Spoke (ADVPN - Auto Discovery VPN) Page Settings

Settings	Guidelines
Name	<p>Enter a unique string of maximum 63 alphanumeric characters without spaces.</p> <p>The string can contain colons, periods, dashes, and underscores.</p>
Description	<p>Enter a description containing maximum 255 characters for the VPN.</p>
Routing Topology	<p>Select OSPF-dynamic routing to generate the OSPF configuration.</p>
VPN Profile	<p>Select a VPN profile from the drop-down list based on the deployment scenario.</p> <ul style="list-style-type: none"> • The Inline profile is applicable only to a particular IPsec VPN. You can view and edit the details by clicking View IKE/IPsec settings on the Create VPN page. • The Shared profile can be used by one or more IPsec VPNs. You can only view the details of the shared profiles by clicking View IKE/IPsec settings.

Table 204: Create Hub-and-Spoke (ADVPN - Auto Discovery VPN) Page Settings *(Continued)*

Settings	Guidelines
Authentication Method	<p>Select an authentication method from the list that the device uses to authenticate the source of IKE messages.</p> <ul style="list-style-type: none"> • RSA-Signatures—Specifies that a public key algorithm, which supports encryption and digital signatures is used. • DSA-Signatures—Specifies that the Digital Signature Algorithm (DSA) is used. • ECDSA-Signatures-256—Specifies that the Elliptic Curve DSA (ECDSA) using the 256-bit elliptic curve secp256r1, as specified in the Federal Information Processing Standard (FIPS) Digital Signature Standard (DSS) 186-3, is used. • ECDSA-Signatures-384—Specifies that the ECDSA using the 384-bit elliptic curve secp384r1, as specified in the FIPS DSS 186-3, is used.
Max Transmission Unit	<p>Select the maximum transmission unit (MTU) in bytes.</p> <p>MTU defines the maximum size of an IP packet, including the IPsec overhead. You can specify the MTU value for the tunnel endpoint. The valid range is 68 to 9192 bytes, and the default value is 1500 bytes.</p>

Table 204: Create Hub-and-Spoke (ADVPN - Auto Discovery VPN) Page Settings (*Continued*)

Settings	Guidelines
Pre-shared Key	<p>Establish a VPN connection using pre-shared keys, which is essentially a password that is same for both parties.</p> <p>Select the type of pre-shared key to use:</p> <ul style="list-style-type: none"> • Autogenerate—Select if you want to automatically generate a unique key per tunnel. When selected, the Generate Unique key per tunnel option is automatically enabled. If you disable Generate Unique key per tunnel option, Security Director generates a single key for all tunnels. • Manual—Select to enter the key manually. By default, the manual key is masked. <p>Pre-shared keys are applicable only if the authentication method is Preshared-based.</p>
Network IP	<p>Enter the IP address of the numbered tunnel interface.</p> <p>This is the subnet address from where the IP address is automatically assigned for tunnel interfaces.</p>
Number of Spoke Devices Per Tunnel Interface	<p>Select All or specify the number of spoke devices to share one tunnel interface on hub.</p>
Devices	<p>Add devices as endpoints in the VPN. You can add maximum two devices.</p> <p>To add devices in route-based VPNs:</p> <ol style="list-style-type: none"> 1. Click Add, and click one of the following: Hub Device, Spoke Device, or Extranet Spoke Device. <p>The Add Device page opens.</p> <ol style="list-style-type: none"> 2. Configure the device parameters as described in Table 202 on page 539. 3. Click OK.

Table 205: Add Device Page Settings

Settings	Guidelines
Device	Select a device.
External Interface	<p>Select the outgoing interface for IKE security associations (SAs).</p> <p>This interface is associated with a zone that acts as its carrier, providing firewall security for it.</p>
Tunnel Zone	<p>Select the tunnel zone.</p> <p>Tunnel zones are logical areas of address space that can support dynamic IP (DIP) address pools for NAT applications to pre- and post-encapsulated IPsec traffic. Tunnel zones also provide flexibility in combining tunnel interfaces with VPN tunnels.</p>
Metric	Specify the cost for an access route for the next hop.
Routing instance	Select the required routing instance.
Certificate	<p>Select a certificate to authenticate the VPN initiator and recipient.</p> <p>This is applicable in one of the following scenarios:</p> <ul style="list-style-type: none"> • The VPN profile is RSA profile or ADVPN profile. • The authentication method is RSA-Signatures, DSA-Signatures, ECDSA-Signatures-256, or ECDSA-Signatures-384.
Trusted CA/ Group	<p>Select the CA profile from the list to associate it with the local certificate.</p> <p>This is applicable in one of the following scenarios:</p> <ul style="list-style-type: none"> • The VPN profile is RSA profile or ADVPN profile. • The authentication method is RSA-Signatures, DSA-Signatures, ECDSA-Signatures-256, or ECDSA-Signatures-384.

Table 205: Add Device Page Settings (Continued)

Settings	Guidelines
Container	<p>The hub authenticates the spoke's IKE ID if the subject fields of the spoke's certificate exactly match the values configured on the hub.</p> <p>You can specify multiple entries for each subject field. The order of values in the fields must match.</p>
Wildcard	<p>The hub authenticates the spoke's IKE ID if the subject fields of the spoke's certificate match the values configured on the hub.</p> <p>The wildcard match supports only one value per field. The order of the fields is inconsequential</p>
Export	<p>Select the type of routes to export.</p> <ul style="list-style-type: none"> • Select the Static Routes check box to export static routes. <p>Juniper Security Director Cloud simplifies VPN address management by enabling the administrator to export static routes to a remote site over a tunnel, allowing the static route networks to participate in the VPN. However, only devices on the hub side can export static default routes to the device side. Devices at the spoke side cannot export static default routes over a tunnel.</p> <p>For eBGP Dynamic Routing, the Static Routes check box is selected by default.</p> • Select the RIP Routes check box to export RIP routes. <p>You can export RIP routes only when Routing Topology is OSPF Dynamic Routing.</p> • Select the OSPF Routes check box to export OSPF routes. <p>You can export OSPF routes only when Routing Topology is RIP-Dynamic Routing.</p> <p>If you select OSPF or RIP export, the OSPF or RIP routes outside the VPN network is imported into a VPN network through OSPF or RIP Dynamic routing protocols.</p>
OSPF Area	<p>Select an OSPF 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>The OSPF area ID is applicable when the Routing Topology is OSPF-Dynamic Routing.</p>

Table 205: Add Device Page Settings (Continued)

Settings	Guidelines
Protected Networks	<p>Configure the addresses or interface type for the selected device to protect one area of the network from the other.</p> <p>When a dynamic routing protocol is selected, the interface option is displayed.</p> <p>You can also create addresses by clicking Add New Address.</p>

Table 206: View IKE/IPsec Settings

Settings	Guidelines
IKE Settings	
IKE Version	<p>Select the required IKE version, either V1 or V2, that is used to negotiate dynamic security associations (SAs) for IPsec.</p> <p>By default, IKE V2 is used.</p>
Mode	<p>Select an IKE policy mode.</p> <ul style="list-style-type: none"> • Main—Uses 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. This mode also provides identity protection. • Aggressive—Takes half the number of messages of main mode, has less negotiation power, and does not provide identity protection. <p>Mode is applicable when the IKE Version is V1.</p>
Encryption Algorithm	Select the appropriate encryption mechanism.
Authentication Algorithm	<p>Select an algorithm.</p> <p>The device uses this algorithm to verify the authenticity and integrity of a packet.</p>
Diffie Hellman group	<p>Select a group.</p> <p>Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process.</p>

Table 206: View IKE/IPsec Settings (Continued)

Settings	Guidelines
Lifetime Seconds	<p>Select a lifetime of an IKE security association (SA).</p> <p>The valid range is from 180 to 86400 seconds.</p>
Dead Peer Detection	<p>Enable this option to permit the two gateways to determine if the peer gateway is up and responding to the Dead Peer Detection (DPD) messages that are negotiated during IPsec establishment.</p>
DPD Mode	<p>Select a DPD Mode.</p> <ul style="list-style-type: none"> • Optimized: R-U-THERE messages are triggered if there is no incoming IKE or IPsec traffic within a configured interval after the device sends outgoing packets to the peer. This is the default mode. • Probe Idle Tunnel: R-U-THERE messages are triggered if there is no incoming or outgoing IKE or IPsec traffic within a configured interval. R-U-THERE messages are sent periodically to the peer until there is traffic activity. • Always-send: R-U-THERE messages are sent at configured intervals regardless of traffic activity between the peers.
DPD Interval	<p>Select an interval in seconds to send dead peer detection messages.</p> <p>The default interval is 10 seconds with a valid range of 2 to 60 seconds.</p>
DPD Threshold	<p>Select the failure DPD threshold value.</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 with a valid range of 1 to 5.</p>
Advance Settings	
General IKE ID	<p>Enable this option to accept peer IKE ID</p> <p>This option is disabled by default. If General IKE ID is enabled, the IKE ID option is disabled automatically.</p>

Table 206: View IKE/IPsec Settings (Continued)

Settings	Guidelines
IKEv2 Re Authentication	<p>Select a reauthentication frequency. Reauthentication can be disabled by setting the reauthentication frequency to 0.</p> <p>The valid range is 0 to 100.</p>
IKEv2 Re Fragmentation Support	<p>Enable this option to split a large IKEv2 message into a set of smaller ones so that there is no fragmentation at the IP level.</p>
IKEv2 Re-fragment Size	<p>Select the size of the packet at which messages are fragmented.</p> <p>By default, the size is 576 bytes for IPv4, and the valid range is 570 to 1320.</p>
IKE ID	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • None • Distinguished name • Hostname • IPv4 address • E-mail Address <p>IKE ID is applicable only when General IKE ID is disabled.</p>
NAT-T	<p>Enable Network Address Translation-Traversal (NAT-T) if the dynamic endpoint is behind a NAT device.</p>
Keep Alive	<p>Select a period in seconds to keep the connection alive.</p> <p>NAT Keepalives are required to maintain the NAT translation during the connection between the VPN peers.</p> <p>The valid range is from 1 to 300 seconds.</p>
IPsec Settings	

Table 206: View IKE/IPsec Settings (Continued)

Settings	Guidelines
Protocol	<p>Select the required protocol to establish the VPN.</p> <ul style="list-style-type: none"> • ESP—The Encapsulating Security Payload (ESP) protocol provides both encryption and authentication. • AH—The Authentication Header (AH) protocol provides data integrity and data authentication.
Encryption Algorithm	<p>Select the encryption method.</p> <p>This is applicable if the Protocol is ESP.</p>
Authentication Algorithm	<p>Select an algorithm.</p> <p>The device uses these algorithms to verify the authenticity and integrity of a packet.</p>
Perfect Forward Secrecy	<p>Select Perfect Forward Secrecy (PFS) as the method that the device uses to generate the encryption key.</p> <p>The PFS generates each new encryption key independently from the previous key. The higher numbered groups provide more security but require more processing time.</p>
Establish Tunnel	<p>Select an option to specify when IKE is activated.</p> <ul style="list-style-type: none"> • Immediately—IKE is activated immediately after VPN configuration changes are committed. • On-traffic—IKE is activated only when data traffic flows and must be negotiated with the peer gateway. This is the default behavior.
Advance Settings	
VPN Monitor	<p>Enable this option to send Internet Control Message Protocol (ICMP) to determine if the VPN is up.</p>

Table 206: View IKE/IPsec Settings (Continued)

Settings	Guidelines
Optimized	<p>Enable this option to optimize VPN monitoring and configure SRX Series Firewalls to send ICMP echo requests, also called pings, only when there is outgoing traffic and no incoming traffic from the configured peer through the VPN tunnel.</p> <p>If there is incoming traffic through the VPN tunnel, the SRX Series Firewalls considers the tunnel to be active and do not send pings to the peer.</p>
Anti Replay	<p>Enable this option for the IPsec mechanism to protect against a VPN attack that uses a sequence of numbers that are built into the IPsec packet.</p> <p>IPsec does not accept a packet for which it has already seen the same sequence number. It checks the sequence numbers and enforces the check rather than just ignoring the sequence numbers.</p> <p>Disable this option if there is an error with the IPsec mechanism that results in out-of-order packets, preventing proper functionality.</p> <p>By default, Anti-Replay detection is enabled.</p>
Install interval	<p>Select the maximum number of seconds to allow for the installation of a re-keyed outbound security association (SA) on the device.</p>
Idle Time	<p>Select the appropriate idle time interval.</p> <p>The sessions and their corresponding translations typically time out after a certain period if no traffic is received.</p>
DF Bit	<p>Select an option to process the Don't Fragment (DF) bit in IP messages.</p> <ul style="list-style-type: none"> • Clear—Disable the DF bit from the IP messages. This is the default option. • Copy—Copy the DF bit to the IP messages. • Set—Enable the DF bit in the IP messages.

Table 206: View IKE/IPsec Settings (Continued)

Settings	Guidelines
Copy Outer DSCP	<p>Enable this option to allow copying of the Differentiated Services Code Point (DSCP) field from the outer IP header encrypted packet to the inner IP header plain text message on the decryption path.</p> <p>The benefit in enabling this feature is that after IPsec decryption, clear text packets can follow the inner class-of-service (CoS) rules.</p>
Lifetime Seconds	<p>Select a lifetime of an IKE security association (SA).</p> <p>The valid range is from 180 to 86400 seconds.</p>
Lifetime Kilobytes	<p>Select the lifetime in kilobytes of an IPsec security association (SA).</p> <p>The valid range is from 64 to 4294967294 kilobytes.</p>

Create a Remote Access VPN—Juniper Secure Connect

Juniper Secure Connect is Juniper Networks's client-based SSL-VPN solution that offers secure remote access for your network resources. Juniper Secure Connect downloads the configuration from SRX Services devices and chooses the most effective transport protocols during connection establishment.

Before You Begin

- Read the ["IPsec VPN Overview" on page 494](#) topic.
- Review the IPsec VPN main page for an understanding of your current data set. See ["IPsec VPN Main Page Fields" on page 499](#) for the field descriptions.
- Create addresses and address sets. See ["Create Addresses or Address Groups" on page 863](#) .
- Create VPN profiles. See ["Creating VPN Profiles" on page 576](#) .
- Define extranet devices. See ["Creating Extranet Devices" on page 587](#) .

1. Select **SRX > IPsec VPN > IPsec VPNs**.

The IPsec VPNs page opens.

2. Click **Create > Remote Access Juniper Secure Connect**.

The Create Remote Access VPN page opens.

3. Complete the IPsec VPN configuration parameters according to the guidelines provided in [Table 207 on page 558](#).

NOTE: Click **View IKE/IPsec Settings** to view or edit VPN profiles. If the VPN profile is default, you can edit the configurations. If the profile is shared, you can only view the configurations.

The VPN connectivity will change from gray to blue line in the topology to show that the configuration is complete. The topology displayed is only for representation.

4. Click **Save** to save the IPsec configuration.

Table 207: Create Remote Access VPN Page Settings

Settings	Guidelines
Name	<p>Enter a unique string of maximum 63 alphanumeric characters without spaces.</p> <p>The string can contain colons, periods, dashes, and underscores.</p>
Description	<p>Enter a description containing maximum 255 characters for the VPN.</p>
Routing Topology	<p>Select Traffic Selector (Auto Route Insertion).</p> <p>A traffic selector is an agreement between IKE peers to permit traffic through a tunnel if the traffic matches a specified pair of local and remote addresses.</p>
VPN Profile	<p>Select a VPN profile from the drop-down list based on the deployment scenario.</p> <ul style="list-style-type: none"> The Inline profile is applicable to a particular IPsec VPN only. You can view and edit the details by clicking View IKE/IPsec settings on the Create IPsec VPN page. The Shared profile can be used by one or more IPsec VPNs. You can only view the details of the shared profiles by clicking View IKE/IPsec settings on the Create IPsec VPN page.

Table 207: Create Remote Access VPN Page Settings (Continued)

Settings	Guidelines
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 based—Specifies that a pre-shared 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. • RSA Signatures—Specifies that a public key algorithm, which supports encryption and digital signatures is used.
Max Transmission Unit	<p>Select the maximum transmission unit (MTU) in bytes.</p> <p>MTU defines the maximum size of an IP packet, including the IPsec overhead. You can specify the MTU value for the tunnel endpoint. The valid range is 68 to 9192 bytes, and the default value is 1500 bytes.</p>
Pre-shared Key	<p>Establish a VPN connection using pre-shared keys, which is essentially a password that is same for both parties.</p> <p>Select the type of pre-shared key you want to use:</p> <ul style="list-style-type: none"> • Autogenerate—Select if you want to automatically generate a unique key per tunnel. When selected, the Generate Unique key per tunnel option is automatically enabled. If you disable the Generate Unique key per tunnel option, Juniper Security Director Cloud generates a single key for all tunnels. • Manual—Select to enter the key manually. By default, the manual key is masked. <p>Pre-shared keys are applicable only if the authentication method is pre-shared-based.</p>

Table 207: Create Remote Access VPN Page Settings (Continued)

Settings	Guidelines
Client Settings	<p>Modify the default client profile and define a local gateway.</p> <p>To modify the default client profile:</p> <ol style="list-style-type: none"> 1. Select the default profile in the Client Settings section. 2. Click the pencil icon. The Remote User page opens. 3. Configure the parameters as described in Table 208 on page 560. <p>To define a local gateway:</p> <ol style="list-style-type: none"> 1. Click the + sign in the Local Gateway section. The Add Device page opens. 2. Configure the device parameters as described in Table 209 on page 562. 3. Click OK.

Table 208: Remote User Page Settings

Settings	Guidelines
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 to 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>

Table 208: Remote User Page Settings (Continued)

Settings	Guidelines
SSL VPN	<p>Enable this option to establish SSL VPN connection from the Juniper Secure Connect Client to the SRX Series Firewall.</p> <p>This is a fallback option when IPsec ports are not reachable. By default, this option is enabled.</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 Windows Hello (fingerprint recognition, face recognition, PIN entry, and so on).</p> <p>Windows Hello must be preconfigured on the client system if the Biometric authentication option is enabled.</p>
Dead Peer Detection	<p>Enable this option to allow the Juniper Secure Connect client to detect if the SRX Series Firewall is reachable.</p> <p>Disable this option to allow the Juniper Secure Connect client to detect till the SRX Series Firewall connection reachability is restored.</p> <p>This option is enabled by default.</p>
DPD Mode	<p>Select a DPD Mode.</p> <ul style="list-style-type: none"> • Optimized: R-U-THERE messages are triggered if there is no incoming IKE or IPsec traffic within a configured interval after the device sends outgoing packets to the peer. This is the default mode. • Probe Idle Tunnel: R-U-THERE messages are triggered if there is no incoming or outgoing IKE or IPsec traffic within a configured interval. R-U-THERE messages are sent periodically to the peer until there is traffic activity. • Always-send: R-U-THERE messages are sent at configured intervals regardless of traffic activity between the peers.
DPD Interval	<p>Select an interval in seconds to send dead peer detection messages.</p> <p>The default interval is 10 seconds with a valid range of 2 to 60 seconds.</p>

Table 208: Remote User Page Settings (Continued)

Settings	Guidelines
DPD Threshold	<p>Select the failure DPD threshold value.</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 with a valid range of 1 to 5.</p>
Certificates	<p>The option to configure the security certificates.</p> <ul style="list-style-type: none"> • Expiry Warning—When enabled, you receive certificate expiration warning when the certificate is about to expire. This option is enabled by default. • Warning Interval—Enter the interval in days when you want the warning to be displayed. • Pin Req Per Connection—When enabled, you must enter the certificate PIN for every connection. This option is enabled by default.
EAP-TLS	<p>The option to use the EAP-TLS authentication method to validate the security certificates.</p> <p>This option is enabled by default.</p>
Window logon	<p>Enable this option to provide users to securely log on to the Windows domain before logging on to the Windows system.</p> <p>The client supports domain login using a credential service provider after establishing a VPN connection to the company network.</p>

Table 209: Add Device Page Settings

Settings	Guidelines
External Interface	<p>Select the outgoing interface for IKE security associations (SAs).</p> <p>This interface is associated with a zone that acts as its carrier, providing firewall security for it.</p>

Table 209: Add Device Page Settings (Continued)

Settings	Guidelines
Tunnel Zone	<p>Select the tunnel zone.</p> <p>Tunnel zones are logical areas of address space that can support dynamic IP (DIP) address pools for NAT applications to pre- and post-encapsulated IPsec traffic. Tunnel zones also provide flexibility in combining tunnel interfaces with VPN tunnels.</p>
User Authentication	<p>Select the authentication profile from the list that will be used to authenticate a user accessing the remote access VPN.</p> <p>Click Add to create a new access profile.</p> <p>NOTE: LDAP authentication is not supported in a remote VPN.</p>
SSL VPN Profile	<p>Select an SSL VPN profile from the list to terminate the remote access connection.</p> <p>To create a new SSL VPN profile:</p> <ol style="list-style-type: none"> 1. Click Add. <p style="padding-left: 20px;">The Add SSL VPN Profile page opens.</p> <ol style="list-style-type: none"> 2. Enter the SSL VPN profile name. 3. Enable Logging option to log SSL VPN events. 4. Enter a SSL termination profile name. 5. Select a server certificate. 6. Click OK.
Certificate	<p>Select a certificate to authenticate the virtual private network (VPN) initiator and recipient.</p>
Trusted CA/Group	<p>Select the CA profile from the list to associate it with the local certificate.</p> <p>This is applicable when authentication method is RSA-Signatures.</p>

Table 209: Add Device Page Settings (Continued)

Settings	Guidelines
Protected Networks	<p>Configure the addresses type for the selected device to protect one area of the network from the other.</p> <p>You can also create addresses by clicking Add New Address.</p>

Table 210: View IKE/IPsec Settings

Settings	Guidelines
IKE Settings	
IKE Version	<p>Select the required IKE version, either V1 or V2, that is used to negotiate dynamic security associations (SAs) for IPsec.</p> <p>By default, IKE V2 is used.</p>
Mode	<p>Select an IKE policy mode.</p> <ul style="list-style-type: none"> • Main—Uses 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. This mode also provides identity protection. • Aggressive—Takes half the number of messages of main mode, has less negotiation power, and does not provide identity protection. <p>Mode is applicable when the IKE Version is V1.</p>
Encryption Algorithm	Select the appropriate encryption mechanism.
Authentication Algorithm	<p>Select an algorithm.</p> <p>The device uses this algorithm to verify the authenticity and integrity of a packet.</p>
Diffie Hellman group	<p>Select a group.</p> <p>Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process.</p>

Table 210: View IKE/IPsec Settings (Continued)

Settings	Guidelines
Lifetime Seconds	<p>Select a lifetime of an IKE security association (SA).</p> <p>The valid range is from 180 to 86400 seconds.</p>
Dead Peer Detection	<p>Enable this option to permit the two gateways to determine if the peer gateway is up and responding to the Dead Peer Detection (DPD) messages that are negotiated during IPsec establishment.</p>
DPD Mode	<p>Select a DPD Mode.</p> <ul style="list-style-type: none"> • Optimized: R-U-THERE messages are triggered if there is no incoming IKE or IPsec traffic within a configured interval after the device sends outgoing packets to the peer. This is the default mode. • Probe Idle Tunnel: R-U-THERE messages are triggered if there is no incoming or outgoing IKE or IPsec traffic within a configured interval. R-U-THERE messages are sent periodically to the peer until there is traffic activity. • Always-send: R-U-THERE messages are sent at configured intervals regardless of traffic activity between the peers.
DPD Interval	<p>Select an interval in seconds to send dead peer detection messages.</p> <p>The default interval is 10 seconds with a valid range of 2 to 60 seconds.</p>
DPD Threshold	<p>Select the failure DPD threshold value.</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 with a valid range of 1 to 5.</p>
Advance Settings	
General IKE ID	<p>Enable this option to accept peer IKE ID</p> <p>This option is disabled by default. If General IKE ID is enabled, the IKE ID option is disabled automatically.</p>

Table 210: View IKE/IPsec Settings (Continued)

Settings	Guidelines
IKEv2 Re Authentication	<p>Select a reauthentication frequency. Reauthentication can be disabled by setting the reauthentication frequency to 0.</p> <p>The valid range is 0 to 100.</p>
IKEv2 Re Fragmentation Support	<p>Enable this option to split a large IKEv2 message into a set of smaller ones so that there is no fragmentation at the IP level.</p>
IKEv2 Re-fragment Size	<p>Select the size of the packet at which messages are fragmented. By default, the size is 576 bytes for IPv4.</p> <p>The valid range is 570 to 1320.</p>
IKE ID	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • None • Distinguished name • Hostname • IPv4 address • E-mail Address <p>IKE ID is applicable only when General IKE ID is disabled.</p>
NAT-T	<p>Enable Network Address Translation-Traversal (NAT-T) if the dynamic endpoint is behind a NAT device.</p>
Keep Alive	<p>Select a period in seconds to keep the connection alive.</p> <p>NAT Keepalives are required to maintain the NAT translation during the connection between the VPN peers.</p> <p>The valid range is from 1 to 300 seconds.</p>
IPsec Settings	

Table 210: View IKE/IPsec Settings (Continued)

Settings	Guidelines
Protocol	<p>Select the required protocol to establish the VPN.</p> <ul style="list-style-type: none"> • ESP—The Encapsulating Security Payload (ESP) protocol provides both encryption and authentication. • AH—The Authentication Header (AH) protocol provides data integrity and data authentication.
Encryption Algorithm	<p>Select the encryption method.</p> <p>This is applicable if the Protocol is ESP.</p>
Authentication Algorithm	<p>Select an algorithm.</p> <p>The device uses these algorithms to verify the authenticity and integrity of a packet.</p>
Perfect Forward Secrecy	<p>Select Perfect Forward Secrecy (PFS) as the method that the device uses to generate the encryption key.</p> <p>The PFS generates each new encryption key independently from the previous key. The higher numbered groups provide more security but require more processing time.</p>
Establish Tunnel	<p>Select an option to specify when IKE is activated.</p> <ul style="list-style-type: none"> • Immediately—IKE is activated immediately after VPN configuration changes are committed. • On-traffic—IKE is activated only when data traffic flows and must be negotiated with the peer gateway. This is the default behavior.
Advance Settings	
VPN Monitor	<p>Enable this option to send Internet Control Message Protocol (ICMP) to determine if the VPN is up.</p>

Table 210: View IKE/IPsec Settings (Continued)

Settings	Guidelines
Optimized	<p>Enable this option to optimize VPN monitoring and configure SRX Series Firewalls to send ICMP echo requests, also called pings, only when there is outgoing traffic and no incoming traffic from the configured peer through the VPN tunnel.</p> <p>If there is incoming traffic through the VPN tunnel, the SRX Series Firewalls considers the tunnel to be active and do not send pings to the peer.</p>
Anti Replay	<p>Enable this option for the IPsec mechanism to protect against a VPN attack that uses a sequence of numbers that are built into the IPsec packet.</p> <p>IPsec does not accept a packet for which it has already seen the same sequence number. It checks the sequence numbers and enforces the check rather than just ignoring the sequence numbers.</p> <p>Disable this option if there is an error with the IPsec mechanism that results in out-of-order packets, preventing proper functionality.</p> <p>By default, Anti-Replay detection is enabled.</p>
Install interval	<p>Select the maximum number of seconds to allow for the installation of a re-keyed outbound security association (SA) on the device.</p>
Idle Time	<p>Select the appropriate idle time interval.</p> <p>The sessions and their corresponding translations typically time out after a certain period if no traffic is received.</p>
DF Bit	<p>Select an option to process the Don't Fragment (DF) bit in IP messages.</p> <ul style="list-style-type: none"> • Clear—Disable the DF bit from the IP messages. This is the default option. • Copy—Copy the DF bit to the IP messages. • Set—Enable the DF bit in the IP messages.

Table 210: View IKE/IPsec Settings (Continued)

Settings	Guidelines
Copy Outer DSCP	<p>Enable this option to allow copying of the Differentiated Services Code Point (DSCP) field from the outer IP header encrypted packet to the inner IP header plain text message on the decryption path.</p> <p>The benefit in enabling this feature is that after IPsec decryption, clear text packets can follow the inner class-of-service (CoS) rules.</p>
Lifetime Seconds	<p>Select a lifetime of an IKE security association (SA).</p> <p>The valid range is from 180 to 86400 seconds.</p>
Lifetime Kilobytes	<p>Select the lifetime in kilobytes of an IPsec security association (SA).</p> <p>The valid range is from 64 to 4294967294 kilobytes.</p>

Importing IPsec VPNs

Juniper Security Director Cloud lets you import your existing large and complex VPN configurations into the portal. You do not have to recreate the same VPN environment to allow Juniper Security Director Cloud to manage it. During the VPN import operation, all VPN-related objects are also imported along with the VPN.

When you import a VPN, Juniper Security Director Cloud adds a new VPN to the VPN list with the name as ImportVPN_<number>.

At any point of the import workflow, you can choose to exit. All your settings and progress are discarded.

1. Select **SRX > IPsec VPN > IPsec VPNs**.

The IPsec VPNs page opens.

2. Click **Import**.

The Import VPNs page opens.

3. Select the devices to import the VPNs.

You can select one or more devices from which the VPN configuration must be imported. The filter option enables you to perform a free-text search on the device name.

Ensure that you select all the devices, otherwise the network topology discovery might vary and the import of the VPN configuration might treat other devices as extranet devices.

NOTE: Hover your mouse cursor over **Supported/unsupported items**. The displayed list gives you an idea about the VPN types and settings that Juniper Security Director Cloud supports, along with the settings that are not supported. Juniper Security Director Cloud displays the other settings that it does not support, but you can modify the features only using CLI.

4. Click **Next**.

The list of VPNs to be imported is displayed.

5. Click **Finish**.

A Job Status page opens displaying the details of the Import VPN job, such as the number of VPNs, the number of devices in each VPN, and the time stamp.

6. Click **OK**.

The imported VPNs are displayed on the IPsec VPN page and the corresponding VPN profiles are listed on the VPN Profiles page.

Deploy an IPsec VPN

1. Select **SRX > IPsec VPN > IPsec VPNs**.

The IPsec VPNs page opens.

2. Select the VPN policy, and click **Deploy**.

The Deploy VPN page opens.

3. Select one of the following:

- **Schedule at a later time** to schedule and to publish the configuration later.
- **Run now** to apply the configuration immediately.

4. Click **Update**.

The Affected Devices page displays the devices where the policies will be published.

Modify IPsec VPN Settings

IN THIS SECTION

- [Modify Device Selection | 571](#)

1. Select **SRX > IPsec VPN > IPsec VPNs**.

The IPsec VPNs page is displayed.

2. Select the IPsec VPN, and click the pencil icon.

Based on the VPN topology, the corresponding edit IPsec VPN page opens.

3. Edit the required fields, and click **OK**.

Follow the applicable configuration guidelines used while creating the IPsec VPN. You can also edit the tunnel settings on the device configuration page by clicking **View/Edit Tunnels**.

Modify Device Selection

1. Select **SRX > IPsec VPN > IPsec VPNs**.

The IPsec VPNs page opens.

2. Select an IPsec VPN, and click the pencil icon.

The Modify IPsec VPN page opens.

3. Click **View/Select Devices**.

4. Edit the device selection.

5. Click **OK**.

Delete an IPsec VPN

IN THIS SECTION

- [Delete an IPsec VPN | 572](#)
- [Delete Hub-and-Spoke IPsec VPNs from Specific Devices | 573](#)

Delete an IPsec VPN

Delete an IPsec VPN by first marking it for deletion, then redeploying the VPN to finally delete it completely. When you delete the IPsec VPN, the VPN configurations are also deleted from the associated devices.

You can delete the following types of VPNs using this method:

- Site-to-site VPN
- Hub-and-Spoke (Establishment by All Peers) VPN
- Hub-and-Spoke (Establishment by Spokes) VPN
- Hub-and-Spoke Auto Discovery VPN
- Remote Access VPN—Juniper Secure Connect

You can also revert the IPsec VPN marked for deletion.

1. Select SRX > IPsec VPN > IPsec VPNs.

The **IPsec VPN** page opens.

2. Select an IPsec VPN to delete, and click the delete icon.

A message indicating the following result is displayed:

- The IPsec VPN will be deleted after you redeploy the VPN.
- The IPsec VPN configuration will also be deleted from the associated devices.

3. Click Yes.

NOTE:

- The IPsec VPN is not deleted from the associated devices at this moment. You must redeploy the IPsec VPN to delete it from the devices.
- You cannot edit the IPsec VPN that is marked to be deleted.

You can revert the IPsec VPN deletion. Hover your mouse cursor over the flag in the Status column, and select **Undo Delete** on the pop-up window. The IPsec VPN status is reverted to the previous status.

The IPsec VPN is marked for deletion, and the status changes to **VPN flagged to be deleted**.

4. Select the IPsec VPN, and click Deploy.

The Deploy page opens.

5. Click OK.

- An IPsec VPN deletion job is created. Click the job ID to go to the Jobs page and view the status of the delete operation.
- After a successful deployment, the selected IPsec VPN is deleted from Juniper Security Director Cloud and all associated devices.

Delete Hub-and-Spoke IPsec VPNs from Specific Devices

In a hub-and-spoke IPsec VPN that has multiple spoke and extranet devices, you can delete the VPN from specific spokes by deleting the spokes and redeploying the VPNs. However, when you delete a spoke that is an extranet device, the device configuration is deleted only from the VPN hub because Juniper Security Director Cloud does not manage the device.

You can delete the IPsec VPN configurations from specific spokes associated with the following types of VPNs using this method:

- Hub-and-Spoke (Establishment by All Peers) VPN
- Hub-and-Spoke (Establishment by Spokes) VPN
- Hub-and-Spoke Auto Discovery VPN

NOTE: You must retain at least one spoke in the hub-and-spoke IPsec VPN without which you won't be able to save the edited VPN.

1. Select SRX > IPsec VPN > IPsec VPNs.

The **IPsec VPN** page opens.

2. Select the IPsec VPN to delete the spokes, and click the pencil icon.

The Edit IPsec VPN page opens.

3. Select the spokes to delete in the Devices section, and click the delete icon.

A message asking for confirmation is displayed.

4. Click **Yes.**

5. Click **Save.**

A message indicating the following result is displayed:

- The deleted spokes will be removed from the IPsec VPN after you redeploy the VPN.
- The IPsec VPN configuration will also be deleted from the deleted devices.

6. Click **Yes.**

NOTE:

- The IPsec VPN configuration is not yet deleted from the spokes and hub. You must deploy the VPN to delete the VPN from the spokes.
- You can revert the changes by editing the IPsec VPN and adding the devices back.

The IPsec VPN status column displays the number of deleted spokes. Hover your mouse cursor over the device count link to view the list of deleted spokes.

7. Select the IPsec VPN, and click **Deploy.**

The Deploy page opens.

8. Click **OK.**

- An IPsec VPN deletion job is created. Click the job ID to go to the Jobs page and view the status of the delete operation.
- After a successful deployment, the selected IPsec VPN is deleted from the deleted spokes. If a deleted spoke is an extranet device, the device configuration is deleted only from the VPN hub because Juniper Security Director Cloud does not manage the device.

IPsec VPN-VPN Profiles

IN THIS CHAPTER

- [VPN Profiles Overview | 575](#)
- [VPN Profiles Main Page Fields | 576](#)
- [Creating VPN Profiles | 576](#)
- [Edit and Clone IPsec VPN profiles | 584](#)
- [Assigning Policies and Profiles to Domains | 585](#)

VPN Profiles Overview

You can use a VPN Profile Wizard to create an object that specifies the VPN proposals, mode of the VPN, and other parameters used in a route-based IPsec VPN. You can also configure the Phase 1 and Phase 2 settings in a VPN profile.

When a VPN profile is created, Juniper Security Director Cloud creates an object in the database to represent the VPN profile. You can use this object to create route-based IPsec VPN.

NOTE: You cannot modify or delete Juniper Networks defined VPN profiles. You can only clone the profiles and create new profiles.

SRX Series Firewalls support preshared key and PKI certificate-based authentication methods in IKE negotiation for IPsec VPNs. The RSA certificate and DSA certificate-based authentication are supported for IKE negotiation. The predefined VPN profile is available with both RSA and DSA certificates-based authentication. The PKI certificate list from the device is automatically retrieved during the device discovery and update-based syslog notifications.

VPN Profiles Main Page Fields

Use the VPN profiles main page to get an overall, high-level view of your VPN settings. You can filter and sort this information to get a better understanding of what you want to configure. [Table 211 on page 576](#) describes the fields on this page.

Table 211: VPN Profiles Main Page Fields

Field	Description
Name	The name of the VPN profile.
Description	The description of the VPN profile.
Type	A VPN profile type can be predefined or custom. Juniper Security Director Cloud comes with predefined proposal sets for both Phase 1 and Phase 2 IKE negotiations. You can use these predefined sets or create your own.
Mode	The Phase1 IKE negotiation mode (main or aggressive) is used to determine the type and number of message exchanges that occur in a phase. Only one mode is used for negotiation, and the same mode must be configured on both sides of the tunnel.
VPN Topology	The types of deployment topologies for IPsec VPN, such as site-to-site, hub-and-spoke, and remote access VPNs.
IPsec VPNs	The IPsec VPNs involved in the VPN profile.
Created By	The user who created the VPN profile.

Creating VPN Profiles

Configure VPN profiles that define security parameters when establishing a VPN connection. You can reuse the same profile to create more VPN tunnels. The VPN profile includes VPN proposals, VPN mode, authentication, and other parameters used in IPsec VPN. When a VPN profile is created, Juniper

Security Director Cloud creates an object in the database to represent the VPN profile. You can use this object to create either route-based or policy-based IPsec VPNs.

NOTE: You cannot modify or delete Juniper Networks-defined VPN profiles. You can only clone the profiles and create new profiles.

You can also configure the IKE negotiation phases known as Phase 1 and Phase 2 settings in a VPN profile. SRX Series Firewalls support the following authentication methods in IKE negotiations for IPsec VPN:

- Preshared key
- ECDSA certificate
- RSA certificate
- DSA certificate

The predefined VPN profile is available for RSA certificates-based authentication. The PKI certificate list from the device is automatically retrieved during the device discovery.

Before You Begin

- Review the VPN profiles main page for an understanding of your current data set. See "[VPN Profiles Main Page Fields](#)" on page 576 for the field descriptions.
- Read the "[VPN Profiles Overview](#)" on page 575 topic.

1. Select **SRX > IPsec VPNs > VPN Profiles.**

The VPN Profiles page opens.

2. Click **Create to create a new VPN profile, and select one of the following options:**

- **Policy Based Site to Site**
- **Site to Site**
- **Hub and Spoke (Establishment All Peers)**
- **Hub and Spoke (Establishment by Spokes)**
- **Hub and Spoke (ADVPN - Auto Discovery VPN)**
- **Remote Access Juniper Secure Connect**

3. Complete the configuration according to the guidelines provided in [Table 212 on page 578](#) .

A new VPN profile with the predefined VPN configuration is created. You can use this object to create IPsec VPNs.

Table 212: VPN Profiles Settings

Setting	Guideline
Name	<p>Enter a unique string of maximum 255 alphanumeric characters without spaces.</p> <p>The string can contain colons, periods, dashes, and underscores.</p>
Description	Enter a description containing maximum 1024 character for the VPN profile.
Authentication Type	<p>Select the required authentication type:</p> <ul style="list-style-type: none"> • Pre-shared based • RSA-Signatures • DSA-Signatures • ECDSA-Signatures-256 • ECDSA-Signatures-384
IKE Version	<p>Select the required IKE version, either V1 or V2, that is used to negotiate dynamic security associations (SAs) for IPsec. By default, IKEv1 is used.</p> <p>In Juniper Security Director Cloud, IKEv2 message fragmentation allows IKEv2 to operate in environments where IP fragments might be blocked and peers would not be able to establish an IPsec security association (SA). IKEv2 fragmentation splits a large IKEv2 message into a set of smaller ones so that there is no fragmentation at the IP level.</p>
Mode	<p>Select a VPN mode:</p> <ul style="list-style-type: none"> • Main—The most common and secure way to establish a VPN when building site-to-site VPNs. The IKE identities are encrypted and cannot be determined by eavesdroppers. • Aggressive—This is an alternative to main mode IPsec negotiation. This is the most common mode when building VPNs from client workstations to VPN gateways, where the IP address of the client is neither known in advance nor fixed.
Encryption Algorithm	Select the appropriate encryption mechanism.

Table 212: VPN Profiles Settings (Continued)

Setting	Guideline
Authentication Algorithm	Select an algorithm. The device uses this algorithm to verify the authenticity and integrity of a packet.
Diffie Hellman Group	Select a group. Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process.
Lifetime Seconds	Select a lifetime of an IKE security association (SA). The valid range is from 180 through 86400 seconds.
Dead Peer Detection	Enable this option to permit the two gateways to determine if the peer gateway is up and responding to the Dead Peer Detection (DPD) messages that are negotiated during IPsec establishment.
DPD Mode	Select a DPD Mode. <ul style="list-style-type: none"> • Optimized: R-U-THERE messages are triggered if there is no incoming IKE or IPsec traffic within a configured interval after the device sends outgoing packets to the peer. This is the default mode. • Probe Idle Tunnel: R-U-THERE messages are triggered if there is no incoming or outgoing IKE or IPsec traffic within a configured interval. R-U-THERE messages are sent periodically to the peer until there is traffic activity. • Always-send: R-U-THERE messages are sent at configured intervals regardless of traffic activity between the peers.
DPD Interval	Select an interval in seconds to send dead peer detection messages. The default interval is 10 seconds with a valid range of 2 to 60 seconds.
DPD Threshold	Select the failure DPD threshold value. 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 with a valid range of 1 to 5.

Table 212: VPN Profiles Settings (Continued)

Setting	Guideline
Advance Settings	
General-IkeID	<p>Enable this option to accept peer IKE ID in general.</p> <p>This option is disabled by default. If General IKE ID is enabled, the IKE ID option is disabled automatically.</p> <ul style="list-style-type: none"> • This option is not available in Aggressive VPN mode. • You cannot use a VPN profile with the General IKE ID option enabled for the Auto VPN and ADVPN.
IKEv2 Re Authentication	<p>Select a reauthentication frequency. Reauthentication can be disabled by setting the reauthentication frequency to 0.</p> <p>The valid range is 0 to 100.</p>
IKEv2 Re Fragmentation Support	<p>Enable this option to split a large IKEv2 message into a set of smaller ones so that there is no fragmentation at the IP level.</p>
IKEv2 Re-fragment Size	<p>Select the size of the packet at which messages are fragmented.</p> <p>By default, the size is 576 bytes for IPv4, and the valid range is 570 to 1320.</p>

Table 212: VPN Profiles Settings (Continued)

Setting	Guideline
IKE Id	<p>Configure the following IKE identifiers:</p> <ul style="list-style-type: none"> • Hostname—The hostname or FQDN is a string that identifies the end system. • User@hostname—A simple string that follows the same format as an e-mail address. User—Enter the e-mail address of the user. We recommend that you use a valid e-mail address of the user for ease of management. • IPAddress—This is the most common form of IKE identity for site-to-site VPNs. This can be either an IPv4 or IPv6 address. This option is available only if the VPN mode is Aggressive and the authentication type is Preshared Key. • DN—The distinguished name used in certificates to identify a unique user in a certificate. This option is available only for RSA, DSA, and ECDSA signature authentication types. <p>NOTE:</p> <ul style="list-style-type: none"> • For the Preshared Key authentication type: <ul style="list-style-type: none"> • If you have enabled the General IKE ID option, the IKE ID option is automatically set to None and you cannot edit this option. • When modifying an IPsec VPN, you cannot edit the IKE ID column in the View/Edit Tunnel page, if you have chosen a VPN profile with the General IKE ID option enabled. • For the certificate-based authentication type: <ul style="list-style-type: none"> • You can edit the IKE ID option even if you have enabled the General IKE ID option because, the <code>local-identity</code> CLI is used for certificate authentication. • When modifying an IPsec VPN, you can edit the IKE ID column in the View/Edit Tunnel page, if you have chosen a VPN profile with the General IKE ID option enabled.
NAT-T	<p>Enable Network Address Translation-Traversal (NAT-T) if the dynamic endpoint is behind a NAT device.</p>

Table 212: VPN Profiles Settings (Continued)

Setting	Guideline
Keep Alive	<p>Select a period in seconds to keep the connection alive.</p> <p>NAT Keepalives are required to maintain the NAT translation during the connection between the VPN peers. The valid range is from 1 to 300 seconds.</p>
IPsec Settings	
Protocol	<p>Select the required protocol to establish the VPN.</p> <ul style="list-style-type: none"> • ESP—The Encapsulating Security Payload (ESP) protocol provides both encryption and authentication. • AH—The Authentication Header (AH) protocol provides data integrity and data authentication.
Encryption Algorithm	<p>Select the necessary encryption method.</p> <p>This is applicable if the Protocol is ESP.</p>
Authentication Algorithm	<p>Select an algorithm.</p> <p>The device uses these algorithms to verify the authenticity and integrity of a packet.</p>
Perfect Forward Secrecy	<p>Select Perfect Forward Secrecy (PFS) as the method that the device uses to generate the encryption key.</p> <p>The PFS generates each new encryption key independently from the previous key. The higher numbered groups provide more security but require more processing time.</p>
Establish Tunnel	<p>Select an option to specify when IKE is activated.</p> <ul style="list-style-type: none"> • Immediately—IKE is activated immediately after VPN configuration changes are committed. • On-traffic—IKE is activated only when data traffic flows and must be negotiated with the peer gateway. This is the default behavior.
Advance Settings	

Table 212: VPN Profiles Settings (*Continued*)

Setting	Guideline
VPN Monitor	Enable this option to send Internet Control Message Protocol (ICMP) to determine if the VPN is up.
Optimized	<p>Enable this option to optimize VPN monitoring and configure SRX Series Firewalls to send ICMP echo requests, also called pings, only when there is outgoing traffic and no incoming traffic from the configured peer through the VPN tunnel.</p> <p>If there is incoming traffic through the VPN tunnel, the SRX Series Firewalls considers the tunnel to be active and do not send pings to the peer.</p>
Anti Replay	<p>Enable this option for the IPsec mechanism to protect against a VPN attack that uses a sequence of numbers that are built into the IPsec packet.</p> <p>IPsec does not accept a packet for which it has already seen the same sequence number. It checks the sequence numbers and enforces the check rather than just ignoring the sequence numbers.</p> <p>Disable this option if there is an error with the IPsec mechanism that results in out-of-order packets, preventing proper functionality.</p> <p>By default, Anti-Replay detection is enabled.</p>
Install interval	Select the maximum number of seconds to allow for the installation of a re-keyed outbound security association (SA) on the device.
Idle Time	<p>Select the appropriate idle time interval.</p> <p>The sessions and their corresponding translations typically time out after a certain period if no traffic is received.</p>
DF Bit	<p>Select an option to process the Don't Fragment (DF) bit in IP messages.</p> <ul style="list-style-type: none"> • Clear—Disable the DF bit from the IP messages. This is the default option. • Copy—Copy the DF bit to the IP messages. • Set—Enable the DF bit in the IP messages.

Table 212: VPN Profiles Settings (Continued)

Setting	Guideline
Copy Outer DSCP	<p>Enable this option to allow copying of the Differentiated Services Code Point (DSCP) field from the outer IP header encrypted packet to the inner IP header plain text message on the decryption path.</p> <p>The benefit in enabling this feature is that after IPsec decryption, clear text packets can follow the inner class-of-service (CoS) rules.</p>
Lifetime Seconds	<p>Select a lifetime of an IKE security association (SA).</p> <p>The valid range is from 180 through 86400 seconds.</p>
Lifetime Kilobytes	<p>Select the lifetime in kilobytes of an IPsec security association (SA).</p> <p>The valid range is from 64 through 4294967294 kilobytes.</p>

Edit and Clone IPsec VPN profiles

IN THIS SECTION

- [Edit a VPN Profile | 584](#)
- [Clone IPsec VPN Profile | 585](#)

You can edit or clone a custom IPsec VPN profile. When you edit or clone a VPN profile migrated from an earlier release, you need to select a VPN topology for the VPN profile.

NOTE: You cannot modify or delete Juniper Networks Predefined VPN profiles. You can only clone the profiles and create new profiles.

Edit a VPN Profile

1. Select **SRX > IPsec VPNs > VPN Profiles**.

The VPN Profiles page opens.

2. Select the IPsec VPN to edit, and click the pencil icon.

NOTE: Select a VPN topology while creating an IPsec VPN. When you edit a VPN profile migrated from an earlier release, you'll need to select a VPN topology for the VPN profile.

The edit window opens showing the same options as when creating a new VPN profile.

3. Click **Save** to save your changes.

Clone IPsec VPN Profile

1. Select **SRX > IPsec VPNs > VPN Profiles**.

The VPN Profiles page opens.

2. Right-click the VPN Profile to clone, and select **Clone**.

You can also select Clone from the More list.

The Clone window opens with editable fields.

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

Assigning Policies and Profiles to Domains

You can assign or reassign policies or profiles to different domains when it is first configured and whenever you want to implement a change.

You can assign only one policy or profile at a time. Before assigning a policy or profile to another domain, Juniper Security Director Cloud checks for the validity of the move. If the move is not acceptable, a warning message appears.

1. Select the landing page for the type of policy or profile to assign to a domain.
2. From the landing page, click **More**.

A list of actions opens.

3. Select **Assign <Policy or Profile> to Domain**.

The Assign <Policy or Profile> to Domain page opens.

NOTE: <Policy or Profile> is the name of the policy or profile that you are assigning to a domain.

4. Select the required items to assign to a domain.

5. Enable this option to ignore warning messages.
6. Click **Assign**.
A policy or profile is assigned to a domain.

IPsec VPN-Extranet Devices

IN THIS CHAPTER

- [Creating Extranet Devices | 587](#)
- [Extranet Devices Main Page Fields | 588](#)
- [Find Usage for Extranet Devices | 589](#)

Creating Extranet Devices

Use the Extranet devices page to manage the third-party devices that Juniper Security Director Cloud does not directly control or manage.

Extranet devices can be ScreenOS devices or other vendor VPN-capable firewall devices that cannot be managed by Juniper Security Director Cloud. Extranet devices in the Juniper Security Director Cloud help users design and manage VPNs residing between SRX Series Firewalls and third-party devices without actually being connected to them.

To configure extranet devices:

Before You Begin

Review the Extranet Devices main page for an understanding of your current data set. See "[Extranet Devices Main Page Fields](#)" on [page 588](#) for the field descriptions

1. Select **Security Subscriptions > VPNs > Extranet Devices**.

The Extranet Devices page opens.

2. Click the plus sign to create a new extranet device.

Complete the configuration according to the guidelines provided in [Table 213 on page 588](#).

Table 213: Create Extranet Device Page Settings

Setting	Guideline
Name	Enter a name containing maximum 63 characters that begins with an alphanumeric character The name can include colons, periods, slashes, and underscores.
Description	Enter a description containing maximum 1024 characters.
IP Address	Enter the IPv4 address for the extranet device.
Hostname	Enter a DNS resolvable name containing maximum 64 characters. The hostname can include alphanumeric characters, dashes, and underscores. This hostname is used to generate an IKE ID.
Created	Displays the name of the user who created the extranet device.

3. Click **OK** to save.

Your changes are saved, a new extranet device is added to Juniper Security Director Cloud.

Extranet Devices Main Page Fields

Use extranet device objects to reference third-party devices that you do not have login or other device controls over. Extranet devices are firewalls that Juniper Security Director Cloud does not directly control and manage.

Table 214: Extranet Devices Main Page Fields

Field	Description
Name	The name of the extranet device.
Description	The description of the extranet device.

Table 214: Extranet Devices Main Page Fields (Continued)

Field	Description
Hostname	The DNS resolvable name of the extranet device. This hostname is used to generate IKE ID.
IP Address	The IPv4 address of the device.
Created By	The user who created the extranet device.
Domain Name	The user domain for mapping objects and managing sections of a network.

Find Usage for Extranet Devices

In Juniper Security Director Cloud, you can find the usage of extranet devices in IPsec VPNs.

1. Select **Security Subscriptions > VPNs > Extranet Devices**.

The Extranet Devices page opens.

2. Right-click an extranet device, and select **Find Usage**.

The Search Results page opens with the IPsec VPN names where the extranet device is used.

If the extranet device is not used by any VPN, the search result will not display any IPsec VPNs.

NAT-NAT Policies

IN THIS CHAPTER

- [NAT Policies Overview | 590](#)
- [About the NAT Policies Page | 594](#)
- [Create a NAT Policy | 595](#)
- [Edit and Delete a NAT Policy | 596](#)
- [About the NAT Policy Rules Page | 599](#)
- [Create a NAT Policy Rule | 601](#)
- [Edit, Clone, and Delete a NAT Policy Rule | 608](#)
- [Common Operations on a NAT Policy Rule | 609](#)
- [Deploy a NAT Policy | 611](#)

NAT Policies Overview

Network Address Translation (NAT) is a form of network masquerading where you can hide devices or sites between zones or interfaces. A trusted zone is a segment of a network on which security measures are applied. It is usually assigned to the internal LAN. An example of an untrusted zone is the internet. NAT modifies the IP addresses of the packets moving between the trusted and untrusted zones.

Whenever a packet exits a NAT device (when traversing from the internal LAN to the external WAN), the device performs a translation on the packet's IP address. The packet's IP address is rewritten with an IP address that was specified for external use. After translation, the packet appears to have originated from the gateway rather than from the original device within the network. This process hides your internal IP addresses from the other networks and keeps your network secure.

Using NAT also enables you to use more internal IP addresses. As these IP addresses are hidden, there is no risk of conflict with an IP address from a different network. This helps you conserve IP addresses.

Juniper Security Director Cloud supports configuring three types of NAT on the SRX Series Firewalls:

- **Source NAT**—Translates the source IP address of a packet leaving a trust zone (outbound traffic). It translates the traffic originating from the device in the trust zone. The source IP address of the traffic

(which is a private IP address), is translated to a public IP address that can be accessed by the destination device specified in the NAT rule. The destination IP address is not translated.

The following uses cases show the support for source NAT translation between IPv6 and IPv4 address domains:

- Translation from one IPv6 subnet to another IPv6 subnet without Network Address Port Translation (NAPT), also known as Port Address Translation (PAT).
- Translation from IPv4 addresses to IPv6 prefixes along with IPv4 address translation.
- Translation from IPv6 hosts to IPv6 hosts with or without NAPT.
- Translation from IPv6 hosts to IPv4 hosts with or without NAPT.
- Translation from IPv4 hosts to IPv6 hosts with or without NAPT.
- Destination NAT—Translates the destination IP address of a packet. Using destination NAT, an external device can send packets to a hidden internal device. As an example, consider the case of a webserver behind a NAT device. Traffic to the WAN-facing public IP address (the destination IP address) is translated to the internal webserver private IP address.

The following uses cases show the support for destination NAT translation between IPv6 and IPv4 address domains:

- Mapping of one IPv6 subnet to another IPv6 subnet
- Mapping between one IPv6 host and another IPv6 host
- Mapping of one IPv6 host (and optional port number) to another special IPv6 host (and optional port number)
- Mapping of one IPv6 host (and optional port number) to another special IPv4 host (and optional port number)
- Mapping of one IPv4 host (and optional port number) to another special IPv6 host (and optional port number)
- Static NAT—Always translates a private IP address to the same public IP address. It translates traffic from both sides of the network (both source and destination). For example, a web-server with a private IP address can access the Internet using a static, one-to-one address translation. In this case, outgoing traffic from the web-server undergoes source NAT translation, and incoming traffic to the web-server undergoes destination NAT translation.

The following uses cases show the support for static NAT translation between IPv6 and IPv4 address domains:

- Mapping of one IPv6 subnet to another IPv6 subnet.

- Mapping between one IPv6 host and another IPv6 host.
- Mapping between IPv4 address *a.b.c.d* and IPv6 address *Prefix::a.b.c.d*.
- Mapping between IPv4 hosts and IPv6 hosts.
- Mapping between IPv6 hosts and IPv4 hosts.

Juniper Security Director Cloud also supports configuring persistent NAT where address translations are maintained in the database for a configurable amount of time after a session ends.

[Table 215 on page 592](#) shows the persistent NAT support for different source NAT and destination NAT addresses.

Table 215: Persistent NAT Support

Source NAT Address	Translated Address	Destination NAT Address	Persistent NAT Support
IPv4	IPv6	IPv4	No
IPv4	IPv6	IPv6	No
IPv6	IPv4	IPv4	Yes
IPv6	IPv6	IPv6	No

[Table 216 on page 592](#) and [Table 217 on page 593](#) show the translated address pool selection for source NAT, destination NAT, and static NAT addresses.

Table 216: Translated Address Pool Selection for Source NAT

Source NAT Address	Destination Address	Pool Address
IPv4	IPv4	IPv4
IPv4	IPv6 - Subnet must be greater than 96	IPv6

Table 216: Translated Address Pool Selection for Source NAT (Continued)

Source NAT Address	Destination Address	Pool Address
IPv6	IPv4	IPv4
IPv6	IPv6	IPv6

Table 217: Translated Address Pool Selection for Destination NAT and Static NAT

Source NAT Address	Destination Address	Pool Address
IPv4	IPv4	IPv4 or IPv6
IPv4	IPv6 - Subnet must be greater than 96	IPv4 or IPv6
IPv6	IPv4	IPv4
IPv6	IPv6	IPv4 or IPv6

NOTE:

- For source NAT, the proxy Neighbor Discovery Protocol (NDP) is available for NAT pool addresses. For the destination NAT and the static NAT, the proxy NDP is available for destination NAT addresses.
- A NAT pool can have a single IPv6 subnet or multiple IPv6 hosts.
- You cannot configure the overflow pool if the address type is IPv6.
- NAT pools permit the address entries of only one version type: IPv4 or IPv6.

About the NAT Policies Page

IN THIS SECTION

- [Tasks You Can Perform | 594](#)
- [Field Descriptions | 594](#)

To access this page, select **SRX > NAT > NAT Policies**.

Use the **NAT Policies** page to create, modify, clone, and delete NAT policies and policy rules. You can filter and sort this information to get a better understanding of what you want to configure.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a NAT policy. See ["Create a NAT Policy" on page 595](#) .
- Modify or delete a NAT policy. See ["Edit and Delete a NAT Policy" on page 596](#) .
- Create, modify, and delete NAT policy rules. See ["About the NAT Policy Rules Page" on page 599](#) .
- Search for a specific NAT policy. Click the Search icon in the top right corner of the page to search for a NAT policy.

You can enter partial text or full text of the keyword in the text box and press Enter.

The search results are displayed on the same page.

- Show or hide columns. Click the **Show Hide Columns** icon in the top right corner of the page.

Field Descriptions

[Table 218 on page 595](#) provides guidelines on using the fields on the **NAT Policies** page.

Table 218: Fields on the NAT Policies Page

Field	Description
Seq.	Order number for the NAT policy.
Name	Displays the name of the NAT policy.
Rules	Number of rules assigned to the NAT policy.
Devices	Device on which the NAT policy will be deployed.
Status	Deployment status for the NAT policy.
Modified By	The user who modified the policy.
Last Modified	The date and time when the policy was modified.
Description	Description of the NAT policy.

Create a NAT Policy

Use the Create NAT Policy page to create NAT policies.

To create a NAT policy:

1. Select **SRX > NAT > NAT Policies**.
The **NAT Policies** page appears.
2. Click the add icon (+).
The **Create NAT Policy** page displays fields required for creating and configuring a NAT policy.
3. Complete the configuration according to the guidelines provided in [Table 219 on page 596](#).
4. Click **OK** to save the changes.
A NAT policy with the configuration you provided is created.

Table 219: Fields on the Create NAT Policy Page

Field	Description
Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 255 characters.
Description	Enter a description for the policy; the maximum length is 255 characters.
Manage Auto-Proxy ARP	Click the toggle button to respond to incoming Address Resolution Protocol (ARP) requests. ARP translates IPv4 addresses to MAC addresses.
Select Devices	Select the device on which you want to apply the policy in the Available column and move them to the Selected column by clicking the greater-than icon (>). NOTE: The Available column lists only those devices that do not have a NAT policy associated with them.
Sequence No.	Click Change Sequence Number . The Select Policy Sequence page appears, displaying all NAT policies. Select the policy you want to reorder and select Move Policy Up or Move Policy Down to reorder your NAT policy among the existing policies.

Edit and Delete a NAT Policy

IN THIS SECTION

- [Edit a NAT Policy | 597](#)
- [Delete a NAT Policy | 597](#)
- [Delete a NAT Policy from Unassigned Devices | 598](#)

You can edit or delete a NAT policy from the **NAT Policies** page.

Edit a NAT Policy

To modify the parameters configured for a NAT Policy:

1. Select **SRX > NAT > NAT Policies**.

The **NAT Policies** page appears.

2. Select the NAT policy you want to edit, and then click on the edit icon (pencil symbol).

The **Edit NAT Policy** page appears, showing the same fields as those seen when you create a new NAT policy.

3. Modify the parameters according to the guidelines provided in ["Create a NAT Policy" on page 595](#) .
4. Click **OK** to save the changes.

The modified NAT policy is displayed in the **NAT Policies** page.

Delete a NAT Policy

You can mark a NAT policy for deletion and delete the policy from the device. You can also revert the policy marked for deletion.

NOTE: When the NAT policy is deleted, the NAT rules associated with the policy are deleted from device.

To delete a NAT policy:

1. Select **SRX > NAT > NAT Policies**.

The **NAT Policies** page opens.

2. Select the NAT policy that you want to delete and then click the delete icon.

A message requesting confirmation for the deletion appears.

3. Click **Yes** to delete the selected NAT policy.

The policy is marked for deletion and the status changes to "NAT flagged to be deleted".

NOTE:

- The policy NAT is not deleted from the device at this moment. You must deploy the policy to delete it from the devices.

- You cannot edit the NAT policy that is marked to be deleted. However, you can edit the rules for the policy. After you edit the rules, the policy status is changed to **Redeploy required**. See ["Edit, Clone, and Delete a NAT Policy Rule" on page 608](#) .

4. Optional: To revert the delete operation, hover over the flag icon in the status column and select **Undo Delete** from the pop-up.

The NAT policy reverts to the previous status.

5. Select the NAT policy and click **Deploy**.

The Deploy page opens.

6. Click **OK**.

- A policy deletion job is created. Click the job ID to go to the Jobs page and view the status of the delete operation.
- After a successful deployment, the selected NAT policy is deleted.

Delete a NAT Policy from Unassigned Devices

If multiple devices are assigned to a NAT policy, you can unassign the devices and re-deploy the NAT policy to delete the policy from the unassigned devices.

NOTE: When you delete a NAT policy, the rules associated with the NAT policy are deleted from device.

1. Select **SRX > NAT > NAT Policies**.

The **NAT Policies** page appears.

2. Select the NAT policy for which you want to unassign the devices, and then click the pencil icon.

The Edit NAT Policy page appears displaying the same options that you entered while creating the NAT policy.

3. Select the devices from the Selected column and click the left-arrow to move the devices to the Available column.

4. Click **OK**.

A message appears requesting confirmation for the deletion of the policy for the unselected devices.

5. Click **Yes**.

The NAT policy status column displays the number of unassigned devices of unassigned devices. Hover over the device count link to view the list of unassigned devices.

NOTE:

- The NAT policy is not deleted from the unassigned devices at this moment. You must deploy the policy to delete it from the unassigned devices.
- You can revert the changes by editing the NAT policy and assigning the devices again to the security policy.

6. Select the NAT policy and click **Deploy**.

The Deploy page opens.

7. Click **OK**.

- A policy deletion job is created. Click the job ID to go to the Jobs page and view the status of the delete operation.
- After a successful deployment, the selected NAT policy is deleted from the assigned devices.

About the NAT Policy Rules Page

IN THIS SECTION

- [Tasks You Can Perform | 599](#)
- [Field Descriptions | 600](#)

To access this page, select **SRX > NAT > NAT Policies**. The **NAT Policies** page appears displaying all existing NAT policies. Click on a NAT policy to view the rules associated with it.

The NAT policy rules page displays the NAT rules associated with the NAT policy and keep track of the number and order of rules for each policy. You can also create a new NAT rule, modify the configured parameters of existing NAT rules, clone, and delete NAT rules, using this page.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a NAT rule. See ["Create a NAT Policy Rule" on page 601](#) .
- Update the sequence of the NAT rules using the up and down arrows that appear when you hover over the NAT rule.
- Modify, clone, and delete NAT rules. See ["Edit, Clone, and Delete a NAT Policy Rule" on page 608](#) .

- Search for a specific NAT rule. Click the Search icon in the top right corner of the page to search for a NAT rule.
- Show or hide columns. Click the **Show Hide Columns** icon in the top right corner of the page.

Field Descriptions

Table 220 on page 600 provides information on the fields in the NAT rules contained within this NAT policy.

Table 220: Fields on the NAT Policy Rules Page

Field	Description
Seq.	Order number for the NAT policy.
Rule Name	NAT policy rule name.
Type	Type of the NAT rule such as source, destination, or static.
Sources	Displays the source endpoints on which the NAT policy applies. A source endpoint can be zone, interface, routing instance, zone, addresses or ports.
Destinations	Displays the destination endpoints on which the NAT policy applies. A destination endpoint can be zone, interface, routing instance, zone, addresses or ports.
Services/Protocols	Services and protocols to permit or deny for the source and destination type NAT rules.
Translation	Displays the translation type applied on the incoming or outgoing traffic.

The **Total Rules** field on the top right corner of the page displays the total number of rules associated with the NAT policy. The **Deploy pending** field displays the deploy status of the rules associated with the NAT policy.

Create a NAT Policy Rule

NAT processing centers on the evaluation of NAT rule sets and rules. A rule set determines the overall direction of the traffic to be processed. After a rule set matches the traffic, each rule in the rule set is evaluated for a match. NAT rules can match on the following packet information:

- Source and destination address
- Source port (for source and static NAT only)
- Destination port

The first rule in the rule set that matches the traffic is used. If a packet matches a rule in a rule set during session establishment, traffic is processed according to the action specified by that rule.

To create NAT rule, click the NAT policy name. The NAT policy rules page appears, providing you with options to configure NAT rules. Alternately, you can click on the rule number listed under **Rules** against the policy, to create a rule. You can configure the following types of NAT rules:

- **Static**—To add a static NAT rule, click **Create** on the top right corner and select **Static**.
- **Source**—To add a source NAT rule, click **Create** on the top right corner and select **Source**.
- **Destination**—To add a destination NAT rule, click **Create** on the top right corner and select **Destination**.

Depending on the type of rule you have chosen, some fields in the rule will not be applicable. In addition to defining rules between zones and interfaces, you can define NAT rules with virtual routers defined on the device.

To create a NAT policy rule:

1. Select **SRX > NAT > NAT Policies**.

The **NAT Policies** page appears that shows the existing NAT policies.

2. Click the name of the NAT policy for which you want to create rules. Alternately, you can click **Add Rule** link against a NAT policy.

The NAT policy rules page appears.

3. Click **Create** and select either **Source**, **Static**, or **Destination**. The page displays fields for creating a NAT rule.
4. Complete the configuration according to the guidelines provided in [Table 221 on page 602](#).
5. Click **OK** to save the changes.

A NAT rule with the configuration you provided is created.

[Table 221 on page 602](#) provides guidelines on using the fields on the **NAT Policies** page.

Table 221: Fields on the NAT Policies Page for Creating NAT Rules

Field	Description
Rule Name	Enter a unique string beginning with a number or letter and consisting of letters, numbers, dashes and underscores. The maximum length is 31 characters.
Description	Enter a description for the policy rule that must be a string excluding '&', '<', '>' and '\n'. The maximum length is 900 characters.
Sources	Click the add icon (+) to select the source endpoints on which the NAT policy rule applies, from the displayed list of Source Ingress Type, Source zones, Source addresses, Source port/port range.
Source Ingress Type	<p>a. Select an ingress type: Zone, Interface, or Routing Instance.</p> <p>b. From the appropriate selector, select the zones, interfaces, or routing instance that you want to associate the rule to, from the Available column.</p> <p>NOTE: For the Routing Instance option, you can select one or more of the available virtual routers on the device. For the group NAT policy, you will see a consolidated list of all virtual routers on all devices that the policy is assigned to.</p> <p>c. Click OK.</p>

Table 221: Fields on the NAT Policies Page for Creating NAT Rules (*Continued*)

Field	Description
Source Addresses	<p>Enter one or more address names or address set names.</p> <ul style="list-style-type: none"> • Any—Add any address to the NAT rule. • Specific—Select the check box beside each address you want to include in the address group. Click the greater-than icon (>) to move the selected address or addresses from the Available column to the Selected column. Note that you can use the fields at the top of each column to search for addresses. .
Source Ports/Port Range	<p>Enter a maximum of eight ports and port ranges separated by commas.</p>
Destinations	<p>Click the add icon (+) to select the destination endpoints on which the NAT policy rule applies, from the displayed list of Destination Ingress Type, Destination zones, Destination addresses, Destination ports/port range.</p> <p>NOTE: When you create a destination NAT rule for traffic arriving on an interface that terminates a VPN link, the translation process might break the VPN link. This will happen if the destination address in a destination NAT rule is specified only as the WAN-facing IP address of that interface. For example, in the following NAT rule, any traffic destined to WAN IP will get translated to the destination pool and will break functionality of the VPN link packets terminating on this interface.</p> <pre>[Any.Address] --> [Wan.IP] :: [Dest-Pool-1]</pre> <p>Therefore, the recommendation in such cases is to use a destination NAT rule with destination field as [Address + Port]. For example:</p> <pre>[Any.Address] --> [Wan.IP + Port] :: [Dest-Pool-1]</pre>

Table 221: Fields on the NAT Policies Page for Creating NAT Rules *(Continued)*

Field	Description
Destination Addresses	<p>Enter one or more address names or address set names.</p> <ul style="list-style-type: none"> • Any—Add any address to the NAT rule. • Specific—Select the check box beside each address you want to include in the address group. Click the greater-than icon (>) to move the selected address or addresses from the Available column to the Selected column. Note that you can use the fields at the top of each column to search for addresses. .
Destination Ports/Port Range	<p>Enter a maximum of eight ports and port ranges separated by commas.</p>
Service/Protocols	<p>Choose one among the following for a NAT rule:</p> <ul style="list-style-type: none"> • None—Select this option if you do not want to set any service or protocols in source or destination NAT. • Services—Select one or more services from the Available list to permit or deny traffic. • Protocols—Select the protocols from the Available list to permit or deny traffic.

Table 221: Fields on the NAT Policies Page for Creating NAT Rules *(Continued)*

Field	Description
Translation	<p>Specify the translation type for the incoming traffic. The translation options vary based on whether you are creating a source, static, or destination NAT rule.</p> <p>Chose one among the following translation types for a source NAT rule:</p> <ul style="list-style-type: none"> • None—No translation is required for the incoming traffic. • Interface—Performs interface-based translations on the source or the destination packet. • Pool—Performs pool-based translations on the source or the destination packet. Click on the add icon (+) in the Select Pool field to choose the translation pool. <p>You can also create a new pool by clicking Add new pool. See "Create a NAT Pool" on page 613 .</p> <p>Chose one among the following translation types for a static NAT rule:</p> <ul style="list-style-type: none"> • Address—Performs address-based translations on the source or the destination packet. Click on the add icon (+) in the Select Address field to choose the translation address. • Corresponding IPv4—Uses the corresponding IPv4 address to perform translations on the source or the destination packet. <p>Chose one among the following translation types for a destination NAT rule:</p> <ul style="list-style-type: none"> • None—Translation is not required for the incoming traffic. • Pool—Performs pool-based translations on the source or the destination packet. Click on the add

Table 221: Fields on the NAT Policies Page for Creating NAT Rules *(Continued)*

Field	Description
	<p>icon (+) in the Select Pool field to choose the translation pool.</p> <p>You can also create a new pool by clicking Add new pool. See "Create a NAT Pool" on page 613 .</p>

Table 222 on page 606 provides guidelines on using the fields on the **Advanced Settings** page for a source NAT rule.

Table 222: Fields on the Advanced Settings Page for Source NAT Rule

Field	Description
Persistent	<p>Click the toggle button to ensure that all requests from the same internal transport address are mapped to the same reflexive transport address.</p> <p>NOTE: For persistence to be applicable for the NAT policy, ensure that port overloading is turned off for the device to which the NAT policy is applicable. Use the following command to turn off port overloading for a device:</p> <pre>[Edit mode] set security nat source interface port-overloading off</pre>

Table 222: Fields on the Advanced Settings Page for Source NAT Rule *(Continued)*

Field	Description
Persistent NAT Type	<p>Configure persistent NAT mappings.</p> <ul style="list-style-type: none"> • Permit any remote host— Any external host can send a packet to the internal host by sending the packet to the reflexive transport address. • Permit target host—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. • Permit target host port—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.
Inactivity Timeout	<p>The amount of time, in seconds, that the persistent NAT binding remains in the site's memory when all the sessions of the binding entry have ended. When the configured timeout occurs, the binding is removed from memory. The value of the inactivity timeout can range from 60 through 7200 seconds. The default value of the inactivity timeout is 60 seconds.</p>
Maximum Session Number	<p>Maximum session number—The maximum number of sessions with which a persistent NAT binding can be associated. For example, if the maximum session number of the persistent NAT rule is 65,536, then a 65,537th session cannot be established if that session uses the persistent NAT binding created from the persistent NAT rule.</p> <p>The range is 8 through 65,536. The default is 30 sessions.</p>
Address Mapping	<p>Click the toggle button to enable or disable the address mapping.</p>

Table 223 on page 608 provides guidelines on using the fields on the **Advanced Settings** page for a static NAT rule.

Table 223: Fields on the Advanced Settings Page for Static NAT Rule

Field	Description
Mapped Port Type	Specify the type of port mapping: <ul style="list-style-type: none"> • Port—Enter a value for Port, ranging from 0 through 65,535. • Range—Enter the port range values in the Start and End fields, ranging from 0 through 65,535.
Routing Instance	Select the routing instance for the static NAT rule.

Edit, Clone, and Delete a NAT Policy Rule

IN THIS SECTION

- [Edit a NAT Policy Rule | 608](#)
- [Clone a NAT Policy Rule | 609](#)
- [Delete a NAT Policy Rule | 609](#)

You can edit, clone, or delete a NAT policy rule from the *NAT Policy* page.

Edit a NAT Policy Rule

To modify the parameters configured for an NAT policy rule:

1. Select **SRX > NAT > NAT Policies**.

The **NAT Policies** page appears, displaying the NAT policies.

2. Click the NAT policy for which you want to edit the NAT policy rules.

The selected *NAT Policy* appears, displaying the rules associated with the NAT policy.

3. Click the pencil icon that appears on the right side of the rule.

The NAT Policy page displays the same options as those that appear when you create a new NAT policy rule.

4. Modify the parameters following the guidelines provided in ["Create a NAT Policy Rule" on page 601](#).
5. Click **OK** to save the changes.

The modified NAT policy rule appears on the *NAT Policy* page.

Clone a NAT Policy Rule

To clone a NAT policy rule:

1. Select **SRX > NAT > NAT Policies**.

The **NAT Policies** page appears, displaying the NAT policies.

2. Click the NAT policy for which you want to clone the NAT policy rules.

The selected *NAT Policy* appears, displaying the rules associated with the NAT policy.

3. Right-click and select **Clone**.

The NAT Policy page displays the same options as those that appear when you create a new NAT policy rule. Update the cloned rule as required.

4. Click **Save** to save the changes.

The modified rule appears on the NAT Policy page

Delete a NAT Policy Rule

To delete a NAT policy rule:

1. Select **SRX > NAT > NAT Policies**.

The **NAT Policies** page appears, displaying the NAT policies.

2. Select the NAT policy whose rule you want to delete.

The selected *NAT Policy* appears, displaying the rules associated with the NAT policy.

3. Hover over the NAT policy rule you want to delete and then click the delete icon (**X**).

An alert message appears, verifying that you want to delete your selection.

4. Click **Yes** to delete the selection.

The selected NAT policy rule is deleted.

Common Operations on a NAT Policy Rule

You can perform common operations on a NAT policy rule from the *NAT Policy* page.

To perform common operations on a NAT policy rule:

1. Select **SRX > NAT > NAT Policies**.

The **NAT Policies** page appears, displaying the NAT policies.

2. Click the NAT policy rule and click **More**.

The dropdown menu shows common operations for a NAT rule.

3. Complete the configuration according to the guidelines provided in the following table.

Table 224: Common Operatons on NAT Policy Rules Page

Field	Description
Add Rule Before	Add a rule before an existing rule.
Add Rule After	Add a rule after an existing rule.
Copy	Copy an existing rule to paste at different order.
Cut	Cut an existing rule to paste at different order.
Paste	Before —Paste the rule before an existing rule. After —Paste the rule after and existing rule.
Clone	Create a copy of an existing rule.
Enable	Enable the rule.
Disable	Disable the rule.
Move	Move the rule by selecting one of the following options: <ul style="list-style-type: none"> • Move Top • Move Up • Move Down • Move Bottom

Table 224: Common Operatons on NAT Policy Rules Page *(Continued)*

Field	Description
Clear All Selections	Clear the sections for the rules.

Deploy a NAT Policy

After adding the rules to the NAT policies, you can deploy the NAT policy by clicking the **Deploy** option that is above the **End Points** panel. You can also deploy one or more policies from the **NAT Policies** page.

To deploy NAT policies:

1. Select **SRX > NAT > NAT Pools**.

The NAT Policies page appears.

2. Select one or more policies and click **Deploy**.

The Deploy page appears.

3. In **Deployment Time** options, select **Run Now** to deploy the policy immediately. Select **Schedule at a later time** and specify the date and time at which the policy should be deployed.

4. Click **OK**.

A job is created. Click the job ID to go to the Jobs page and view the status of the deploy operation.

NAT-NAT Pools

IN THIS CHAPTER

- [NAT Pools Overview | 612](#)
- [About the NAT Pools Page | 612](#)
- [Create a NAT Pool | 613](#)
- [Edit, Clone, and Delete a NAT Pool | 617](#)

NAT Pools Overview

A NAT pool is a set of IP addresses that you can define and use for address translation. NAT policies perform address translation by translating internal IP addresses to the addresses in these pools. Unlike static NAT, where there is a one-to-one mapping that includes destination IP address translation in one direction and source IP address translation in the reverse direction, with source NAT, you translate the original source IP address to an IP address in the address pool. With destination NAT, you translate the original destination address to an IP address in the address pool.

About the NAT Pools Page

IN THIS SECTION

- [Tasks You Can Perform | 613](#)

To access this page, select **SRX > NAT > NAT Pools**.

Use the **NAT Pools** page to create, modify, clone, and delete NAT pools. You can filter and sort this information to get a better understanding of what you want to configure.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a NAT pool. See ["Create a NAT Pool" on page 613](#) .
- Modify, clone, or delete a NAT pool. See ["Edit, Clone, and Delete a NAT Pool" on page 617](#) .
- View the details of a NAT pool by selecting **More > Detailed View**, or by right-clicking a NAT pool and select **Detailed View**.
- Search for a specific NAT pool. Click the Search icon in the top right corner of the page to search for a NAT pool. You can enter partial text or full text of the keyword in the text box and press Enter.

The search results are displayed on the same page.

- Show or hide columns. Click the **Show Hide Columns** icon at the top right corner of the page.

[Table 225 on page 613](#) provides description of the fields on the **NAT Pools** page.

Table 225: Fields on the NAT Pools Page

Field	Description
Name	Displays the name of the NAT pool.
Pool Type	Displays the NAT pool type. A NAT pool can be of type Source or Destination .
Pool Address	Displays the IP address of the NAT pool.
Description	Displays the description provided about the NAT pool when it was created.

Create a NAT Pool

Use the **Create NAT Pool** page to create NAT pools.

To create a NAT pool:

1. Select **SRX > NAT > NAT Pools**.

The **NAT Pools** page appears.

- Click the add icon (+).

The **Create NAT Pool**

- Complete the configuration according to the guidelines provided in [Table 226 on page 614](#).
- Click **OK** to save the changes. A NAT pool is available with the configuration you provided.

[Table 226 on page 614](#) provides guidelines on using the fields on the **Create NAT Pool** page.

Table 226: Fields on the Create NAT Pool Page

Field	Description
General Information	
Name	Enter a unique string of alphanumeric characters, dashes, spaces, and underscores. Colons and periods are not allowed. The maximum length is 31 characters.
Description	Enter a description string excluding '&', '<', '>' and '\n' characters. The maximum length is 900 characters.
Pool Type	Select a NAT pool type to configure: <ul style="list-style-type: none"> • Source • Destination
Pool Address	Select a NAT pool address or click Add new address to create a NAT pool address.
Routing Instance	
Devices	Select the devices to which the NAT pool is applicable.
Routing Instance	Select the required routing instance from the list of available routing instances for the selected device.

Table 226: Fields on the Create NAT Pool Page (*Continued*)

Field	Description
Port	Enter the destination port number that is used for port forwarding. The value of the port can be any value between 1024 to 65535.
Advanced	
Pool Translation	<p>Select the translation type for the incoming traffic:</p> <ul style="list-style-type: none"> • No Translation—No translation required for the incoming traffic. • Port/Range—Set the global default single port range for source NAT pools with port translation. • Overload—Multiple source addresses are translated to pool addresses. If you set Overload as the translation type, the value of the Pool Address field cannot be an IP range or subnet, but it will be a single address.
Host Address Base	Enter the base address of the original source IP address range. The Host Address Base is used for IP address shifting.
Address Pooling	<p>Select a NAT address pooling behavior:</p> <ul style="list-style-type: none"> • Paired—Use this option for applications that require all sessions associated with one internal IP address to be translated to the same external IP address for multiple sessions. • Non-Paired—Use this option for applications that can be assigned IP addresses in a round-robin fashion.

Table 226: Fields on the Create NAT Pool Page (*Continued*)

Field	Description
Port overloading factor	Enter the port overloading capacity in source NAT. The value can be any value between 2 to 32. If the port-overloading-factor is set to x, each translated IP address will have x number of ports available.
Address Sharing	Enable address sharing so that multiple internal IP addresses can be mapped to the same external IP address. Select this option only when the source NAT pool is configured with no port translation. When a source NAT pool has only one or a few external IP addresses available, the address sharing option with a many-to-one address mapping increases NAT resources and improves traffic.
Port	Enter the port number for the NAT pools. The value of the port can be any value between 1024 to 65535.
Start	Enter the start port value for the source NAT pools. The value of the port range can be any value between 1024 to 65535.
End	Enter the end port value for the source NAT pools. The value of the port range can be any value between 1024 to 65535.

Table 226: Fields on the Create NAT Pool Page (*Continued*)

Field	Description
Overflow Pool Type	<p>Select a source pool to use when the current address pool is exhausted.</p> <ul style="list-style-type: none"> • Interface—Allow the egress interface IP address to support overflow. • Pool—Name of the source address pool. • Overflow Pool—When addresses from the original source NAT pool are exhausted, IP addresses and port numbers are allocated from the overflow pool. A user-defined source NAT pool or an egress interface can be used as the overflow pool. When the overflow pool is used, the pool ID is returned with the address.

Edit, Clone, and Delete a NAT Pool

IN THIS SECTION

- [Edit a NAT Pool | 617](#)
- [Clone a NAT Pool | 618](#)
- [Delete a NAT Pool | 618](#)

Edit a NAT Pool

To modify the parameters configured for a NAT pool:

1. Select **SRX > NAT > NAT Pools**.

The **NAT Pools** page appears.

2. Select the NAT pool that you want to edit, and click the edit icon (pencil symbol).

The **Edit NAT Pool** page appears, displaying the same options that are displayed when creating a new NAT pool.

3. Modify the parameters according to the guidelines provided in ["Create a NAT Pool" on page 613](#) .
4. Click **OK** to save the changes.

Clone a NAT Pool

To clone a NAT pool:

1. Select **SRX > NAT > NAT Pools**.

The **NAT Pools** page appears.

2. Right-click the NAT pool that you want to clone and then click **Clone**, or select **More > Clone**.

The **Clone NAT Pool** page appears with editable fields. Modify the parameters of the cloned NAT pool as per your requirements.

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

The cloned NAT pool appears at the end of the NAT pools list in the **NAT Pools** page.

Delete a NAT Pool

To delete a NAT pool:

1. Select **SRX > NAT > NAT Pools**.

The **NAT Pools** page appears.

2. Select the NAT pool you want to delete and then click the delete icon.

An alert message appears, verifying that you want to delete the NAT pool.

3. Click **Yes** to delete the NAT pool.

Identity-JIMS

IN THIS CHAPTER

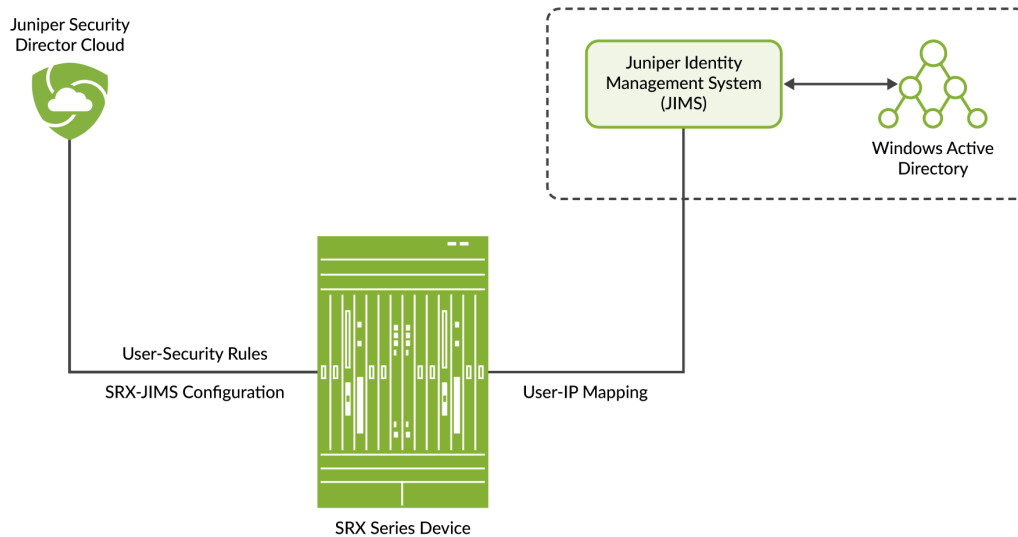
- [Juniper Identity Management Service Overview | 619](#)
- [About the Identity Management Profile Page | 621](#)
- [Create Identity Management Profiles | 622](#)
- [Edit, Clone, and Delete Identity Management Profiles | 625](#)
- [Deploy the Identity Management Profile to SRX Series Firewalls | 627](#)

Juniper Identity Management Service Overview

Juniper Identity Management Service (JIMS) is a standalone Windows service application that collects and maintains a large database of user, device, and group information from Active Directory domains. JIMS collects advanced user identities from different authentication sources for SRX Series Firewalls. JIMS enables the device to rapidly identify thousands of users in a large, distributed enterprise.

Juniper Security Director Cloud is used to push the JIMS configuration to SRX Series Firewalls. You can create an identity management profile in Juniper Security Director Cloud and deploy the identity management profile to SRX Series Firewalls. Based on the deployed identity management profile, the SRX Series Firewalls query the JIMS server to obtain required information.

Figure 17: Juniper Security Director Cloud, SRX, and JIMS Connectivity



SRX Series Firewalls communicate with JIMS through HTTP or HTTPS connection. Use HTTP connection for debugging and HTTPS for deployments. SRX Series Firewalls consist of primary and secondary JIMS configurations. These devices must always query the primary JIMS. The secondary JIMS is available as a fall back option with limited resources. You must use the secondary JIMS when the HTTP GET query or number of queries to the primary JIMS fails. SRX Series Firewalls constantly scrutinize the failed primary JIMS and revert to the primary JIMS, once it is up and running.

NOTE:

- Juniper Security Director Cloud does not directly communicate with JIMS server. SRX Series Firewalls query the JIMS server to obtain the user identity information. For more information about different query modes, see [Understanding Advanced Query Feature for Obtaining User Identity Information from JIMS](#) and [Configuring Advanced Query Feature for Obtaining User Identity Information from JIMS](#).
- SRX firewall authentication can also push the authentication entries to JIMS.
- IP and user mapping information might be inaccurate, if the user identities in JIMS are cleared, delayed, or missing.

About the Identity Management Profile Page

IN THIS SECTION

- [Tasks You Can Perform](#) | 621
- [Field Descriptions](#) | 621

To access this page, click **SRX > Identity > JIMS**.

Use the Identity Management Profile page to obtain advanced user identity from different authentication sources for SRX Series Firewalls.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create the identity management profile. See "[Create Identity Management Profiles](#)" on page 622 .
- Edit, clone, and delete an existing identity management profile. See "[Edit, Clone, and Delete Identity Management Profiles](#)" on page 625 .
- Deploy the identity management profile. See "[Deploy the Identity Management Profile to SRX Series Firewalls](#)" on page 627 .

Field Descriptions

[Table 227 on page 621](#) provides guidelines on using the fields on the Identity Management Profile page.

Table 227: Fields on the Identity Management Profile Page

Field	Description
Name	Specifies the name of the identity management profile.
Description	Specifies the description for the identity management profile.
Primary JIMS Server	Specifies the IP address of the primary Juniper Identity Management System (JIMS) server.

Table 227: Fields on the Identity Management Profile Page *(Continued)*

Field	Description
Devices	Specifies the name of a SRX Series Firewall.

Create Identity Management Profiles

Use the Create Identity Management Profile page to create a JIMS profile and to obtain user identities.

To create an identity management profile:

1. Select **SRX > Identity > JIMS**.

The Identity Management Profile page appears.

2. Click the + sign.

The Create Identity Management Profile page appears.

3. Complete the configuration by using the guidelines in [Table 228 on page 622](#).

4. Click **OK**.

Table 228: Fields on the Create Identity Management Profile Page

Field	Description
General	
Name	Enter a unique string that begins with alphanumeric characters. You can use colons, periods, dashes, and underscores. The maximum length is 62 characters.
Description	Enter a description for the identity management profile. The maximum length is 255 characters.
Primary JIMS server	Enter a valid IPv4 address of the primary JIMS server. SRX Series Firewalls always query the primary JIMS to obtain the user identities.

Table 228: Fields on the Create Identity Management Profile Page (*Continued*)

Field	Description
Primary CA certificate path	<p>Enter the certificate path of the primary JIMS server. The SRX Series Firewall uses this certificate to verify the certificate of the JIMS server for the SSL connection that is used for the user query function. For example: '/var/tmp/RADIUSServerCertificate.crt'</p> <p>When SRX Series Firewall does not receive the information from JIMS through the Web API POST requests, user query enables the SRX Series Firewall to query JIMS for authentication and identity information for an individual user.</p>
Secondary Identity	Enable this option to use the secondary JIMS server as a fallback when the primary JIMS server fails. By default, this option is disabled.
Secondary JIMS server	<p>Enter a valid IPv4 address of the secondary JIMS server.</p> <p>The secondary JIMS is available as a fall back option with limited resources. Use the secondary JIMS when the <i>HTTP GET</i> or number of queries to the primary JIMS fails.</p>
Secondary JIMS certificate path	Enter the certificate path of the secondary JIMS server. The SRX Series Firewall uses this certificate to verify the JIMS server certificate for the SSL connection, used for the user query function.

Assign Devices—Add Devices

Device Name	Select the SRX Series Firewall from the list for JIMS to send the report on user identities.
Client ID	Enter the client ID that the SRX Series Firewall requires to obtain an access token for the JIMS user query function. The client ID must be consistent with the API client configured on JIMS.
Secret Key	Enter the client secret used with the client ID that the SRX Series Firewall requires to obtain an access token. The client secret must be consistent with the API client configured on JIMS.

NOTE: If you delete the assigned device, the JIMS profile configuration is removed from the device. If you add any new device the JIMS profile configuration is assigned to the new device.

Connection Settings

Table 228: Fields on the Create Identity Management Profile Page (Continued)

Field	Description
Connection Type	<p>Select the application protocol from the list to connect the SRX Series Firewall to JIMS for user query request. You identify the connection protocol along with the configuration that identifies JIMS. The user query function allows the SRX Series Firewall to request user authentication and identity information for an individual user from JIMS.</p> <ul style="list-style-type: none"> • HTTP—Protocol that JIMS uses to connect to the SRX Series Firewall. • HTTPS—Secure version of the protocol that JIMS uses to connect to the SRX Series Firewall. <p>If you do not select the connection type, HTTPS is used by default.</p>
Port	<p>Select the connection port of the JIMS server, from the list. Default port number is 443. The range is 1 to 65535.</p>
Token API	<p>Enter the token API used to generate the URL to acquire an access token. The token API is combined with the connection method and the IP address of JIMS to produce the complete URL used to acquire an access token.</p> <p>For example, if the token API is <i>oauth</i>, the connection method is HTTPS, and the IP address of JIMS is 192.0.2.199, the complete URL to acquire an access token would be https://192.0.2.199/api/oauth.</p> <p>The default token API is oauth_token/oauth.</p>
Query API	<p>Enter the query API to specify the path of the URL that the SRX Series Firewall uses to query JIMS for an individual user. For the SRX Series Firewall to be able to make a request, you must have configured the query API to obtain an access token.</p> <p>The SRX Series Firewall generates the complete URL for the user query request by combining the query API string with the connection method (HTTP/HTTPS) and the JIMS IP address.</p> <p>The default token API is user_query/v2.</p>
Advanced	
Maximum items per batch	<p>Enter the value for maximum number of reports to include in the JIMS response.</p> <p>Range: 100 through 1000.</p>

Table 228: Fields on the Create Identity Management Profile Page (*Continued*)

Field	Description
Query interval	<p>Enter the time interval, in seconds, for SRX Series Firewalls to periodically query JIMS for the newly generated user identities.</p> <p>Range: 1 through 60 seconds.</p>
Query delay time	<p>Enter the time in seconds for the SRX Series Firewall to delay before sending the individual IP queries to JIMS for authentication and identity information for individual users.</p> <p>After the delay timeout expires, the SRX Series Firewall performs the following actions:</p> <ul style="list-style-type: none"> • Sends the query to JIMS. • Creates a pending entry for the user in the Routing Engine authentication table. <p>Range: 1 through 60 seconds</p>
Invalid timeout	<p>Enter the timeout interval (in minutes) after which, the idle entries in the JIMS authentication table expire. The timeout interval begins from when the user authentication entry is added to the authentication table. This value can be between 10 and 1440 minutes, where a value of 0 means no timeout.</p>
IP query	<p>Click the toggle button to disable the IP address query function that is enabled by default.</p>
Filter for domain	<p>The SRX Series Firewall sends a query to JIMS for the user identity information within the specified domains. Enter a comma-separated list of up to 25 domain names. A domain name can be an alphanumeric string of up to 64 characters that can also contain dashes, underscores, and dots.</p> <p>Example: example.net</p>

Edit, Clone, and Delete Identity Management Profiles

IN THIS SECTION

- [Edit Identity Management Profiles | 626](#)

- [Clone Identity Management Profiles | 626](#)
- [Delete Identity Management Profiles | 627](#)

You can edit, clone, and delete the identity management profiles from the Identity Management Profiles page. You can clone an identity management profile to easily create an identity management profile. You can delete the unused identity management profiles.

Edit Identity Management Profiles

To edit an identity management profile:

1. Select **SRX > Identity > JIMS**.

The Identity Management Profile page appears.

2. Select the identity management profile that you want to edit, and click the pencil icon.

The Edit Identity Management Profile page appears, showing the same fields that are displayed when you create an identity management profile.

3. Edit the identity management profile fields as needed.

The changes are saved and you are returned to the Identity Management Profile page.

Clone Identity Management Profiles

To clone an identity management profile:

1. Select **SRX > Identity > JIMS**.

The Identity Management Profile page appears.

2. Select the identity management profile that you want to clone, and select **Clone** from the More list or right-click menu.

The Clone Identity Management Profile page appears, showing the same fields for creating an identity management profile.

3. Modify the identity management profile fields as needed.

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

The cloned identity management profile is created and you are returned to the Identity Management Profile page.

Delete Identity Management Profiles

NOTE: If you delete an identity management profile, it is deleted from the assigned devices as well.

To delete one or more identity management profiles:

1. Select **SRX > Identity > JIMS**.

The Identity Management Profile page appears.

2. Select the identity management profile that you want to delete, and click the **Delete**.

A warning dialog box appears asking you to confirm the deletion.

3. Click **Yes** to delete the selected identity management profiles.

The identity management profiles are deleted and you are returned to the Identity Management Profile page.

Deploy the Identity Management Profile to SRX Series Firewalls

To deploy the identity management profiles to SRX Series Firewalls:

1. Select **SRX > Identity > JIMS**.

The Identity Management Profile page appears.

2. Select the identity management profile that you want to deploy, and click **Deploy**.

The deploy status message page appears showing the link for job IDs.

3. Click the job ID to see the deploy status.

4. (Optional) Select **Administration > Jobs** and click the job name link to see the deploy status.

RELATED DOCUMENTATION

[About the Identity Management Profile Page | 621](#)

[Create Identity Management Profiles | 622](#)

[Edit, Clone, and Delete Identity Management Profiles | 625](#)

Identity-Active Directory

IN THIS CHAPTER

- [About the Active Directory Profile Page | 628](#)
- [Create an Active Directory Profile | 629](#)
- [Deploy an Active Directory Profile to SRX Series Firewalls | 634](#)
- [Edit, Clone, and Delete an Active Directory Profile | 635](#)

About the Active Directory Profile Page

IN THIS SECTION

- [Tasks You can Perform | 628](#)
- [Field Descriptions | 629](#)

Active Directory configuration is used by the SRX Series Firewalls to contact the Active Directory server. Active Directory enables you to configure the IP address-to-user mapping information and the user-to-group mapping information to access the LDAP server. You can view, create, modify, clone, and delete Active Directory profile. You can deploy Active Directory profiles on one or more SRX Series Firewalls.

To access this page, click **SRX > Identity > Active Directory**.

Tasks You can Perform

You can perform the following tasks from this page:

- Create an Active Directory profile. See ["Create an Active Directory Profile" on page 629](#) .
- Modify or delete an existing Active Directory profile. See ["Edit, Clone, and Delete an Active Directory Profile" on page 635](#) .

- Deploy the Active Directory profile to SRX Series Firewalls. See "[Deploy an Active Directory Profile to SRX Series Firewalls](#)" on page 634 .

Field Descriptions

[Table 229 on page 629](#) provides guidelines on using the fields on the Active Directory page.

Table 229: Fields on the Active Directory Profile Page

Field	Description
Name	Specifies the name of the Active Directory.
Active Directory Domains	Specifies the domain for which the status is displayed. Example: Global
Devices	Lists the assigned devices for a directory. Example: SRX
Description	Describes the Active Directory.

RELATED DOCUMENTATION

| [Integrated User Firewall Overview](#)

Create an Active Directory Profile

Use the Create Active Directory Profile page to configure the IP address-to-user mapping information and the user-to-group mapping information to access the LDAP server.

To create an Active Directory profile:

1. Select **SRX > Identity > Active Directory**.
The Active Directory Profile page appears.
2. Click the + icon.
3. Complete the configuration by using the guidelines in [Table 230 on page 630](#) .

4. Click **OK**.

A Summary page providing a preview of the complete configuration appears.

Table 230: Fields on the Create Active Directory Profile Page

Field	Description
<i>General Information</i>	
Name	<p>Enter a unique string of alphanumeric characters including:</p> <ul style="list-style-type: none"> • Colons • Periods • Dashes • Underscores <p>The maximum length is 62 characters.</p>
Description	<p>Enter a description for the Active Directory profile. The maximum length is 255 characters.</p>
<i>Add Domain Settings</i>	
General	
Domain Name	<p>Enter the name of the domain. The maximum length is 64 characters. The SRX Series Firewall can have the integrated user firewall configured in a maximum of two domains.</p> <p>Example: example.net</p>
Description	<p>Enter a description for the LDAP server domain. The maximum length is 255 characters.</p>
Domain Controller	

Table 230: Fields on the Create Active Directory Profile Page (*Continued*)

Field	Description
Username	<p>Enter the Active Directory account name. The range is 1 through 64 characters.</p> <p>Example: administrator</p>
Password	<p>Enter the password of the Active Directory account. The range is 1 through 128 characters.</p> <p>Example: \$ABC123</p>
Domain Controller	<p>Click the plus sign to create new domain controllers.</p> <ul style="list-style-type: none"> • Domain Controller Name— Enter the name that can range from 1 through 64 characters. You can configure a maximum of 10 domain controllers. • Address—IP address of the domain controller.
<i>User Group Mapping (LDAP)</i>	
Credential Options	<p>Select one of the following options.</p> <ul style="list-style-type: none"> • Use Domain Controllers username/password • Specify username/password
Address	<p>Specify the IP address of the LDAP server. If no address is specified, the system uses one of the configured Active Directory domain controllers.</p> <p>Example: 192.0.2.15</p>
Port	<p>Specify the port number of the LDAP server. If no port number is specified, the system uses port 389 for plain text or port 636 for encrypted text.</p>

Table 230: Fields on the Create Active Directory Profile Page (*Continued*)

Field	Description
Base DN	Enter the LDAP base distinguished name (DN). Example: DC=example,DC=net
Username	Enter the username of the LDAP account. If no username is specified, the system will use the configured domain controller's username. Example: administrator
Password	Enter the password for the account. If no password is specified, the system uses the configured domain controller's password.
Advanced	
SSL	Click the toggle button to enable Secure Sockets Layer (SSL) to ensure secure transmission with the LDAP server. This field is disabled by default and the password is sent in plain text.
Authentication Algorithm	Click the toggle button to specify the algorithm used while the SRX Series Firewall communicates with the LDAP server. By default, <code>simple</code> is selected to configure simple (plain text) authentication mode.
<i>IP-User Mapping</i>	
Event log scanning interval	Enter the scanning interval at which the SRX Series Firewall scans the event log on the domain controller. The range is 5 through 60 seconds.

Table 230: Fields on the Create Active Directory Profile Page (*Continued*)

Field	Description
Event log span	<p>Enter the time of the earliest event log on the domain controller that the SRX Series Firewall will initially scan. This scan applies to the initial deployment only. After WMIC and the user identification start working, the SRX Series Firewall scans only the latest event log.</p> <p>The range is 1 through 168 seconds.</p>
<i>Assign Device</i>	
Device	<p>Select these devices from the Available column and move to the Selected column.</p> <p>You can also search for the devices in the search field in both the Available and Selected columns. You can search these devices by entering the device name, device IP address, or device tag.</p>
<i>Timeout</i>	
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 that when a user is no longer active, a timer starts 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 thirty minutes. To disable timeout, set the interval to zero. The range is 10 through 1440 minutes.</p>

Table 230: Fields on the Create Active Directory Profile Page (*Continued*)

Field	Description
WMI Timeout	<p>Configure the number of seconds that the domain PC has to respond to the SRX Series Firewall's query through Windows Management Instrumentation (WMI) or Distributed Component Object Module (DCOM).</p> <p>If there is no response from the domain PC within the <code>wmi-timeoutinterval</code>, 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 exists for the probed IP address, and no response is received from the domain PC within the <code>wmi-timeout</code> interval, the probe fails and that entry is deleted from the table.</p> <p>The range is 3 through 120 seconds.</p>
<i>Filter</i>	
Filter	<p>Set the range of IP addresses that must be monitored or not monitored.</p> <ul style="list-style-type: none"> • Include—Specify to include IP addresses from the Available column. • Exclude—Specify to exclude IP addresses from the Available column. <p>Click Add New Address to create an IP address and add it as either include or exclude from monitoring.</p>

Deploy an Active Directory Profile to SRX Series Firewalls

To deploy an Active Directory profile to SRX Series Firewalls:

1. Select **SRX > Identity > Active Directory**.

The Active Directory Profile page appears.

2. Select the required SRX Series Firewall to deploy the Active Directory profile, and click **Deploy**.

A new job is created.

3. Select **Administration**>**Jobs** and click the job name link to see the deploy status.

The Job status page appears showing the state of the deployed job.

Edit, Clone, and Delete an Active Directory Profile

IN THIS SECTION

- [Edit an Active Directory Profile | 635](#)
- [Clone an Active Directory Profile | 635](#)
- [Delete an Active Directory Profile | 636](#)

You can edit and delete Active Directory profiles. This topic contains the following sections:

Edit an Active Directory Profile

To edit an Active Directory profile:

1. Select **SRX** > **Identity** > **Active Directory**.

The Active Directory Profile page appears listing the existing Active Directory profiles.

2. Select the Active Directory profile that you want to edit and click the pencil icon.

The Edit Active Directory Profile page appears, showing the same options as when creating a new Active Directory profile.

3. Click **OK** after completing editing.

Clone an Active Directory Profile

To clone an Active Directory profile:

1. Select **SRX** > **Identity** > **Active Directory**.

The Active Directory Profile page appears listing the existing Active Directory profiles.

2. Select the Active Directory profile that you want to clone and click **More** > **Clone**.

The Clone Active Directory Profile page appears, showing the same options as when creating a new Active Directory profile.

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

Delete an Active Directory Profile

To delete an Active Directory profile from all devices:

1. Select **SRX > Identity > Active Directory**.

The Active Directory Profile page appears listing the existing Active Directory profiles.

2. Select the active directory profile that you want to delete and then click the delete icon.

The the selected active directory profile is deleted from all the SRX Series Firewalls. An alert message appears verifying that you want to delete your selection.

3. Click **Yes** to delete your selection.

Identity-Access profile

IN THIS CHAPTER

- [LDAP Functionality in Integrated User Firewall Overview | 637](#)
- [About the Access Profile Page | 639](#)
- [Create Access Profiles | 640](#)
- [Deploy the Access Profile to SRX Series Firewalls | 645](#)
- [Edit, Clone, and Delete Access Profiles | 646](#)

LDAP Functionality in Integrated User Firewall Overview

IN THIS SECTION

- [Understanding the Role of LDAP in an Integrated User Firewall | 637](#)
- [Understanding the LDAP Server Configuration and Base Distinguished Name | 638](#)
- [LDAP Authentication Method | 638](#)
- [LDAP Server Username, Password, and Server Address | 638](#)

The topics in this section use the term *Lightweight Directory Access Protocol (LDAP)* to apply specifically to LDAP functionality within the integrated user firewall feature.

This topic includes the following sections:

Understanding the Role of LDAP in an Integrated User Firewall

SRX Series Firewalls use the Lightweight Directory Access Protocol (LDAP) to get user and group information necessary to implement the integrated user firewall feature. The SRX Series Firewall acts as an LDAP client communicating with an LDAP server. In a common implementation scenario, the domain

controller acts as the LDAP server. The LDAP module in the SRX Series Firewall, by default, queries the Active Directory in the domain controller.

The SRX Series Firewall downloads user and group lists from the LDAP server. The device also queries the LDAP server for user and group updates. The SRX Series Firewall downloads a first-level, user-to-group mapping relationship and then calculates a full user-to-group mapping.

Understanding the LDAP Server Configuration and Base Distinguished Name

Most of the LDAP server configuration is optional, because the common implementation uses the domain controller as the LDAP server. The SRX Series Firewall periodically (every two minutes) queries the LDAP server to get the user and group information changed since the last query.

The only required LDAP server configuration is the LDAP base distinguished name (DN), which is at the top level of the LDAP directory tree. Microsoft Active Directory follows the convention of deriving the base DN from a company's Domain Name System (DNS) domain components. An example of a base DN is `dc=juniper, dc=net`.

LDAP Authentication Method

By default, the LDAP authentication method uses simple authentication. The client's username and password are sent to the LDAP server in plaintext. Keep in mind that the password is clear and can be read from the network.

To avoid exposing the password, you can use simple authentication within an encrypted channel, namely Secure Sockets layer (SSL), as long as the LDAP server supports LDAP over SSL. After enabling SSL, the data sent from the LDAP server to the SRX Series Firewall is encrypted.

LDAP Server Username, Password, and Server Address

The LDAP server's username, password, IP address, and port are all optional, but they can be configured.

- If the username and password are not configured, the system uses the configured domain controller's username and password.
- If the LDAP server's IP address is not configured, the system uses the address of one of the configured Active Directory domain controllers.
- If the port is not configured, the system uses port 389 for plaintext or port 636 for encrypted text.

About the Access Profile Page

IN THIS SECTION

- [Tasks You Can Perform | 639](#)
- [Field Descriptions | 639](#)

To access this page, click **SRX > Identity > Access Profile**.

Access profiles enable access configuration on the network—this consists of authentication configuration. Juniper Security Director Cloud supports RADIUS, Lightweight Directory Access Protocol (LDAP), and local authentication as authentication methods. You can use the Access Profile page to configure the Lightweight Directory Access Protocol (LDAP) for SRX Series Firewalls that use the integrated user firewall feature. The SRX Series Firewall acts as an LDAP client communicating with an LDAP server.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create an access profile. See ["Create Access Profiles" on page 640](#).
- Modify, clone, or delete an existing access profile. See ["Deploy the Access Profile to SRX Series Firewalls" on page 645](#).
- Deploy the access profile to SRX Series Firewalls. See ["Deploy the Access Profile to SRX Series Firewalls" on page 645](#).

Field Descriptions

[Table 231 on page 639](#) provides guidelines on using the fields on the Access Profile page.

Table 231: Access Profile Main Page Fields

Field	Description
Name	Name of the access profile.

Table 231: Access Profile Main Page Fields (Continued)

Field	Description
Order1	Shows the order in which Junos OS tries different authentication methods when verifying that a client can access the devices.
Order2	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.
Description	Describes the access profile.
Local Users	Users with local authentication.
LDAP Server (Address)	Specifies the IP address of the LDAP authentication server.
RADIUS Server (Address)	Specifies the IP address of the RADIUS authentication server.

Create Access Profiles

Use the Access Profile page to create access profile with local, LDAP, or RADIUS authentication methods.

To create access profile with local, LDAP, or RADIUS authentication methods:

1. Select **SRX > Identity > Access Profile**.
2. Click the + icon.
3. Complete the configuration by using the guidelines in [Table 232 on page 641](#).
4. Click **OK**.

A summary page display a preview of the complete configuration.

Table 232: Access Profile Configuration Parameters

Field	Description
<i>General Setting</i>	
Access Profile Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. The maximum length is 255 characters.
Description	Enter a description for the access profile. The maximum length is 255 characters.
<i>Assign Device</i>	
Device	Select these devices from the Available column and move to the Selected column. You can also search for the devices in the search field in both the Available and Selected columns. You can search these devices by entering the device name, device IP address, or device tag.
Authentication	Select the authentication method the device should use to authenticate users; <ul style="list-style-type: none"> • Local • RADIUS • LDAP
Local	Provide the following details: <ul style="list-style-type: none"> • Address Assignment—Select the address pool or create an address pool. • User Name—Enter the user name. • Secret—Enter the password for the server. • XAUTH IP Address—Enter the IPv4 address of the external authentication server. • Groups—Enter the group name to store several user accounts together on the external authentication servers.

Table 232: Access Profile Configuration Parameters *(Continued)*

Field	Description
RADIUS	<p>Select the toggle button to specify the details of RADIUS servers.</p> <p>To configure RADIUS Servers:</p> <ol style="list-style-type: none"> 1. Click the + icon. 2. Enter the following details: <ul style="list-style-type: none"> • IP Address—Enter the 32-bit IP address of the server. • Secret—Enter the password for the server. • Port—Enter the port number on which to contact the RADIUS server. The range is 1 through 65,535. • Retry—Enter the number of retries that a device can attempt to contact RADIUS server. The range is 1 through 10. • Routing Instance—Enter the routing instance used to send RADIUS packets to the RADIUS server. A routing instance is a collection of routing tables, the interfaces contained in the routing tables, and the routing protocol parameters that control the information in the routing tables. • 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 RADIUS authentication server. The range is 3 to 90 seconds. 3. Click OK.

Table 232: Access Profile Configuration Parameters *(Continued)*

Field	Description
LDAP	<p>Select the toggle button to specify the details of LDAP server.</p> <p>To configure LDAP Servers:</p> <ol style="list-style-type: none"> 1. Click the + icon. 2. Enter the following details: <ul style="list-style-type: none"> • IP Address—Enter the IPv4 address of the LDAP server. • Port—Enter the port number on which to contact the LDAP server. The range is 1 through 65,535. • Retry—Enter the number of retries that a device can attempt to contact an LDAP server. The range is 1 through 10. • Routing Instance—Enter the routing instance used to send LDAP packets to the LDAP server. A routing instance is a collection of routing tables, the interfaces contained in the routing tables, and the routing protocol parameters that control the information in the routing tables. • Source Address—Enter a source address for each configured LDAP server. Each LDAP request sent to an LDAP server uses the specified source address. • Timeout—Enter the amount of time that the local device waits to receive a response from an LDAP server. The range is 3 to 90 seconds. 3. Click OK.
<i>LDAP Options</i>	
Revert Interval	Specify the amount of time that elapses before the primary server is contacted if a backup server is being used. The range is 60 through 4,294,967,295 seconds.

Table 232: Access Profile Configuration Parameters (Continued)

Field	Description
Base distinguished name	<p>Specify the base distinguished name, that is used in one of the following ways:</p> <ul style="list-style-type: none"> • If you use the Assemble option to assemble the user's distinguished name and the base distinguished name is appended to a username to generate the user's distinguished name. The resulting distinguished name is used in the LDAP bind call. • If you are using the search filter to search for the user's distinguished name. The search is restricted to the subtree of the base distinguished name. <p>The base distinguished name is a series of basic properties that define the user. For example, in the base distinguished name, o=juniper, c=us, where o for organization, and c stands for country.</p>
LDAP Option Type	
Assemble	Specify that a user's LDAP distinguished name is assembled through the use of a common name identifier, the username, and base distinguished name.
Common name	Enter a common name identifier used as a prefix for the username during the assembly of the user's distinguished name. For example, uid specifies "user id," and cn specifies "common name."
Search Filter	Enter the name of the filter to find the user's LDAP distinguished name. For example, a filter cn specifies that the search matches a user whose common name is the username.
Admin Search	Perform an LDAP administrator search. By default, the search is an anonymous search. To perform an administrator search, you must specify administrator credentials, which are used in the bind as part of performing the search.
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>For example, cn=admin, ou=eng, o=juniper, dc=net.</p>
Password	Configure the plain-text password for the administrative user. This password is used in the bind for performing the LDAP search.

Table 232: Access Profile Configuration Parameters (*Continued*)

Field	Description
Order 1	<p>Configure the order in which the different user authentication methods are tried when a user attempts to log in. For each login attempt, the method for authentication starts with the first one, until the password matches.</p> <p>The method can be one or more of the following:</p> <ul style="list-style-type: none"> • NONE—No authentication for the specified user. • LDAP—Use LDP. The SRX Series Firewall uses this protocol to get user and group information necessary to implement the integrated user firewall feature. • Local—Use a locally configured password in the access profile. <p>You can set the password to none or configure for the following authentication orders:</p> <ul style="list-style-type: none"> • LDAP • Radius servers • Local • Radius—Use RADIUS authentication services. <p>If RADIUS servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order.</p>
Order 2	<p>Configure 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.</p>

Deploy the Access Profile to SRX Series Firewalls

To deploy the access profile to SRX Series Firewalls:

1. Select **SRX > Identity > Access Profile**.

The Access Profile page appears.

2. Select the access profile that you want to deploy, and click **Deploy**.

The Update Access Profile page appears.

A new job is created.

3. Click the job ID to see the update status.

The Job Status page appears showing the state of the updated job.

Edit, Clone, and Delete Access Profiles

IN THIS SECTION

- [Edit Access Profiles | 646](#)
- [Clone Access Profiles | 646](#)
- [Delete Access Profiles | 647](#)

You can edit, clone, and delete access profiles. This topic contains the following sections:

Edit Access Profiles

To edit an access profile:

1. Select **SRX > Identity > Access Profile**.

The Access Profile page appears listing the existing access profiles.

2. Select the access profile that you want to edit and click the edit icon.

The Edit Access Profile page appears, showing the same options as when creating a new access profile.

3. Click **OK** after completing editing.

Clone Access Profiles

To edit an access profile:

1. Select **SRX > Identity > Access Profile**.

The Access Profile page appears listing the existing access profiles.

2. Select the access profile that you want to clone, right-click and select **Clone** or select **More > Clone**.

The Clone Access Profile page appears, showing the same options as when creating a new access profile.

3. Click **OK** after filling the details.

Delete Access Profiles

To delete an access profile from Juniper Security Director Cloud:

1. Select **SRX > Identity > Access Profile**.

The Access Profile page appears listing the existing access profiles.

2. Select the access profile and click the **Delete**.

The delete access profile page opens.

3. Select **Delete From Security Director Inventory**.

This deletes the selected access profile from Juniper Security Director Cloud portal.

To delete an access profile from devices and Juniper Security Director Cloud portal:

1. Select **SRX > Identity > Access Profile**.

The Access Profile page appears listing the existing access profiles.

2. Select the access profile and click the **Delete**.

The delete access profile page opens.

3. Select **Delete From Device and Security Director Inventory**

This deletes the selected access profile from the SRX Series Firewalls and the Juniper Security Director Cloud portal.

Identity-Address Pools

IN THIS CHAPTER

- [About the Address Pool Page | 648](#)
- [Create Address Pool | 649](#)
- [Edit and Delete Address Pool | 650](#)

About the Address Pool Page

IN THIS SECTION

- [Tasks You Can Perform | 648](#)
- [Field Descriptions | 649](#)

To access this page, click **SRX > Identity > Address Pools**.

An address pool is a set of Internet Protocol (IP) addresses available for allocation to users, such as in host configurations with the DHCP. An address-assignment pool supports IPv4 address. You can create centralized IPv4 address pools independent of the client applications that use the pools.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create an address pool. See ["Create Address Pool" on page 649](#) .
- Edit and delete an address pool. See ["Edit and Delete Address Pool" on page 650](#) .

Field Descriptions

Table 233 on page 649 provides guidelines on using the fields on the Address Pool page.

Table 233: Fields on the Address Pool Page

Field	Description
Name	Specifies the address pool name.
Network Address	Specifies the network address.
Primary DNS	Specifies the primary DNS IP address.
Secondary DNS	Specifies the secondary DNS IP address.
Primary WINS	Specifies the primary Windows IP address.
Secondary WINS	Specifies the secondary Windows IP address.
Address Ranges	Specifies the address range name.

Create Address Pool

You can create centralized IPv4 address pools independent of the client applications that use the pools.

To create an address pool:

1. Select **SRX > Identity > Address Pools**.
2. Click the + icon.
The Create Address Pool page is displayed.
3. Configure according to the guidelines in [Table 234 on page 650](#).
4. Click the + icon to configure a named range of IPv4 addresses, used within an address-assignment pool.
5. Enter the lower and upper limit of an address range.
6. Click **OK**.

Table 234: Address Pool Configuration Parameters

Field	Description
General	
Pool Name	Enter the name of the address pool that begins with an alphanumeric character. Colons, periods, slashes, dashes, and underscores are allowed. The maximum length is 63 characters.
Network Address	Enter the network address (valid IPv4 prefix) used by 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 Windows IPv4 address.
Secondary WINS Server	Enter the secondary Windows IPv4 address.

RELATED DOCUMENTATION

[About the Address Pool Page | 648](#)

[Edit and Delete Address Pool | 650](#)

Edit and Delete Address Pool**IN THIS SECTION**

- [Edit an Address Pool | 651](#)
- [Delete an Address Pool | 651](#)

You can edit and delete an address pool.

Edit an Address Pool

To edit an address pool:

1. Select **SRX > Identity > Address Pools**.
The Address Pool page is displayed.
2. Select an address pool and click the pencil icon to edit address pool.
The Edit Address Pool page is displayed.
3. Edit the required fields.
4. Click **OK**.

Delete an Address Pool

To delete an address pool:

1. Select **SRX > Identity > Address Pools**.
The Address Pool page is displayed.
2. Select an address pool and click the delete icon.
A pop-up is displayed with a confirmation message.
3. Click **Yes** to delete the address object.

RELATED DOCUMENTATION

[About the Address Pool Page | 648](#)

[Create Address Pool | 649](#)

5

PART

Secure Edge

Service Management | 653

Security Policy | 683

Security Subscriptions | 704

Service Administration | 775

Identity | 816

CASB and DLP | 846

Service Management

IN THIS CHAPTER

- [Juniper Secure Edge Overview | 653](#)
- [About the Service Locations Page | 660](#)
- [Create a Service Location | 662](#)
- [Edit and Delete Service Locations | 664](#)
- [About the Sites Page | 665](#)
- [Create a Site | 668](#)
- [Create Bulk Sites | 674](#)
- [Edit and Delete Sites | 675](#)
- [About the IPsec Profiles Page | 676](#)
- [Create an IPsec Profile | 677](#)
- [Edit or Delete an IPsec Profile | 681](#)
- [About the External Probe Page | 682](#)

Juniper Secure Edge Overview

IN THIS SECTION

- [Benefits of Juniper Secure Edge | 658](#)
- [Create Your Juniper Secure Edge Organization | 659](#)

Juniper Secure Edge provides full-stack Secure Services Edge (SSE) capabilities to protect web, SaaS, and on-premise applications and provide users with consistent and secure access that follows them wherever they go. When combined with Juniper's AI-Driven SD-WAN, Juniper Secure Edge provides a

best-in-suite SASE solution that helps you deliver seamless and secure end-user experiences that leverage existing architectures and grow with them as they expand their SASE footprint.

Juniper Secure Edge provides a user-friendly and security-focused GUI interface that allows an administrator to perform specific tasks. When you log in to Juniper Secure Edge, the main menu on the left that is displayed and the actions that you can perform depend on your access privileges. [Table 235 on page 654](#) lists the main menu that is available in Juniper Secure Edge, a brief description of each menu item, and a link to the relevant topic in the Juniper Secure Edge User Guide.

Table 235: GUI Menu and Description

Menu	Description
Dashboard	<p>You can view information such as top events, top denials, top applications, top source and destination IP addresses, top traffic, and top infected hosts in graphical security widgets.</p> <p>These security widgets offer users a customized view of network security and can be added, removed, and rearranged as per each user's preference. See "About the Dashboard" on page 20 .</p>

Table 235: GUI Menu and Description (Continued)

Menu	Description
Monitor	<p>You can view following information from the Monitor menu:</p> <ul style="list-style-type: none"> • Site Tunnel Status—View the status of the configured tunnels between sites and service locations. See "About the Site Tunnel Status Page" on page 103 . • Service Locations—View the status of all the service locations, the users in a location, the bandwidth consumed by the users, and the available storage. See "About the Service Locations Page" on page 660 . • ATP—Juniper Advanced Threat Prevention Cloud (ATP Cloud) is a cloud-based service that provides complete advanced anti-malware and anti-ransomware protection against “zero-day” and unknown threats. Monitor the status of compromised hosts, malicious threat sources, suspicious file downloads, Domain Name System (DNS) Domain Generation Algorithm (DGA) detections, tunnel detections, encrypted traffic insights, quarantined e-mails, blocked e-mails, and telemetry of blocked web and email files in ATP Cloud. See "Hosts Overview" on page 108 . • ATP Report Definitions—Build custom threat assessment reports which meet your needs for viewing incidents during specific time-frames. See "About the ATP Report Definition Page" on page 183 .

Table 235: GUI Menu and Description (Continued)

Menu	Description
Secure Edge	<p>You can manage the following services from the Secure Edge menu:</p> <ul style="list-style-type: none"> • Service Management <ul style="list-style-type: none"> • Service Locations—Manage service locations for Juniper Secure Edge instances. Service locations are the connection (access) point for both onpremises and roaming users. See "About the Service Locations Page" on page 660 . • Sites—Manage sites that are usually aligned with physical locations of customers, such as a branch or office. See "About the Sites Page" on page 665 . • IPsec Profiles—Create IPsec profiles to define the parameters with which an IPsec tunnel is established when the Customer Premises Equipment (CPE) devices start communicating with your Juniper Secure Edge instance. See "About the IPsec Profiles Page" on page 676 . • Security Policy—Manage the rules of Juniper Secure Edge policies which specify the actions to take for specific sets of traffic. You can filter and sort this information to get a better understanding of what to configure. See "About the Secure Edge Policy Page" on page 683 . • Security Subscriptions <ul style="list-style-type: none"> • IPS—Manage IPS rules and exempt rules in IPS profiles that are deployed on a device. See "IPS Policies Overview" on page 705 . • Web Filtering—Manage web filtering profiles which enable you to manage Internet usage by preventing access to inappropriate Web content over HTTP. See "Web Filtering Profiles Overview" on page 715 .

Table 235: GUI Menu and Description (Continued)

Menu	Description
	<ul style="list-style-type: none"> • Content Filtering—Manage content filtering policies that determine the file type based on the file content and not based on the file extensions. See "Content Filtering Policies Overview" on page 747 . • SecIntel—Configure a SecIntel profile group to add SecIntel profiles, such as C&C, DNS, and infected hosts. Once created, you can assign this group to the security policy. See "SecIntel Profiles Overview" on page 753 . • Anti-malware—Configure anti-malware profile and associate the profile with security policies. Anti-malware profiles define the content to scan for any malware and the action to be taken when malware is detected. See "Anti-malware Profiles Overview" on page 766 . • DNS Security—Create a DNS security profile for Domain Generation Algorithm (DGA) detection and tunnel detection. See "Create a DNS Security Profile" on page 772 . • ETI—Create an ETI profile that detects malicious threats hidden in encrypted traffic without intercepting and decrypting the traffic. See "Create an Encrypted Traffic Insights Profile" on page 774 . • Service Administration <ul style="list-style-type: none"> • Certificate Management—Manage the device certificates to establish TLS or SSL sessions. See "Certificate Management Overview" on page 776 . • PAC Files—Manage proxy auto configuration files which tell a web browser where to direct the traffic for a URL. See "Proxy Auto Configuration Files Overview" on page 784 .

Table 235: GUI Menu and Description (*Continued*)

Menu	Description
	<ul style="list-style-type: none"> • Explicit Proxy Profiles—Create an explicit proxy profile which tells Juniper Secure Edge the ports to listen to for the client-side traffic and the traffic to decrypt or bypass. See "Configure an Explicit Proxy Profile" on page 795 . • Decrypt Profiles—Manage decrypt profiles which allow you to define the types of traffic that should be exempted from decryption. See "Decrypt Profiles Overview" on page 806 . • Identity <ul style="list-style-type: none"> • User Authentication—Configure authentication profiles to authenticate the end users. See "End User Authentication Overview" on page 816 . • JIMS—Onboard JIMS Collector which collects and maintains a large database of user, device, and group information from Active Directory domains or system log services. See "Juniper Identity Management Service Overview" on page 833 .
Shared Services	<p>ATP—Configure various settings to protect against compromised hosts, malicious threat sources, suspicious file downloads, Domain Name System (DNS) Domain Generation Algorithm (DGA) detections, tunnel detections, encrypted traffic insights, quarantined e-mails, blocked e-mails, and telemetry of blocked web and email files in Juniper Advanced Threat Prevention Cloud (ATP Cloud). See "File Inspection Profiles Overview" on page 939 .</p>

Benefits of Juniper Secure Edge

- **Secure the Remote Workforce**—Support the WFA workforce wherever users are located. Security policies follow the user wherever they go, whether they're on or off the network.
- **Single-Policy Framework**: Use the same policy framework as with the SRX Series Firewalls and apply security policies to remote users and branch sites. Create policies once and apply everywhere with

unified policy management, including user- and application-based access, IPS, anti-malware and secure web access within a single policy framework.

- **Leverage Existing Investments—**Moving to a cloud-based security architecture shouldn't mean abandoning existing IT investments. Organizations can transition at their own pace without forcing administrators to toggle between separate management platforms for on-premises and cloud-delivered security. Juniper customers can use the physical, virtual, containerized SRX firewalls, and now cloud-delivered Secure Edge services, completely managed by Security Director Cloud with a single-policy framework, allowing for full visibility and consistent security across both the edge and the data center from one UI.
- **Dynamic User Segmentation Based on Zero Trust Principles—**Maintain the security of data around identity- and risk-driven policies. Juniper Secure Edge delivers a consistent security policy framework with policies that automatically adapt based on new risk and attack vectors and follow the user wherever they go, providing secure access to employees and third-party contractors through granular policy control, to further protect data by adhering to Zero Trust principles.
- **Security Assurance—**Whether it's a rule for a traditional firewall policy or policy delivered as a service, it's important that rules are placed in the proper order to be effective when needed. With Juniper Secure Edge organizations can utilize Security Director Cloud's automation, and duplicate and shadowed rules are flagged before committed. Rule hit counts are highlighted so administrators can quickly make changes, ensuring that policies are effective for the intended users at the intended time, and makes cleaning up deprecated rules easy for the organization when they know these rules are no longer in use. This takes a big chunk of the stress out of day-to-day operations.
- **Integrate with Any Identity Provider—**Juniper Secure Edge is flexible and easily integrates with any identity service to define user-based policies and application usage based on individual users or user groups via direct integration with Azure AD and Okta, and SAML 2.0 support to integrate with all other identity services.
- **Proven Security Effectiveness—**Validated protection from attacks that is more than 99% effective against client- and server-side exploits, malware and C2 traffic, regardless of where the users and applications are located, ensuring consistent security enforcement.

Create Your Juniper Secure Edge Organization

1. Open the URL to the [Juniper Security Director Cloud](#) portal.
2. In the portal, click **Create an Organization Account**.
The Login Credentials page opens. Use this page to set the login credentials for your account.
3. Enter the following details and click **Next**.
 - E-mail address—your preferred e-mail address.
 - Password—a password of your choice.

The Contact Details page opens.

4. Enter your full name, company name, country, the phone number for your organization and click **Next**.

The Organization Account Details page opens.

5. Type the name of your organization or the organization that will be using Juniper Security Director Cloud to manage devices.
6. Read the terms and conditions of use, and if you agree, click **Create Organization Account**.
You will receive an e-mail to verify your e-mail address and to send a request to the Juniper Security Director Cloud team to activate your organization account.
7. Log in to your e-mail account, open the e-mail, and click **Activate Organization Account** to send a request to activate your organization account.

NOTE:

- You must verify your e-mail address and click the **Activate Organization Account** button within 24 hours after receiving the e-mail. Otherwise, your account details will be deleted from Juniper Security Director Cloud, and you will have to re-create your account and send the activation request.
- After verifying your e-mail and sending the account activation request, you will receive an e-mail about your organization account activation status within 7 working days.

If your account activation request is approved, you will receive an e-mail with log in page information.

8. Click **Go to Login Page** and enter your e-mail address and password to log in and start using the Juniper Security Director Cloud portal.

About the Service Locations Page

IN THIS SECTION

- [Tasks You Can Perform | 661](#)
- [Field Descriptions | 661](#)

To access this page, select **Secure Edge > Service Management > Service Locations**.

A service location, also known as POP (point of presence), represents Juniper Secure Edge cloud service instance. The service location is the access point for both on-premises and roaming users through which your security policies and configurations are enforced. You can select two service locations to provide maximum availability in case of site level failures in the cloud, for Juniper Secure Edge instance. You can also use this page to edit and to delete the existing POPs.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a service location—See ["Create a Service Location" on page 662](#).
- Edit or delete a service location—See ["Edit and Delete Service Locations" on page 664](#).
- View the status of existing service locations.

Field Descriptions

[Table 236 on page 661](#) describes the fields on the **Service Locations** page.

Table 236: Fields on the Service Locations Page

Field	Description
Name	Name of the service location pair.
Service Locations	Secure Edge service locations in one or more geographic regions.
Subscriptions	List of linked subscriptions.
Total Users	The total number of users who can use the Secure Edge in a particular geographic region.
Cloud IP	Public IP address of a Juniper Secure Edge instance.

Table 236: Fields on the Service Locations Page (Continued)

Field	Description
Status	<p>Possible statuses include:</p> <ul style="list-style-type: none"> • In progress: The creation of Service Edge is in progress. <p>NOTE: It might take 10 to 15 minutes for Service Edge to become active.</p> <ul style="list-style-type: none"> • Active: Service Edge is active at the service location. • Failed: The creation of Service Edge has failed.

Create a Service Location

Use the **Create Service Location** page to create a pair of POPs (points of presence) for Juniper Secure Edge. Service Location is the set of service instances running in a POP location for a user. If you want to create additional pair of service locations, you must purchase additional licenses. By default, Secure Edge subscription enables you to create a single pair of service locations across geographies. The total users specified for a service location tells Secure Edge the capacity that it needs to provision for.

To create a service location:

1. Select **Secure Edge > Service Management > Service Locations**.

The **Service Locations** page appears.

2. Click the add icon (+).

The **Create Service Location** wizard appears.

3. Complete the configuration according to the guidelines provided in [Table 237 on page 663](#).

NOTE: Fields marked with * are mandatory.

4. Click **OK**.

A service location is created. You are returned to the **Service Locations** page where a confirmation message is displayed.

NOTE:

- Service locations are available in North America, Europe and Asia Pacific regions.
- When you create two or more service location pairs for different geographic locations, you can assign any of the service locations as the primary service location and secondary service location on the **Traffic Forwarding** wizard of **Create Site** page.

Table 237: Service Location Settings

Setting	Guideline
Name	Enter a unique name for the service location pair. Use a maximum of 255 alphanumeric characters.
Locations	
Location 1	Select location 1 for Secure Edge in the region.
Location 2	Select location 2 for Secure Edge in the region.
Subscriptions	
Subscriptions	<p>Select the available subscriptions from the list.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • To add more than one subscription to the service location pair, click +. To delete the subscription, select the checkbox and click the delete icon. • For a pair of service locations, the selected subscriptions should be either Standard or Advanced.
Total users	Shows the total number of users who can use Secure Edge for the selected subscriptions. You can increase the total user capacity by linking more subscriptions of the same type.

Edit and Delete Service Locations

IN THIS SECTION

- [Edit a Service Location | 664](#)
- [Delete a Service Location | 664](#)

You can edit and delete the service locations from the **Service Locations** Page.

Edit a Service Location

You cannot modify the Name and Edge Locations that are defined while editing a service location. You can only link subscriptions to increase the number of users who can use the service.



WARNING: Downgrade of number of users is not supported.

To link more subscriptions to a service location:

1. Select **Secure Edge > Service Management > Service Locations**.
The **Service Locations** page appears, displaying the existing service locations.
2. Select the custom service location that you want to update and click the pencil icon.
The **Update Service Location** page appears, displaying the same fields that are presented when you create a service location.
3. Link the additional subscriptions as needed.
4. Click **OK** to save your changes.
You are taken to the **Service Locations** page. A confirmation message appears indicating the status of the edit operation.

Delete a Service Location

NOTE: Before deleting a service location, ensure that the POP location is not assigned to Sites. If you try to delete a service location that is used in Sites, an error message is displayed.

To delete one or more service locations:

1. Select **Secure Edge > Service Management > Service Locations**.

The **Service Locations** page appears, displaying the existing service locations.

2. Select one or more service locations that you want to delete and click the delete icon.

An alert message appears, asking you to confirm the delete operation.

3. Click **Yes** to delete the selected service locations.

A confirmation message appears, indicating the status of the delete operation.

About the Sites Page

IN THIS SECTION

- [Tasks You Can Perform | 665](#)
- [Field Descriptions | 667](#)

To access this page, select **Secure Edge > Service Management > Sites**.

A site is a customer location such as a branch or office. Some or all of Internet bound traffic from customer sites may be forwarded to the Juniper Secure Edge cloud through GRE or IPsec tunnels from CPE devices at the site. You can view and manage the existing sites configuration using Sites page. You can also use this page to create, edit, and delete sites.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a site—See "[Create a Site](#)" on page 668 .
- Edit or delete a site—See "[Edit and Delete Sites](#)" on page 675 .
- View the site, CPE, and tunnel configuration details in a hierarchy-based structure—See [Table 238 on page 667](#) .
- View the details of a site. To do this, hover over the site name and click the Detail icon or Click **More** and select **Detail**.
- Sort the sites. Click the **Name** column to sort the sites based on the site name.
- Clone a site. To do this:
 1. Select a site that you want to clone.

2. Select **Clone** from the More list.

The Clone Site page appears with editable fields. For more information on the fields, see ["Create a Site" on page 668](#) .

3. Edit the required configurations and click **Finish** at the end of the workflow.

- Create bulk sites—See ["Create Bulk Sites" on page 674](#) .
- Export sites. To do this, click **Export** in the top-right corner of the page.

Once the export process is complete, click **Download** to download all the deployed site details.

- Refresh the status of the tunnels configured. To do this click **Refresh Tunnels** at the top-right corner of the page.
- View and deploy the undeployed sites. To do this, click the **Undeployed** tab, select the sites that show the Deploy Status as **Ready to Deploy**, and then click **Deploy** at the top-right corner of the page.
- View the list of sites that are deployed under Deployed tab.
- Add and hide advanced filter.

To add filters:

1. Click the filter icon and then select **Show advanced filter**.

The Add Criteria window opens.

2. Select the values for Field and Conditions from the list.
3. Enter the value for the selected field and conditions.
4. Click **Add** and then click **Save**.

The Save Filter page opens.

5. Enter a filter name. If you want to make this saved filter as default, then enable **Set as default**.

The filter is saved.

NOTE: Click **X** to clear the saved filters.

6. Click **Close** once the successful message is displayed.

To hide a filter click the filter icon and then select **Hide advanced filter**.

Field Descriptions

Table 238 on page 667 describes the fields on the Sites page.

Table 238: Fields on the Sites Page

Field	Description
Name	<p>The name of the site.</p> <p>Click the arrow before the site name to view the following details:</p> <ul style="list-style-type: none"> • CPE Name • IPsec Profile Name • CPE Tunnels A—Number of up/down tunnels in service location A. • CPE Tunnels B—Number of up/down tunnels in service location B. • Tunnel Configurations—Tunnel configurations for customer premises equipment (CPE).
Users	Number of users who can use the network at the site.
Service Location A	The Service Location A to which the traffic from the site will be forwarded.
Service Location B	The Service Location B to which the traffic from the site will be forwarded.
Deploy Status	Success or failure of site deployment.
Protected Networks	List of IP address ranges at the site that are protected by Secure Edge.
Description	The description for the site.

Create a Site

Use the **Create Site** page to create a site. You can forward the Internet bound traffic from CPE devices at this site to Juniper Secure Edge through GRE or IPsec tunnels. You can create the following types of tunnels:

- GRE
- IPsec:
 - Static
 - Dynamic

To create a Site:

1. Select **Secure Edge>Service Management>Sites**.
The Sites page appears.
2. Click the add icon (+).
The **Create Site** page opens.
3. Configure the fields on the Site Details tab according to the guidelines in [Table 239 on page 668](#) .

NOTE: Fields in the Secure Edge UI marked with an asterisk (*) are mandatory.

Table 239: Site Details Settings

Setting	Guideline
Service Locations	
Service location A	Select the first service location A from the list to which your on-premises sites should connect.
Service location B	Select the second service location B from the list to which your on-premises sites should connect.
Number of Users	Enter the number of users at the site.
Site Details	

Table 239: Site Details Settings (Continued)

Setting	Guideline
Name	Enter a unique string for the site name containing maximum 63 alphanumeric characters. The name can contain dashes and underscores.
Description	Enter a description containing maximum 255 characters for the site.
Country	Select the country where the site is located.
Postal code	Enter the postal code of the site.
Site address	Enter the location address of the site.
External probe	Enable this option for a site to allow CPE to check tunnel health status by sending ICMP packets to the probe destination. For more information on the probe destination, see "About the External Probe Page" on page 682 .
Protected networks	Click the add icon (+) to enter the IP address ranges at the site that should have access to Secure Edge.

4. Click **Next**.
The Traffic Forwarding page appears.
5. Click + to add CPE and interfaces or click on the pencil icon to edit the existing traffic forwarding configuration.
6. Configure the fields on the Traffic Forwarding page according to the guidelines in [Table 240 on page 669](#) .

Table 240: Traffic Forwarding Settings

Setting	Guideline
Add CPE and Interfaces.	

Table 240: Traffic Forwarding Settings (Continued)

Setting	Guideline
CPE Name	<p>Enter the CPE device name for the site. To configure the interfaces:</p> <ol style="list-style-type: none"> a. Click + and enter the following details: <ol style="list-style-type: none"> i. Interface Name—Enter interface name. ii. Tunnel Type—Select the type of tunnel as either IPsec or GRE to forward the traffic. iii. IP Address Type—Enter the device IP address. This option is enabled only when you select the IPsec IP address type as Static IP address, or when you select the type of tunnel as GRE. iv. IKE ID—Enter the Internet Key Exchange (IKE) ID (domain name) for the site. This option is enabled only when you select the type of IP address as Dynamic IP address. v. External Interface—Enter the external interface name. An external interface is the method by which you connect your device to the Internet/network. The default value is ge-0/0/0.0. b. Click the tick icon on the right-side of the row once done with the configuration or click X to cancel.
IPsec Profile Name	<p>Select the IPsec profile from the list. To create a new IPsec profile, click Create New. For information on the IPsec profile field options, see "Create an IPsec Profile" on page 677 .</p> <p>NOTE: This option is enabled only when you select tunnel type as IPsec.</p>

Table 240: Traffic Forwarding Settings (Continued)

Setting	Guideline
Pre-shared key	Enter the pre-shared key to authenticate the remote access user. The key should be minimum 6 characters long with at least one lower case, one upper case, one number and one special character. NOTE: This option is enabled only when you select tunnel type as IPsec.

7. Click **OK** and then click **Close**.

8. Click **Next**.

The CPE Configuration page appears.

9.

NOTE: When you enable **Skip CPE Configuration**, the CPE routing configuration is not generated. When you expand the site name and then click **View** under Tunnel Configurations, Junos CLI tab shows no configuration.

Enable **Skip CPE Configuration** when configuring a CPE device using Mist, when configuring a Juniper SSR SD-WAN device, or when configuring a third-party CPE device.

Disable **Skip CPE Configuration** when configuring a Junos CPE device using the CLI editor to allow Secure Edge to generate a proposed Junos CLI tunnel configuration. Copy and paste this configuration into the Junos CPE device's CLI editor.

Configure the fields on the CPE Configuration page according to the guidelines in [Table 241 on page 671](#).

Table 241: Traffic Forwarding Configuration Settings on the CPE Configuration Page

Setting	Guideline
CPE Name	Displays the CPE device name of the site. NOTE: To edit this option, click Back at the top-right corner and edit the configuration in Traffic Forwarding page.

Table 241: Traffic Forwarding Configuration Settings on the CPE Configuration Page *(Continued)*

Setting	Guideline
Interfaces	<p>Displays the number of external interfaces configured. Hover over the number to view the interface details. The default value is ge-0/0/0.0.</p> <p>NOTE: To edit this option, click Back at the top-right corner and edit the configuration in Traffic Forwarding page.</p>
IPsec Profile Name	<p>Displays the IPsec profile name that you have selected while configuring the Traffic Forwarding.</p> <p>NOTE: To edit this option, click Back at the top-right corner and edit the configuration in Traffic Forwarding page.</p>
Pre-shared Key	<p>Displays the pre-shared key that you have entered while configuring the Traffic Forwarding.</p> <p>NOTE: To edit this option, click Back at the top-right corner and edit the configuration in Traffic Forwarding page.</p>

10. When **Skip CPE Configuration** is disabled, you can configure the following options (optional):
 - a. Select the CPE and click the pencil icon on the right-side of the row.
 - b. Configure the CPE routing configuration fields on the CPE Configuration page according to the guidelines in [Table 242 on page 672](#)

Table 242: CPE Configuration Settings

Setting	Guideline
Primary SL	<p>Select the Service Location from the list that primarily process the traffic sent from Site CPE device to Secure Edge. If the primary Service Location fails, the other service location becomes the secondary and process the traffic from the Site CPE device to Secure Edge.</p> <p>The default service location is Service Location A.</p>

Table 242: CPE Configuration Settings (Continued)

Setting	Guideline
Tunnel seed	<p>Enter the tunnel seed number between 1 and 1000. This seed number determines Junos OS CLI tunnel interface identifiers.</p> <p>For example, the first tunnel interface is assigned the designator SEED+1 and the second tunnel interface is assigned the designator SEED+2.</p> <p>The default value is 1.</p>
Tunnel Security Zone	Enter the type of zone for tunnel security. The default zone is trust.
External Interface Zone	Enter the type of zone for external interface. The default zone is untrust.
Tunnel Routing-Instance	Enter the routing instance that contains the tunnel destination address. Your configuration may not have a routing-instance. If so, leave this field blank.

- c. Scroll-down and click the tick icon on the right-side of the row once the configuration is complete.

11. Click **Next**.

The summary tab with the details entered in Site Details tab, Traffic Forwarding tab and CPE Configuration opens.

12. Review the summary and click **Finish** to complete Site creation.

The Sites page opens with a message that the operation is in progress and then successful.

The new site is added to Juniper Secure Edge.

NOTE:

- If you see **Failed** in the Deploy Status column, recheck your service location configurations.

- If you want to undeploy the created site or any existing deployed sites, select the site and click **Undeploy** at the top-right corner of the page.

13. Click the arrow before the site name to view the CPE and tunnel configuration details.

14. Click **View** in the Tunnel Configurations column.

The View Tunnel Configurations page appears showing the tunnel configuration commands and the configuration summary.

15. Click **Copy to Clipboard** in the Junos CLI tab or follow the configuration in the Configuration Summary tabs accordingly and paste it to the device to configure tunnels.

After configuring the tunnels successfully, expand the site name and then click **View** under Tunnel Configurations to view the following operational status:

- Green tick icon indicates the number of tunnels that are configured successfully in Juniper Secure Edge.
- Red x icon indicates the number of tunnels that are inactive between the CPE device and Juniper Secure Edge.

You can also view the tunnel status at **Monitor > Tunnel Status > Site Tunnel Status**. For more information, see ["About the Site Tunnel Status Page" on page 103](#) .

Create Bulk Sites

Use the **Create Bulk Sites** page to create a set of new sites by uploading a bulk site template file in Microsoft Excel format.

To create bulk sites:

1. Select **Secure Edge > Service Management > Sites**.

The Sites page appears.

2. Select **More > Create bulk sites**.

The **Create Bulk Sites** wizard appears.

3. Click **Download Template** option and download the Microsoft Excel file to your local system.

4. Fill the details of the sites under each column of the Microsoft Excel file. For more information about the fields required for sites, see ["Create a Site" on page 668](#) .

5. Browse and upload the Microsoft Excel file filled with sites details.

After you upload the Microsoft Excel file, you can see the list of imported sites and other undeployed sites under **Undeployed** tab on the sites page.

NOTE: If you get errors after uploading the Microsoft Excel file, click **Download validated excel sheet** link to download the validated Microsoft Excel file to view and fix the errors. Then, upload the updated Microsoft Excel file.

6. Select one or more sites that you have imported using Microsoft Excel file on the **Sites** page and click **Deploy**.

You can see the **Deploy status** column as **Deployed** on the **Sites** page after the successful generation of tunnel configurations.

RELATED DOCUMENTATION

| [Create a Site | 668](#)

Edit and Delete Sites

IN THIS SECTION

- [Edit a Site | 675](#)
- [Delete a Site | 676](#)

You can edit and delete the Sites from the Sites Page. This topic has the following sections:

Edit a Site

To modify the parameters configured for a site:

1. Select **Secure Edge > Service Management > Sites**.
The Sites page appears.
2. Select the site that you want to edit. Click the edit icon (pencil symbol) on the top-right corner of the page.

NOTE: You cannot modify the site Name.

The **Edit Site** page appears, displaying the same options that are displayed when creating a new site.

3. Modify the parameters according to the guidelines provided in ["Create a Site" on page 668](#) .
4. Click **Finish** to save your changes. If you want to discard your changes, click **Cancel**.
If you click **Finish**, you will see the modified site and other undeployed sites under **Undeployed** tab on the **Sites** page.
5. Click **Deploy**.
You can see the **Deploy Status** column as **Success** under **Deployed** tab on the **Sites** page after the successful generation of tunnel configurations.

Delete a Site

To delete a site:

1. Select **Secure Edge > Service Management > Sites**.
The Sites page appears.
2. Select the set of sites which you want to delete and then click the delete icon (trash can).
An alert message appears, verifying that you want to delete the sites.
3. Click **Yes** to delete the sites. If you do not want to delete, click **Cancel** instead.
If you click **Yes**, the selected sites are deleted.

About the IPsec Profiles Page

IN THIS SECTION

- [Tasks You Can Perform | 676](#)
- [Field Descriptions | 677](#)

To access this page, select **Secure Edge > Service Management > IPsec Profiles**.

IPsec profiles define the parameters with which an IPsec tunnel is established when the Customer Premises Equipment (CPE) devices start communicating with your Secure Edge solution in cloud.

Use this page to view, create, edit and delete IPsec profiles.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create an IPsec profile—See ["Create an IPsec Profile" on page 677](#) .
- Edit or delete an IPsec profile—See ["Edit or Delete an IPsec Profile" on page 681](#) .
- View the details of an IPsec profile—Select an IPsec profile and click **More > Detail**, or mouse over the IPsec profile, and click the **Detailed View** icon. The Site Details tab appears on the right side of the IPsec profiles page.

Field Descriptions

[Table 243 on page 677](#) describes the fields on the IPsec Profiles page.

Table 243: Fields on the IPsec Profiles Page

Field	Description
Profile Name	The name of the IPsec profile.
Description	The description of the IPsec profile.
IKE Auth Method	The selected authentication method for an Internet Key Exchange (IKE) proposal.
IKE Encryption Algorithm	The selected encryption algorithm for an Internet Key Exchange (IKE) proposal.
IPsec Encryption Algorithm	The selected IPsec encryption algorithm to allow data communication securely.

Create an IPsec Profile

Use the Create IPsec Profile page to configure IPsec profiles. IPsec profiles define the parameters with which you can establish IPsec tunnels.

To create an IPsec profile:

1. Select **Secure Edge > Service Management > IPsec Profiles**.

The IPsec Profiles page opens.

2. Click the add icon (+).

The Create IPsec Profile page appears.

3. Complete the configuration according to the guidelines in [Table 244 on page 678](#) .

NOTE: Fields marked with an asterisk (*) are mandatory.

Table 244: Create IPsec Profile Settings

Setting	Guideline
Name	<p>Enter a unique IPsec profile name that is a string of maximum 18 characters without spaces.</p> <p>The string can contain alphanumeric characters and special characters such as colons, hyphens, periods, and underscores.</p>
Description	Enter the description for the IPsec profile.
IKE Settings	

Table 244: Create IPsec Profile Settings (Continued)

Setting	Guideline
IKE Auth Method	<p>Select an authentication method from the list that the device uses to authenticate the source of IKE messages.</p> <ul style="list-style-type: none"> • PSK—Specifies that a pre-shared 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. • ECDSA_256—Specifies that the Elliptic Curve Digital Signature Algorithm (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_384—Specifies that the ECDSA using the 384-bit elliptic curve secp384r1, as specified in the FIPS DSS 186-3, is used. • ECDSA_521—Specifies that the ECDSA using the 521-bit elliptic curve secp521r1, as specified in the FIPS DSS 186-3, is used. • RSA—Specifies that a public key algorithm, which supports encryption and digital signatures, is used.
Diffie-Hellman group	<p>Select a group from the list.</p> <p>Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process.</p>
Encryption algorithm	<p>Select the appropriate encryption mechanism for an Internet Key Exchange (IKE) proposal.</p>
Authentication algorithm	<p>Select an algorithm from the list.</p> <p>The device uses this algorithm to verify the authenticity and integrity of a packet.</p>

Table 244: Create IPsec Profile Settings (Continued)

Setting	Guideline
Lifetime seconds	<p>Select a lifetime of an IKE security association (SA).</p> <p>The valid range is from 180 to 86400 seconds. The common default value for IKE lifetime is 86400 seconds (1 day).</p> <p>NOTE: IKE lifetime value must be greater than the IPsec lifetime value.</p>
IPsec Settings	
Encryption algorithm	Select the IPsec encryption method that allows data to communicate securely.
Authentication algorithm	<p>Select an algorithm from the list.</p> <p>The device uses these algorithms to verify the authenticity and integrity of a packet.</p>
Lifetime seconds	<p>Select a value for the IPsec lifetime.</p> <p>The common default value for IPsec lifetime is 3600 seconds (1 hour).</p>
Perfect forward secrecy group	<p>Select Perfect Forward Secrecy (PFS) group as the method that the device uses to generate the encryption key.</p> <p>The PFS generates each new encryption key independently from the previous key. The higher numbered groups provide more security but require more processing time.</p>

4. Click **OK**.

The IPsec Profiles page opens with a message indicating that the IPsec profile is created successfully.

After you create an IPsec profile, you can assign it on the Traffic Forwarding tab of the Sites creation page, if you select the Tunnel Type as IPsec.

Edit or Delete an IPsec Profile

IN THIS SECTION

- [Edit an IPsec Profile | 681](#)
- [Delete an IPsec Profile | 681](#)

You can edit and delete the IPsec profiles from the IPsec Profiles page.

Edit an IPsec Profile

To edit an IPsec profile:

1. Select **Secure Edge > Service Management > IPsec Profiles**.

The IPsec Profiles page appears.

2. Select the IPsec profile that you want to edit. Click the edit icon (pencil symbol).

NOTE: You cannot modify the IPsec profile Name.

The Modify IPsec Profile page appears, displaying the same options that are displayed when creating a new IPsec profile.

3. Modify the IPsec profile fields. See "[Create an IPsec Profile](#)" on page 677 .

4. Click **OK** to save your changes.

The IPsec profiles page opens with a message that the IPsec profile was successfully updated.

Delete an IPsec Profile

To delete an IPsec profile:

1. Select **Secure Edge > Service Management > IPsec Profiles**.

The IPsec Profiles page appears.

2. Select one or more IPsec profiles, and click the delete (trash can) icon.

A warning message asking you to confirm the deletion is displayed.

3. Click **Yes** to proceed with the deletion.

The IPsec Profiles page opens with a message indicating the status of the delete operation.

About the External Probe Page

To access this page, select **Secure Edge > Service Management > External Probe**.

Use this page to configure probe settings to enable external probe for a site, which are used by CPE to monitor the tunnel health status.

To configure the external probe settings:

1. Enter the following configuration settings:

- Destination address—Enter the destination IPv4 address or DNS server.

By default, the destination IP address is 8.8.8.8 (Google Public DNS).

- Source subnet—Enter the source IPv4 address subnet and mask.

This feature supports all CPE devices with RPM-based ping capability, including the Junos OS and Mist/SSR devices. You can enable this feature for both IPsec and GRE tunnels.

2. Click **Save**.

Probe settings are configured. You can now enable external probe while creating a site at **Secure Edge > Service Management > Sites**.

RELATED DOCUMENTATION

[Create a Site](#) | 668

Security Policy

IN THIS CHAPTER

- [About the Secure Edge Policy Page | 683](#)
- [Add a Secure Edge Policy Rule | 687](#)
- [Edit, Clone, and Delete a Secure Edge Policy Rule | 693](#)
- [Reorder a Security Policy Rule | 694](#)
- [Select a Secure Edge Policy Source | 695](#)
- [Select a Secure Edge Policy Destination | 696](#)
- [Select Applications and Services | 697](#)
- [Common Operations on a Secure Edge Policy | 698](#)
- [Deploy Secure Edge Policies | 699](#)
- [Add SRX Policy Rules to Secure Edge Policy \(From Secure Edge Policy Page\) | 700](#)

About the Secure Edge Policy Page

IN THIS SECTION

- [Tasks You Can Perform | 684](#)
- [Field Description | 684](#)

To access this page, click **Secure Edge > Security Policy**.

Secure Edge policy specifies what actions to take for specific sets of traffic. Use the Secure Edge Policy page to view and manage policy rules. You can filter and sort this information to get a better understanding of what you want to configure.

Policy rules are executed in the order of their appearance. You must be aware of the following:

- Policy rules are applied from top to bottom. For example, Secure Edge policy has two rules *Rule-a* and *Rule-b*. *Rule-b* has sequence number 1 and the *Rule-a* has sequence number 2. If you deploy the policy, the rules are applied in the following sequence:
 1. *Rule-b*
 2. *Rule-a*
- Newly created policy rules go to the end of the list.
- You can change the order of policy rules. See, "[Reorder a Security Policy Rule](#)" on page 694 for more details.
- The last rule in the policy list is the default policy, which has the default action of denying all traffic.
- A policy rule can mask another policy rule.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a Secure Edge policy. See "[Add a Secure Edge Policy Rule](#)" on page 687
- Modify, clone, or delete a Secure Edge policy. See "[Edit, Clone, and Delete a Secure Edge Policy Rule](#)" on page 693
- Deploy a Secure Edge policy. See "[Deploy Secure Edge Policies](#)" on page 699
- Search for a Secure Edge policy. Click the search icon in the top-right corner of the page. You can enter partial text or full text of the keyword in the text box, and press Enter. The search results are displayed on the same page.
- Show or hide columns. Click the **Show Hide Columns** icon at the top right corner of the page.

Field Description

[Table 245 on page 685](#) provides guidelines on using the fields on the Secure Edge Policy page.

Table 245: Fields on the Secure Edge Policy Page

Field	Description
Seq	<p>The order number for the policy. The policy lookup is performed in the order that the policies are configured. The first policy that matches the traffic is used.</p> <p>Below the sequence number, you can also see the hit count. It displays how often a particular policy is used based on traffic flow. The hit count is the number of hits since the last reset.</p>
Rule Name	The name of the Secure Edge policy.
Sources	The source endpoint to which a Secure Edge policy applies. A source endpoint consists of sites, addresses, and user groups.
Destinations	The destination endpoint to which a Secure Edge policy applies. A destination endpoint can be addresses and URL categories.
Applications/Services	The applications and services associated with the security policy.

Table 245: Fields on the Secure Edge Policy Page *(Continued)*

Field	Description
Action	<p>The action applies to all traffic that matches the specified criteria.</p> <ul style="list-style-type: none"> • Permit—Device permits traffic using the type of security authentication applied to the policy. • Deny—Device silently drops all packets for the session and does not send any active control messages such as TCP Resets or ICMP unreachable. • Reject—Device sends a TCP reset if the protocol is TCP, and device sends an ICMP Unreachable if the protocols are UDP, ICMP, or any other IP protocol. This option is useful when dealing with trusted resources, so that applications do not waste time waiting for timeouts and instead get the active message. • Redirect—The redirect URL or a custom message to be shown when HTTP requests are blocked.

Table 245: Fields on the Secure Edge Policy Page (*Continued*)

Field	Description
Security Subscriptions	<p>The advanced security options are:</p> <ul style="list-style-type: none"> • IPS—IPS profile to monitor and prevent intrusions. • Decrypt—Decrypt profile to decrypt the SSL encryption. • Web Filtering—Web filtering to prevent access to inappropriate Web content over HTTP. • Content Filtering—Content filtering filters the content based on the file type, application, and direction. • SecIntel—SecIntel profiles that are grouped together. • Anti-malware—Anti-malware profile to scan the content for any malware and take actions when malware is detected. • CASB—Juniper Cloud Access Security Broker (CASB) profiles to detect and respond to insider threats and advanced cyberattacks.
Options	<p>This displays scheduling, logging, and captive portal information applicable to the Secure Edge policy.</p> <p>NOTE: Captive portal option is available only when you configure the source user group as unauthenticated users.</p>

Add a Secure Edge Policy Rule

Use this page to add Secure Edge policy rule that controls transit traffic within a context. The traffic is classified by matching its source sites, the source and destination addresses, and the application that the traffic carries in its protocol headers with the policy database.

You can also enable advanced security protection by specifying one or more of the following:

- Intrusion prevention system (IPS) profile

- Decrypt profile
- Web filtering
- Content filtering
- SecIntel group
- Anti-malware
- Cloud Access Security Broker (CASB)

Juniper Secure Edge provides the following methods to authenticate your on-premises users and devices:

- Juniper Identity Management System (JIMS)—You may deploy Juniper Identity Management System (JIMS) Collectors at your locations. JIMS retrieves the domain-joined authenticated users from your Active Directory and passes the information to Juniper Secure Edge service. This action allows your domain-joined users to access their applications seamlessly through Juniper Secure Edge without having to re-authenticate again, ensuring the best user experience.

NOTE: You can also retrieve user group information without deploying on-premises JIMS Collectors. Configure Identity Provider (IdP) settings in Juniper Secure Edge to retrieve user group information from Microsoft Entra ID (Azure AD) or Okta . Juniper Secure Edge receives user group information from Microsoft Entra ID or Okta. Administrators can use the user groups to manage security policies.

- Captive portal—You may also enable the captive portal option to require Juniper Secure Edge to authenticate your on-premises users. Consider this option if you want to authenticate your non-domain joined users by Juniper Secure Edge and if you want to have a backup authentication mechanism in case JIMS Collectors are not able to communicate with your Active Directory servers. By default, this feature is disabled for on-premises users. Before enabling the captive portal feature, consider the following:
 - You must make policy exceptions for on-premises users (such as guest users) and devices that your Active Directory cannot authenticate.
 - If you want to permit such users or devices to access through Juniper Secure Edge, you must place such exception policies above the captive portal policy.
 - Furthermore, you must place such users and devices in their own IP subnets so that manage the policy configurations.
 - The captive portal policy will work only for browser-based traffic.

- The recommended DHCP lease time is five hours. You must renew the lease before it expires or request a new IP address if the lease is not renewed. If the DHCP lease is not renewed or if a new IP address is assigned by DHCP, you must re-authenticate again.

To configure a Secure Edge policy rule:

1. Select **Secure Edge > Security Policy.**

The Secure Edge Policy page appears.

2. Click +.

The option to create Secure Edge policy rule appears inline on the Secure Edge Policy page.

3. Complete the configuration according to the guidelines provided in [Table 246 on page 689](#) .

4. Click the check mark icon ✓ to save the changes.

A new Secure Edge policy rule with the provided configuration is saved, and a confirmation message is displayed.

Table 246: Fields on the Secure Edge Policy Add Page

Field	Description
Rule Name	Enter a unique string beginning with a number or letter and consisting of letters, numbers, dashes and underscores. No spaces are allowed, and the maximum length is 63 characters. If you do not enter a name, the rule is saved with a default name assigned by Juniper Secure Edge.
Description	Enter a description for the policy rule; maximum length is 900 characters. The description must be a string excluding '&', '<', '>' and '\n' characters.
Sources	Click the add icon (+) to select the source end points on which the Secure Edge policy rule applies, from the displayed list of sites, addresses, and user groups.
Destinations	Click the add icon (+) to select the destination end points on which the Secure Edge policy rule applies, from the displayed list of addresses and URL categories.

Table 246: Fields on the Secure Edge Policy Add Page (*Continued*)

Field	Description
Application/Services	<p>Click the add icon (+) to select the applications and services.</p> <p>NOTE: Select the dependent applications for the CASB supported cloud applications. For information on the dependent applications, see "Create a CASB Profile" on page 726 .</p>
Action	<p>From the drop-down menu, select the action for the traffic between the source and destination.</p> <ul style="list-style-type: none"> • Permit—Device permits the traffic. • Deny—Device silently drops all packets for the session and does not send any active control messages such as TCP Resets or ICMP unreachable. • Reject—Device drops the packet and sends the following message based on traffic type: <ul style="list-style-type: none"> • TCP traffic: Device sends the TCP reset message to the source host. • UDP traffic: Device sends the ICMP message "destination unreachable, port unreachable". • For all other traffic: Device drops the packet without notifying the source host. • Redirect—When a policy blocks HTTP or HTTPS traffic with a reject action, you can define a response in the unified policy to notify the connected client. Redirect options: <ul style="list-style-type: none"> • Message—Select the message from the drop-down list or click Create redirect message and enter the message (in the Block Message field). • URL—Select the redirect URL from the drop-down list, or click Add redirect URL and enter the redirect URL.

Table 246: Fields on the Secure Edge Policy Add Page (Continued)

Field	Description
Security Subscriptions	<p>NOTE: You can configure all the security subscription options only if you select Permit for the action.</p> <ul style="list-style-type: none"> <p>• IPS— When you set the action to Permit, you can enable an IPS profile. Enable an IPS profile to monitor and prevent intrusions.</p> <p>• Decrypt profile—When you set the action to Permit or Reject, you can specify a decrypt profile by selecting a profile from the list. You can use the Decrypt profile to specify the traffic that may be decrypted or bypassed for decryption by Secure Edge. Click Create New, if you want to add a new Decrypt profile. NOTE: You must select a decrypt profile if you have selected a CASB profile.</p> <p>• Web filtering—When you set the action to Permit, you can specify a Web filtering profile by selecting a profile from the list. You can use the Web filtering profile to manage internet usage by preventing access to inappropriate Web content over HTTP. Click Create New, if you want to add a new Web filtering profile.</p> <p>• Content filtering—When you set the action to Permit, you can specify a Content filtering profile by selecting a profile from the list. You can use the Content filtering profile to filter the content based on the file type, application, and direction. The content filtering policy evaluates traffic before all other content security policies. Therefore, if traffic meets criteria configured in the content filter, the content filter acts first upon this traffic.</p>

Table 246: Fields on the Secure Edge Policy Add Page (*Continued*)

Field	Description
	<p>Click Create New, if you want to add a new Content filtering profile.</p> <ul style="list-style-type: none"> <p>SecIntel group—When you set the action to Permit, you can specify a SecIntel profile group by selecting a profile from the list.</p> <p>You use the SecIntel profile group to assign a group of different SecIntel profiles.</p> <p>Click Create New, if you want to add a new SecIntel group.</p> <p>Anti-malware—When you set the action to Permit, you can specify an antimalware profile by selecting a profile from the list.</p> <p>You can use the antimalware profile to define the content to scan for any malware and the action to be taken when a malware is detected.</p> <p>Click Create New if you want to add a new antimalware profile.</p> <p>CASB—When you set the action to Permit, you can specify a CASB profile by selecting a profile from the list.</p> <p>You can use the CASB profile to automatically detect anomalous usage and suspicious behavior.</p> <p>Click Create New if you want to add a new CASB profile. For more information, see "Create a CASB Profile" on page 726 .</p>

Table 246: Fields on the Secure Edge Policy Add Page (*Continued*)

Field	Description
Options	<p>Select a pre-saved schedule from the list.</p> <p>Policy schedules enable you to define when a policy is active, and thus are an implicit match criterion. Click Create Schedule to define a new schedule. You can define the day of the week and the time of the day when the policy is active. For instance, you can define a security policy that opens or closes access based on business hours.</p> <p>Enable the Logging option to log events when sessions are created.</p> <p>Enable the Captive Portal for site traffic option to allow authenticated on-premises site users to log in to Juniper Secure Edge. By default, captive portal option is enabled for roaming users and disabled for on-premises site users.</p>

Edit, Clone, and Delete a Secure Edge Policy Rule

IN THIS SECTION

- [Edit a Secure Edge Policy Rule | 693](#)
- [Clone a Secure Edge Policy Rule | 694](#)
- [Delete a Secure Edge Policy Rule | 694](#)

You can edit, clone, and delete Secure Edge policy rules from the **Secure Edge > Security Policy** page.

Edit a Secure Edge Policy Rule

To modify the parameters configured for a Secure Edge policy rule:

1. Select **Secure Edge > Security Policy**.

The **Secure Edge Policy** page appears, displaying the list of Secure Edge policies.

2. Select the Secure Edge policy rule that you want to edit, and click the pencil icon.
3. Modify the parameters and click ✓ to save the changes.

The modified rule appears on the Secure Edge Policy page.

Clone a Secure Edge Policy Rule

To clone a Secure Edge policy rule:

1. Select **Secure Edge** > **Security Policy**.

The Secure Edge Policy page appears.

2. Right-click the Secure Edge policy rule to clone, and select **Clone**. Alternatively, click **More** drop-down menu, and select **Clone**.

Update the cloned policy rule as required.

3. Click ✓ to save the changes.

The modified policy rule appears on the **Secure Edge Policy** page.

Delete a Secure Edge Policy Rule

To delete a Secure Edge policy rule:

1. Select **Secure Edge** > **Security Policy**.

The Secure Edge Policy page appears.

2. Select the Secure Edge policy rule you want to delete, and then click the delete icon.

An alert message appears, verifying that you want to delete the selected policy.

3. Click **Yes** to delete the selected policy rule.

Reorder a Security Policy Rule

The action of the first security policy rule that matches the traffic is applied to the packet. If there is no matching rules, the packet is dropped. The rules are matched from top to bottom, so it is a good idea to place more specific rules near the top of the list.

Steps to change the security policy rule order:

1. Select **Secure Edge** > **Security Policy**.

The **Secure Edge Policy** page is displayed with a list of security policy rules.

2. Click the security policy rule that you want to reorder.

3. Click **More**, and select any of the following options to change the rule ordering:

- Move Top
- Move Up

- Move Down
- Move Bottom

The modified rule order appears on the Secure Edge Policy page.

4. Preview and deploy the policy with the reordered rules. For details, see ["Deploy Secure Edge Policies" on page 699](#)

Select a Secure Edge Policy Source

You can view and select the source end point from the complete list of sites, addresses, and user groups.

1. Click the **Sources** field.
A list of relevant endpoints is displayed.
2. Complete the configuration according to the guidelines provided in [Table 247 on page 695](#)

Table 247: Source Fields on the Secure Edge Policy Page

Field	Description
Sites	Select the sites that are required as sources for the Secure Edge policy.
Addresses	<p>Select one of the following address options:</p> <ul style="list-style-type: none"> • Any—Add any address to the security policy. • Specific—Select the check box beside each address you want to include in the address group. Click the greater-than icon (>) to move the selected address or addresses from the Available column to the Selected column. Note that you can use the fields at the top of each column to search for addresses.

Table 247: Source Fields on the Secure Edge Policy Page (*Continued*)

Field	Description
User groups	<p>Select one of the following users or groups options:</p> <ul style="list-style-type: none"> • Any—Add any user or a group to the security policy. • Specific—Select the check box beside each user you want to include in the user group. Click the greater-than icon (>) to move the selected address or addresses from the Available column to the Selected column. Note that you can use the fields at the top of each column to search for addresses.

3. Click **OK** to select the end point as a source.

Select a Secure Edge Policy Destination

You can view and select the destination end point from the complete list of addresses.

1. Click on **Destinations**. A list of relevant end points is displayed.
2. Complete the configuration according to the guidelines provided in [Table 248 on page 696](#).

Table 248: Destination Fields on the Secure Edge Policy Page

Field	Description
Addresses	<p>Enter one or more address names or address set names.</p> <ul style="list-style-type: none"> • Any—Add any address to the security policy rule. • Specific—Select the check box beside each address you want to include in the address group. Click the greater-than icon (>) to move the selected address or addresses from the Available column to the Selected column. Note that you can use the fields at the top of each column to search for addresses.

Table 248: Destination Fields on the Secure Edge Policy Page (*Continued*)

Field	Description
URL Categories	<p>Enable the toggle button to configure the URL category:</p> <ul style="list-style-type: none"> • None • Any—Add any URL to the security policy. • Specific—Select the check box beside each URL you want to include. Click the greater-than icon (>) to move the selected URLs from the Available column to the Selected column.

3. Click **OK** to select the end point as a destination.

Select Applications and Services

IN THIS SECTION

- [Add Applications and Services to Security Policy | 697](#)

The following procedure provides instructions to add applications and services to the Secure Edge policy.

Add Applications and Services to Security Policy

You can add the applications and services to the existing security policy.

1. Click on **Applications/Services**. Applications & Services page is displayed.
2. Complete the configuration according to the guidelines provided in [Table 249 on page 698](#)

Table 249: Applications and Services Fields on the Security Policy Rule Page

Field	Description
Applications	<p>Select one of the following options for the applications:</p> <ul style="list-style-type: none"> • None • Any—Add any application to the security policy. • Specific—Click the + icon to add the application signatures and select the check boxes next to the application to be added. <p>NOTE: You can search for a specific application by entering the search criteria in the search field. You can search the applications by their name.</p>
Services	<p>Select one of the following options for the services:</p> <ul style="list-style-type: none"> • Default—Junos-default services. • Any—Add any service to the security policy. • Specific—Select the check box beside each service you want to include. Click the greater-than icon (>) to move the selected service or services from the Available column to the Selected column. Note that you can use the fields at the top of each column to search for services.

3. Click **OK** to add the selected applications and services to the security policy rule.

Common Operations on a Secure Edge Policy

You can perform common operations on a Secure Edge policy rule from the *Secure Edge Policy* page.

To perform common operations on a security policy:

1. Select **Secure Edge > Security Policy**.
The **Secure Edge Policy** page appears.
2. Click the security policy and click **More**.

The following common operations are available for a security policy.

- Add a rule before an existing rule.
- Add a rule after an existing rule.
- Create a copy of an existing rule.
- Enable the rule.
- Disable the rule.
- Probe latest hits to get the latest policy rule hit count. The hit count is incremented by 1 each time an entry is matched.
- Reset the hit count for a rule. Resetting sets the current hit count to zero.
- Move the rule by selecting one of the following options:
 - Move Top
 - Move Up
 - Move Down
 - Move Bottom
- Clear the sections for the rules.

Deploy Secure Edge Policies

After configuring the rules to the Secure Edge policies, you can deploy the Secure Edge policies by clicking the **Deploy** option. You can also deploy one or more policies from the **Secure Edge Policy** page.

To deploy Secure Edge policies:

1. Select **Secure Edge > Security Policy**.

The Security Policy page appears.

2. Select one or more policies and click **Deploy**.

The Deploy page appears.

3. Complete the configuration as per the guidelines provided in [Table 250 on page 700](#)

Table 250: Fields on the Deploy page

Field	Description
Deployment Time	<p>Choose one of the following options</p> <ul style="list-style-type: none"> • Run Now—Select this option to deploy the policy immediately. • Schedule at a later time—Select this option to specify the date and time at which the policy should be deployed.
Service Locations	Review the list of service locations to which the Secure Edge policy will be deployed.

4. Click **OK**.

A job is created. Click the job ID to go to the Jobs page and view the status of the deploy operation.

Add SRX Policy Rules to Secure Edge Policy (From Secure Edge Policy Page)

To migrate your on-premises security policies to Secure Edge, you must convert the security policy rules to Secure Edge policy. Use the Add SRX policy rules to Secure Edge policy page to add rules from the SRX policy to Secure Edge policy.

The Secure Edge policy supports only a single pair of zones (trust to untrust). All the selected zones of the SRX policy in the source endpoints are converted as trust zone. The destination endpoints are converted as untrust zone.

NOTE: Before initiating the conversion of SRX policy rules to Secure Edge policy, the system administrator must ensure that the source identities referred in the SRX policy rules are in-sync with JIMS Secure Edge source identities. This is to avoid any customization issues at a later stage.

To add the SRX policy rules to Secure Edge policy:

1. Select **Secure Edge > Security Policy**.

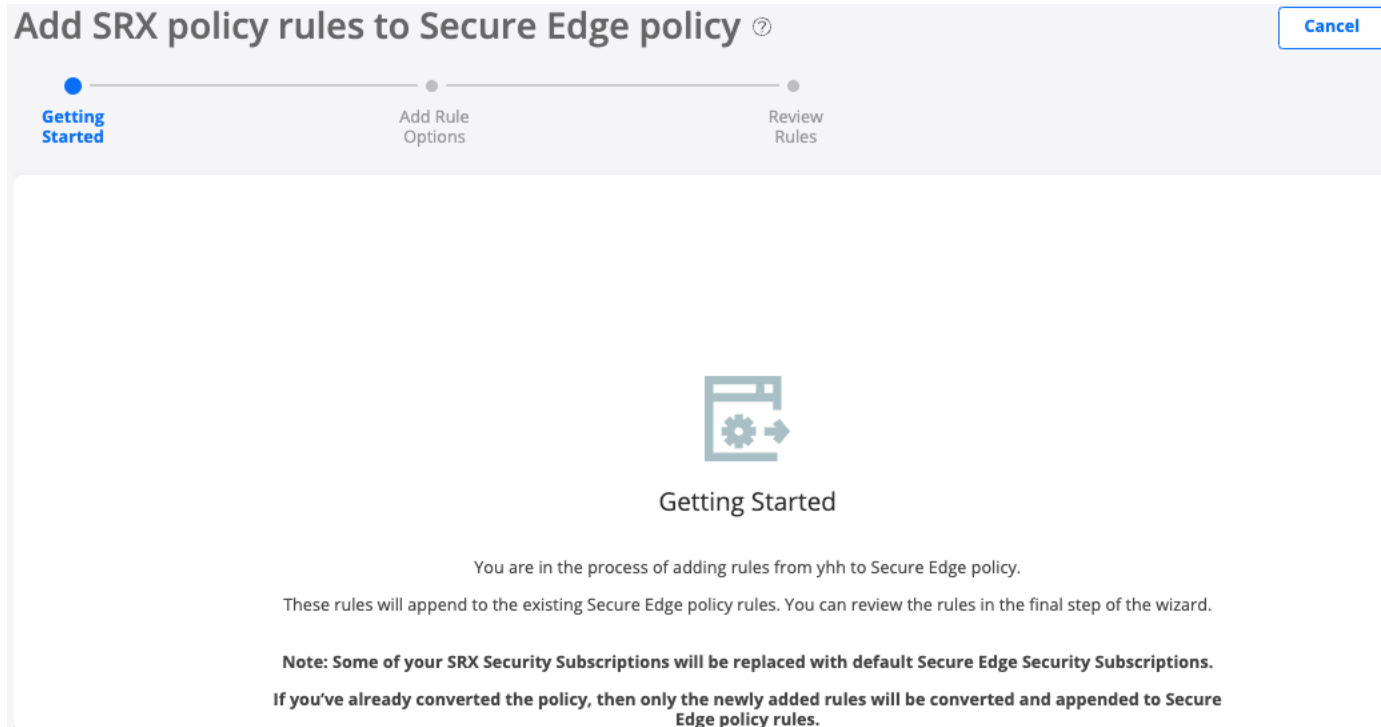
The Secure Edge Policy page appears.

2. From the More list, select **Add rules from SRX policy**.

The Add SRX policy rules to Secure Edge policy page appears.

3. Select the SRX policy to be added to the Secure Edge policy and click **Next**.
The Getting Started page provides additional information about adding the SRX policy rules to Secure Edge policy, as shown in [Figure 18 on page 701](#).

Figure 18: Getting Started Page



4. Click **Next**.
5. Complete the configuration as shown in the following table.

Table 251: Fields on the Add Rule Options page

Field	Description
<i>Add Rule Options</i>	
Name	Name of the SRX policy.
Source (trust) zones	Select zones in the existing rules that are applicable for the Internet. These zones are set as source (trust) zones in the Secure Edge policy rule.

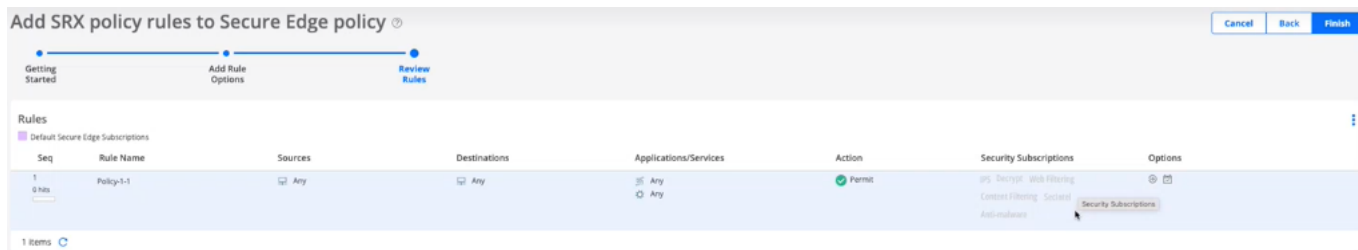
Table 251: Fields on the Add Rule Options page (*Continued*)

Field	Description
Destination (untrust) zones	Select zones in the existing rules that are applicable for the Internet. These zones are set as destination (untrust) zones in the Secure Edge policy rule.

6. Click **Next**.

The Rules Review page appears, as shown in [Figure 19 on page 702](#)

Figure 19: Rules Review Page



7. In the Review Rules page, preview the converted rules.

For the advanced security profiles conversion, Secure Edge policy takes the following actions:

- IPS—Policy is ignored and not converted. Default IPS of Secure Edge policy is associated. For more information, see ["About the IPS Profiles Page" on page 334](#).
- Content filtering—Policy is ignored and not converted. Default Content filtering profile of Secure Edge policy is associated. For more information, see ["About the Content Filtering Profiles Page" on page 427](#).
- Decrypt profile—Decrypt profiles are converted as it is except for the root certificate. The root certificate set is converted to Secure Edge with the name "jsec-ssl-proxy-root-cert". The decrypt profile name is prefixed with "jse-".
- Web filtering—Profile is converted and a new Secure Edge Web Filtering profile is created with categories that map to current actions and defaults.
- Antivirus profile—Profile is ignored and not converted.
- Antispam profile—Profile is ignored and not converted.
- SecIntel profile—SecIntel profiles are converted as it is. The profile name is prefixed with "jse-".

- Anti-malware profiles—SMTP and IMAP Anti-malware profiles are ignored and not converted. HTTP Anti-malware profile is converted as it is. The profile name is prefixed with “jse-”.

8. Click **Finish** after reviewing the rules.

A job is created to add rules to Secure Edge. Once the conversion is successful, you are taken back to the Secure Edge Policy page. The converted rules are appended at the bottom of the existing Secure Edge policy rules. You can reorder the converted rules. You can perform all the other operations on the converted rules.

Figure 20: Secure Edge Policy Page

Seq	Rule Name	Sources	Destinations	Applications/Services	Action	Security Subscriptions	Options
1	rule-with-features-open-fo	Any	Any	None	Permit	IPS, Decrypt, Web Filtering, Content Filtering, SecuShield, Anti-malware	
2	Host-53-policy-2-zone-rule_clone Host-53-policy-2-zone-rule	Any	Any	Any	Permit	IPS, Decrypt, Web Filtering, Content Filtering, SecuShield, Anti-malware	
3	Veers-vSRX-53-16-5-1_clone-1	Any	Any	Any	Permit	IPS, Decrypt, Web Filtering, Content Filtering, SecuShield, Anti-malware	
4	untrust-trust-rule-max-description Juniper SDenCloud is your portal to Secure Access S...	Any	Any	Any	Permit	IPS, Decrypt, Web Filtering, Content Filtering, SecuShield, Anti-malware	
5	Veers-vSRX-53-16-deactivate-4b-rule Veers-vSRX-53-16-deactivate-4b-rule	Any	Any	Any	Permit	IPS, Decrypt, Web Filtering, Content Filtering, SecuShield, Anti-malware	
6	Zone1-Zone2-webproxy-rule Rule is disabled due to unsupported configurations ...	Any	Any	Any	Permit	IPS, Decrypt, Web Filtering, Content Filtering, SecuShield, Anti-malware	
7	Global-Policy-rules-trust-untrust	Any	Any	Any	Permit	IPS, Decrypt, Web Filtering, Content Filtering, SecuShield, Anti-malware	
8	Global-Policy-rules-trust-untrust_clone	Any	Any	Enhanced_Abused_Drugs	Permit	IPS, Decrypt, Web Filtering, Content Filtering, SecuShield, Anti-malware	
9	Global-Policy-rules-malware-dso-zone	Any	Any	Any	Redirect	IPS, Decrypt, Web Filtering, Content Filtering, SecuShield, Anti-malware	
10	Global-Policy-rules-malware-dso-zone	Any	Any	Any	Permit	IPS, Decrypt, Web Filtering, Content Filtering, SecuShield, Anti-malware	

The final step is to deploy the converted policy. Select the policy and click **Deploy**.

NOTE:

- You cannot reconvert SRX policy rules that are already converted to the Secure Edge Policy rules. However, if you have added new rules to that particular SRX policy, only the newly added rules are added to the Secure Edge policy rules.
- Global rules are selected only if they are matched with the selected source and destination zones. Global rules that are not associated with a source or destination zone are ignored and not converted.

Security Subscriptions

IN THIS CHAPTER

- [IPS Policies Overview | 705](#)
- [About IPS Policies | 705](#)
- [Create IPS Rule | 707](#)
- [Edit, Clone, and Delete IPS Rules | 710](#)
- [Create Exempt Rule | 711](#)
- [Edit, Clone, and Delete Exempt Rule | 713](#)
- [Web Filtering Profiles Overview | 715](#)
- [About the Web Filtering Profiles Page | 715](#)
- [Create a Web Filtering Profile | 718](#)
- [Edit, Clone, and Delete a Web Filtering Profile | 721](#)
- [CASB Overview | 722](#)
- [About the CASB Profiles Page | 724](#)
- [Create a CASB Profile | 726](#)
- [Edit and Delete a CASB Profile | 731](#)
- [About the CASB Rules Page | 732](#)
- [Add Rules to a CASB Profile | 735](#)
- [Edit and Delete a CASB Rule | 739](#)
- [About the Application Instances Page | 740](#)
- [Create an Application Instance | 742](#)
- [Edit and Delete an Application Instance | 745](#)
- [About the Application Tagging Page | 746](#)
- [Content Filtering Policies Overview | 747](#)
- [About the Content Filtering Policies Page | 748](#)
- [Create a Content Filtering Policy | 749](#)
- [Add Rules in a Content Filtering Policy | 750](#)
- [Edit and Delete a Content Filtering Policy | 751](#)

- [Edit, Clone, and Delete a Content Filtering Policy Rule | 752](#)
- [SecIntel Profiles Overview | 753](#)
- [About SecIntel Profiles | 754](#)
- [Create Command and Control Profile | 755](#)
- [Create DNS Profile | 757](#)
- [Create Infected Hosts Profile | 759](#)
- [Edit, Clone, and Delete SecIntel Profile | 761](#)
- [About SecIntel Profile Groups | 762](#)
- [Create SecIntel Profile Group | 764](#)
- [Edit, Clone, and Delete SecIntel Profile Group | 765](#)
- [Anti-malware Profiles Overview | 766](#)
- [About Anti-malware Profiles | 767](#)
- [Create Anti-malware Profile | 768](#)
- [Edit, Clone, and Delete Anti-malware Profile | 771](#)
- [Create a DNS Security Profile | 772](#)
- [Create an Encrypted Traffic Insights Profile | 774](#)

IPS Policies Overview

An intrusion prevention system (IPS) policy defines how your device handles the network traffic. It allows you to enforce various attack detection and prevention techniques on traffic traversing your network. You can define policy rules to match a section of traffic based on a zone, network, and application, and then take active or passive preventive actions on that traffic.

About IPS Policies

IN THIS SECTION

- [Tasks You Can Perform | 706](#)

To access this page, select **Secure Edge > Security Subscriptions > IPS**.

The intrusion prevention system (IPS) profile is deployed on a device by associating the profile with a firewall policy intent, which is deployed on the device. You can associate IPS rules or exempt rules with an IPS profile.

Use this page to view, add, modify, clone, or delete the IPS rules and exempt rules in the IPS profiles.

Tasks You Can Perform

- Create an IPS rule—See ["Create IPS Rule" on page 707](#) .
- Create an exempt rule—See ["Create Exempt Rule" on page 711](#) .
- Edit, clone, or delete an IPS rule—See ["Edit, Clone, and Delete IPS Rules" on page 710](#) .
- Edit, clone, or delete an Exempt rule—See ["Edit, Clone, and Delete Exempt Rule" on page 713](#) .
- Search for rules by using keywords—Click the search icon, enter the search term in the text box, and press Enter. The search results are displayed on the same page.
- Filter rules—Click the filter icon (funnel), and specify one or more filtering criteria. The filtered results are displayed on the same page.

NOTE: Filtering is applicable only to some fields.

- **Table 252: Fields on the IPS Policy Page**

Field	Description
Name	The name of the IPS rule.
IPS Signatures	Displays the IPS signatures associated with the IPS rule. If multiple signatures are associated with the rule, the number of additional signatures is displayed. Hover over the number to view the full list of signatures.
Action	Displays the action to be taken when the IPS rule is matched.

Table 252: Fields on the IPS Policy Page (Continued)

Field	Description
Options	Displays the configuration options for IPS rules. Hover over the arrow icon to view the logging options configured.

Create IPS Rule

You can create intrusion prevention system (IPS) rules only for customized IPS profiles.

To create an IPS rule:

1. Select **Secure Edge > Security Subscriptions > IPS**.

The IPS Policy page appears.

2. Click the add (+) icon on the IPS Rules tab.

The parameters for an IPS rule are displayed inline at the top of the page.

3. Complete the configuration according to the guidelines in [Table 253 on page 707](#).

4. Click the check mark (✓) to save your changes.

The changes are saved and a confirmation message is displayed at the top of the page.

You can use the IPS profile in a firewall policy intent. When you deploy the firewall policy on the device, the IPS and exempt rules associated with the profile are also deployed.

Table 253: Create IPS Rule Settings

Setting	Guideline
Name	Juniper Security Edge generates a unique rule name by default. You can modify the name. The name must begin with an alphanumeric character and can contain maximum 63 characters, which includes alphanumeric characters and some special characters, such as colons, hyphens, forward slashes, periods, and underscores.

Table 253: Create IPS Rule Settings (Continued)

Setting	Guideline
Description	Enter a description containing maximum 1024 characters for the rule.
IPS Signatures	<p>Add one or more IPS signatures and IPS signature static and dynamic groups to be associated with the rule:</p> <ol style="list-style-type: none"> <li data-bbox="857 632 1422 758">a. Click the + icon inside the text box. A list of IPS signatures and IPS signature static and dynamic groups opens. <li data-bbox="857 789 1422 852">b. (Optional) Click the add (+) icon to add signatures. The Add IPS Signatures popup window opens. <li data-bbox="857 884 1422 947">c. (Optional) Enter a search term and press Enter to filter the list of items displayed. <li data-bbox="857 978 1422 1083">d. Click a list item to add it to the IPS signatures and IPS signature static or dynamic groups associated with the rule. <li data-bbox="857 1115 1422 1178">e. (Optional) Repeat the preceding step to add more signatures, static groups, and dynamic groups.

Table 253: Create IPS Rule Settings (Continued)

Setting	Guideline
Action	<p>Select the action to be taken when the monitored traffic matches the attack objects specified in the rules:</p> <ul style="list-style-type: none"> • Recommended (default)—Uses the action that Juniper Networks recommends when an attack is detected. All predefined attack objects have a default action associated with the objects. • No action—No action is taken. Use this action to only generate logs for some traffic. • Drop Connection—Drops all packets associated with the connection and prevents traffic for the connection from reaching its destination. Use this action to drop connections for traffic that is not prone to spoofing. • Drop Packet—Drops a matching packet before it can reach its destination but does not close the connection. Use this action to drop packets for attacks in traffic that is prone to spoofing, such as UDP traffic. Dropping a connection for such traffic could result in a denial of service that prevents traffic from a legitimate source IP address. • Close Client—Closes the connection and sends an RST packet to the client, but not to the server. • Close Server—Closes the connection and sends an RST packet to the server, but not to the client. • Close Client and Server—Closes the connection and sends a TCP reset (RST) packet to both the client and the server. • Ignore Connection—Stops scanning traffic for the rest of the connection if an attack match is found. IPS disables the rulebase for the specific connection.

Table 253: Create IPS Rule Settings (Continued)

Setting	Guideline
Options	Enable Log attacks option to create a log.

Edit, Clone, and Delete IPS Rules

IN THIS SECTION

- [Edit an IPS Rule | 710](#)
- [Clone an IPS Rule | 711](#)
- [Delete IPS Rules | 711](#)

Edit an IPS Rule

You can edit IPS rules associated only with customized IPS profiles, and not the rules associated with predefined (system-generated) profiles.

To edit an IPS rule:

1. Select **Secure Edge > Security Subscriptions > IPS**.

The IPS Policy page opens.

2. Click the IPS RULES tab and select the IPS rule.

3. Click edit (pencil) icon.

The rule selected for editing is displayed inline at the top of the page.

4. Modify the rule. See "[Create IPS Rule](#)" on page 707 .

5. Click the check mark (✓) to save your changes.

The changes are saved and a confirmation message is displayed at the top of the page.

If the IPS belongs to an IPS profile that is referenced in a firewall policy intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.

Clone an IPS Rule

Cloning enables you to easily create an IPS rule based on an existing one. You can clone IPS rules associated only with customized IPS profiles, and not rules associated with predefined (system-generated) profiles.

To clone an IPS rule:

1. Select **Secure Edge > Security Subscriptions > IPS**.

The IPS Policy page opens.

2. Click the IPS RULES tab and select the IPS rule.

3. Select a rule, and select **More > Clone**.

The rule selected for cloning is displayed inline at the top of the page.

4. Modify the rule. See "[Create IPS Rule](#)" on page 707 .

5. Click the check mark (✓) to save your changes.

The new rule is created and a confirmation message is displayed at the top of the page.

Delete IPS Rules

You can delete IPS rules associated only with customized IPS profiles, and not the rules associated with predefined (system-generated) profiles.

To delete IPS rules:

1. Select **Secure Edge > Security Subscriptions > IPS**.

The IPS Policy page opens.

2. Click the IPS RULES tab and select the IPS rule.

3. Select one or more rules, and click the delete (trash can) icon.

A warning message asking you to confirm the deletion is displayed.

4. Click **Yes**.

A message indicating the status of the delete operation is displayed at the top of the page.

If the deleted IPS rule belongs to an IPS profile that is referenced in a firewall policy intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.

Create Exempt Rule

You can create intrusion prevention system (IPS) exempt rules only for customized IPS profiles.

To create an exempt rule:

1. Select **Secure Edge > Security Subscriptions > IPS**.

The IPS Policy page opens.

2. Click the **Exempt Rules** tab.

3. Click the add (+) icon.

The parameters for an exempt rule are displayed inline at the top of the page.

4. Complete the configuration according to the guidelines in [Table 254 on page 712](#) .

5. Click the check mark (✓) to save your changes.

The changes are saved and a confirmation message is displayed at the top of the page.

You can use the IPS profile in a firewall policy intent. When you deploy the firewall policy on the device, the IPS and exempt rules associated with the profile are also deployed.

Table 254: Create Exempt Rule Settings

Setting	Guideline
Name	<p>Juniper Secure Edge generates a unique rule name by default. You can modify the name.</p> <p>The name must begin with an alphanumeric character and can contain maximum 63 characters, which includes alphanumeric characters and some special characters, such as colons, hyphens, forward slashes, periods, and underscores.</p>
Description	<p>Enter a description containing maximum 1024 characters for the rule.</p>

Table 254: Create Exempt Rule Settings (Continued)

Setting	Guideline
<p>IPS Signatures</p>	<p>Add one or more IPS signatures and IPS signature static and dynamic groups to be associated with the rule:</p> <ol style="list-style-type: none"> a. Click inside the text box with the + icon. A list of IPS signatures and IPS signature static and dynamic groups opens. b. (Optional) Click the add (+) icon to add signatures. The Add IPS Signatures popup window opens. c. (Optional) Enter a search term and press Enter to filter the list of items displayed. d. Click a list item to add it to the IPS signatures and IPS signature static or dynamic groups associated with the rule. e. (Optional) Repeat the preceding step to add more signatures, static groups, and dynamic groups.

Edit, Clone, and Delete Exempt Rule

IN THIS SECTION

- [Edit an Exempt Rule | 713](#)
- [Clone an Exempt Rule | 714](#)
- [Delete Exempt Rules | 714](#)

Edit an Exempt Rule

You can edit exempt rules associated only with customized IPS profiles, and not the rules associated with predefined (system-generated) profiles.

To edit an exempt rule:

1. Select **Secure Edge > Security Subscriptions > IPS**.

The IPS Policy page appears.

2. Click the EXEMPT RULES tab, then select the rule.
3. Click edit (pencil) icon.

The rule selected for editing is displayed inline at the top of the page.

4. Modify the rule. See "[Create Exempt Rule](#)" on page 711 .
5. Click the check mark (✓) to save your changes.

The changes are saved and a confirmation message is displayed at the top of the page.

If the exempt rule belongs to an IPS profile that is referenced in a firewall policy intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.

Clone an Exempt Rule

Cloning enables you to easily create an exempt rule based on an existing one. You can clone exempt rules associated only with customized IPS profiles, and not rules associated with predefined (system-generated) profiles.

To clone an exempt rule:

1. Select **Secure Edge > Security Subscriptions > IPS**.

The IPS Policy page appears.

2. Click the EXEMPT RULES tab.
3. Select a rule, and select **More > Clone**.

The rule selected for cloning is displayed inline at the top of the page.

4. Modify the rule. See "[Create Exempt Rule](#)" on page 711 .
5. Click the check mark (✓) to save your changes.

The new rule is created and a confirmation message is displayed at the top of the page.

Delete Exempt Rules

You can delete exempt rules associated only with customized IPS profiles, and not the rules associated with predefined (system-generated) profiles.

To delete exempt rules:

1. Select **Secure Edge > Security Subscriptions > IPS**.

The IPS Policy page opens.

2. Click the EXEMPT RULES tab.
3. Select one or more rules, and click the delete (trash can) icon.

A warning message asking you to confirm the deletion is displayed.

4. Click **Yes**.

A message indicating the status of the delete operation is displayed at the top of the page.

If the deleted exempt rule belongs to an IPS profile that is referenced in a firewall policy intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.

Web Filtering Profiles Overview

Juniper Secure Edge blocks or permits Web access based on built-in web categories or user-defined web categories.

Web filtering profiles enable you to manage Internet usage by preventing access to inappropriate Web content over HTTP. Juniper Networks provides a list of 178 categories which you can use to create Web filtering profiles and manage Web access in your enterprise network.

About the Web Filtering Profiles Page

IN THIS SECTION

- [Tasks You Can Perform | 715](#)
- [Field Descriptions | 716](#)

To access this page, select **Secure Edge > Security Subscriptions > Web Filtering Profiles**.

Use the Web Filtering Profiles page to view and to manage Web filtering profiles.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a Web filtering profile—See "[Create a Web Filtering Profile](#)" on page 718 .
- Edit, clone, or delete a Web filtering profile—See "[Edit, Clone, and Delete a Web Filtering Profile](#)" on page 721 .

- View the details of a Web filtering profile—Select the Web filtering profile to view the details and from the More menu, select **Detailed View**. The Web Filtering Profile Details page appears. [Table 256 on page 717](#) describes the fields on this page.
- Clear the selected Web filtering profiles—Click **Clear All Selections** to clear any Web filtering profiles that you might have selected.
- Search for Web filtering profiles using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.

Field Descriptions

[Table 255 on page 716](#) describes the fields on the Web Filtering Profiles page.

Table 255: Web Filtering Profiles Page Fields

Field	Description
Name	The name of the Web filtering profile.
Permitted Categories	The Juniper Networks pre-defined categories and custom categories of Web content that is permitted in the enterprise network.
Permitted & Logged Categories	The Juniper Networks pre-defined categories and custom categories of Web content that is permitted and logged in the enterprise network.
Denied Categories	The Juniper Networks pre-defined categories and custom categories of Web content that is denied in the enterprise network.
Quarantined Categories	The Juniper Networks pre-defined categories and custom categories of Web content that is quarantined in the enterprise network when detected.
Description	The description of the Web filtering profile.

Table 256: Web Filtering Profile Details Page Fields

Field	Description
Name	The name of the Web filtering profile.
Description	The description of the Web filtering profile.
Permitted Categories	The Juniper Networks pre-defined categories and custom categories of Web content that is permitted in the enterprise network.
Permitted & Logged Categories	The Juniper Networks pre-defined categories and custom categories of Web content that is permitted and logged in the enterprise network.
Denied Categories	The Juniper Networks pre-defined categories and custom categories of Web content that is denied in the enterprise network.
Quarantined Categories	The Juniper Networks pre-defined categories and custom categories of Web content that is quarantined in the enterprise network when detected.
Default action	The action for uncategorized URLs with no assigned action.
Fallback option	The fallback action to be used in the following scenarios: <ul style="list-style-type: none"> • The ThreatSeeker Websense Cloud servers are unreachable. • Requests to ThreatSeeker Cloud time out. • The device has too many requests to process.
Block options	The option selected to either block a URL address or a display a custom message when HTTP Web contents are blocked.

Table 256: Web Filtering Profile Details Page Fields (Continued)

Field	Description
Redirect Message	The redirect URL address or a custom message when HTTP requests are blocked.

Create a Web Filtering Profile

Web filtering profiles enable you to manage Internet usage by preventing access to inappropriate Web content over HTTP.

1. Select **Secure Edge > Security Subscriptions > Web Filtering Profiles**.

The Web Filtering Profiles page opens.

2. Click the **+** to create a Web filtering profile.

The Create Web Filtering Profile page opens.

3. Click **Next** to navigate to the next page.

4. Complete the configuration according to the guidelines provided in [Table 257 on page 718](#).

NOTE: Fields marked with * are mandatory.

Table 257: Fields on the Create Web Filtering Profile Page

Setting	Guideline
Name	Enter a unique name containing maximum 29 characters for the Web filtering profile.
Description	Enter a description containing maximum 255 characters for the Web filtering profile.

Table 257: Fields on the Create Web Filtering Profile Page *(Continued)*

Setting	Guideline
Force safe search	<p>Enable to filter explicit results and to prevent such results from appearing in your search results.</p> <p>Safe search ensures that embedded objects, such as images on the URL received from the search engines, are safe and that undesirable content is not returned to the client.</p>
Predefined URL categories	<p>View and edit the Juniper Networks pre-defined categories list</p> <p>Select the URL category, click Set action, then select one of the following actions for the category:</p> <ul style="list-style-type: none"> • Default • Log and permit • Block • Permit • Quarantine
Custom URL categories	<p>Create a list of custom URL categories.</p> <p>Click + to open the Add Custom URL Categories page. Select the category to add, and click Set action, then select one of the following actions:</p> <ul style="list-style-type: none"> • Log and permit • Block • Permit • Quarantine

Table 257: Fields on the Create Web Filtering Profile Page (*Continued*)

Setting	Guideline
Default action	<p>Select an action for the uncategorized URLs with no assigned action.</p> <p>This setting is used only if no reputation action is assigned.</p>
Fallback option	<p>Select the fallback action to be used in the following scenarios:</p> <ul style="list-style-type: none"> • The ThreatSeeker Websense Cloud servers are unreachable. • Requests to ThreatSeeker Cloud time out. • The device has too many requests to process.
Block options	<p>Select to block either a URL address or display a custom message when HTTP Web contents are blocked.</p>
Redirect message	<p>Specify the redirect URL or a custom message to be sent when HTTP requests are blocked. The maximum length is 1024 characters.</p> <p>NOTE: If a message begins with http: or https:, the message is considered a block URL. Messages that begin with values other than http: or https: are considered custom block messages.</p>

5. Click **Finish**.

A Web filtering profile is created, and the Web Filtering Profiles page opens with a confirmation message.

Edit, Clone, and Delete a Web Filtering Profile

IN THIS SECTION

- [Edit a Web Filtering Profile | 721](#)
- [Clone a Web Filtering Profile | 721](#)
- [Delete a Web Filtering Profile | 722](#)

You can edit, clone, and delete Web filtering profiles from the Web Filtering Profiles page. This topic has the following sections:

Edit a Web Filtering Profile

You cannot modify the default profiles present in the system.

1. Select **Secure Edge > Security Subscriptions > Web Filtering Profiles**.
The Web Filtering Profiles page opens, displaying the existing Web filtering profiles.
2. Select the custom Web filtering profile to edit, and click the pencil icon.
The Edit Web Filtering Profiles page opens.
3. Edit the Web filtering profile fields according to the guidelines provided in [Table 163 on page 405](#) .
4. Click **OK** to save your changes.

The Web Filtering Profiles page opens with a confirmation message indicating the status of the edit operation.

Clone a Web Filtering Profile

Cloning enables you to easily create a Web filtering profile based on an existing one.

1. Select **Secure Edge > Security Subscriptions > Web Filtering Profiles**.
The Web Filtering Profiles page opens, displaying the existing Web filtering profiles.
2. Select the Web filtering profile to clone, and select **More > Clone**.
The Clone Web Filtering Profiles page opens.
3. Edit the Web filtering profile fields according to the guidelines provided in [Table 163 on page 405](#) .
4. Click **OK** to save your changes.

The Web Filtering Profiles page opens with a confirmation message indicating the status of the clone operation.

Delete a Web Filtering Profile

Before deleting a Web filtering profile, ensure that the profile is not used in a content security profile. If you try to delete a Web filtering profile that is used in a content security profile, an error message is displayed.

1. Select **Secure Edge > Security Subscriptions > Web Filtering Profiles**.

The Web Filtering Profiles page opens, displaying the existing Web filtering profiles.

2. Select the custom Web filtering profiles to delete, and click the delete icon.

A message asking you to confirm the delete operation is displayed.

3. Click **Yes** to delete the selected Web filtering profiles.

A confirmation message indicating the status of the delete operation is displayed.

CASB Overview

IN THIS SECTION

- [Benefits of CASB | 723](#)

Massive adoption of cloud services and applications has created new targets and threats like never before. What's more, the widespread use of mobile devices is the new reality that organizations regularly interact with users they don't manage. Your systems, applications, and data are constantly in contact with mobile phones, tablets, and laptops that you do not control. Manual and people-centric cloud security approaches fail in such situations. Organizations must use automation to supplement their cloud security needs.

Juniper Secure Edge provides full-stack Security Service Edge (SSE) capabilities to protect web, Software as a Service (SaaS), and on-premises applications and provide users with consistent and secure access that follows them wherever they go.

A New Solution for Cloud Security—Cloud Access Security Broker (CASB)

CASB provides visibility into the security of your cloud applications. You can create CASB profiles in the Juniper Secure Edge to apply granular controls to ensure authorized access, threat prevention, and compliance to secure your data. You can also assign rules to a CASB profile and associate the profile with a Secure Edge policy to automatically detect anomalous usage and suspicious behavior.

[Table 258 on page 723](#) lists the Juniper Secure Edge supported cloud applications and their activities.

Table 258: Juniper Secure Edge Supported Cloud Applications and their Activities

Cloud Application	Supported Activities
Box	Login, Upload, Download, and Share
Dropbox	Login, Upload, Download, and Share
Gmail	Login, Read, Compose, Send, Upload Attachment, and Download Attachment
Google Docs	Login, Upload, Download, and Share
Microsoft OneDrive	Login, Upload, Download, and Share
Salesforce	Login, Upload, Download, and Share
SharePoint	Login, Upload, Download, and Share
Slack	Login, Chat, Audio/Video, and FileTransfer

Benefits of CASB

- Allow only validated users to access the data that is stored in the cloud to prevent unauthorized access. Data access control provides maximum visibility and control to the security teams over SaaS applications, enhancing Juniper Secure Edge's cloud-delivered security capabilities.
- Protect SaaS applications by granularly controlling user actions, scanning all existing and new files within SaaS applications for malware, and preventing the upload and download of compromised files.

RELATED DOCUMENTATION

| [About the CASB Profiles Page](#) | 724

About the CASB Profiles Page

IN THIS SECTION

- [Tasks You Can Perform | 724](#)
- [Field Descriptions | 725](#)

To access this page, select **Secure Edge > Security Subscriptions > CASB > CASB Profiles**.

Juniper Secure Edge provides full-stack Security Service Edge (SSE) capabilities to protect web, Software as a Service (SaaS), and on-premises applications and provide users with consistent and secure access that follows them wherever they go.

Cloud Access Security Broker (CASB) provides visibility into the security of your cloud applications. You can apply granular controls to ensure authorized access, threat prevention, and compliance to secure your data.

Use this page to add, edit, delete, or reset CASB profile preferences. You can also assign rules to a CASB profile and associate the profile with a Secure Edge policy to automatically detect anomalous usage and suspicious behavior.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a CASB profile. See ["Create a CASB Profile" on page 726](#) .
- Edit or delete a CASB profile. See ["Edit and Delete a CASB Profile" on page 731](#) .
- Add rules to a CASB profile. See ["Add Rules to a CASB Profile" on page 735](#) .
- Edit or delete a CASB profile rule. See ["Edit and Delete a CASB Rule" on page 739](#) .
- Associate CASB profiles with the Secure Edge Policy. To do this:
 1. Click the **Secure Edge Policy** link available under the CASB page title to directly navigate to the Secure Edge Policy page.
 2. Click **+** to add a new rule or click the pencil icon to edit an existing rule.
 3. Click **+** for Security Subscriptions and select a CASB profile from the CASB list.

NOTE: Alternatively, you can navigate to **Secure Edge > Security Policy** to associate the CASB profile to a Secure Edge policy.

- Add filters. To do this:

1. Click the filter icon and then select **Show advanced filter**.

The Add Criteria window opens.

2. Select the values for Field and Condition from the list.
3. Enter the value for the selected field and conditions.
4. Click **Add**.
5. Click **Save**.

The Save Filter page opens.

6. Enter a filter name. If you want to make this saved filter as default, then enable **Set as default**.

The filter is saved.

NOTE: Click **X** to clear the saved filters.

7. Click **Close** once the successful message is displayed.

- Hide filters. To do this, click the filter icon and then select **Hide advanced filter**.
- Search for CASB profiles using keywords. To do this, click the search icon and enter the search term in the text box and press **Enter**. The search results are displayed on the same page.
- Show or Hide Columns. To do this, choose to show or hide a specific column in the table. To do this, hover over the vertical ellipses, select **Show/Hide Columns**, and select the check box of the columns to display in the table.
- Reset Preference. To do this, reset the displayed columns to the default set of columns for each tab in the table. Hover your mouse cursor over the vertical ellipses and select **Reset Preference**.

Field Descriptions

[Table 259 on page 726](#) describes the fields on the CASB Profiles page.

Table 259: CASB Profiles Page Fields

Field	Description
Name	Displays a CASB profile name.
Rules	Displays the number of rules assigned to the CASB profile. Click Add Rules to configure a rule to control specific actions that can be performed on each cloud application.
Activity Logging	Displays the activity logging for the CASB profile. For example, Login, Upload, and Share.

Create a CASB Profile

You configure Cloud Access Security Broker (CASB) rules to control specific actions on each cloud application to secure your data.

By default, Juniper Secure Edge provides a pre-populated profile called **default-casb-profile**. You can choose to either modify and use the pre-populated profile, or create your own profile.

Once you create a CASB profile, assign it to a Secure Edge policy. The assigned CASB profile ensures that the traffic flows between cloud providers and organizational users (either on-premises or roaming) complies with the Secure Edge policy.

[Table 260 on page 726](#) lists the dependent applications that you must select in the Applications/ Services field when assigning a CASB profile to a Secure Edge policy.

Table 260: Secure Edge Policy—Dependent Applications for CASB Supported Cloud Applications

CASB Supported Cloud Applications	Dependent Applications When Configuring Secure Edge Policy
Box	BOXDOTNET

Table 260: Secure Edge Policy—Dependent Applications for CASB Supported Cloud Applications
(Continued)

CASB Supported Cloud Applications	Dependent Applications When Configuring Secure Edge Policy
Dropbox	<ul style="list-style-type: none">• DROPBOX-CLEAR• DROPBOX-UPLOAD• DROPBOX-DOWNLOAD• DROPBOX-LAN-SYNC
Salesforce	SALESFORCE and SALESFORCE-CHATTER

Table 260: Secure Edge Policy—Dependent Applications for CASB Supported Cloud Applications
(Continued)

CASB Supported Cloud Applications	Dependent Applications When Configuring Secure Edge Policy	
Gmail and Google Docs	<ul style="list-style-type: none"> • GOOGLE-DOCS-SPREADSHEET • GOOGLE-NEWS • GOOGLE-TAKEOUT • GOOGLE-CALENDAR • GOOGLE-WEBLIGHT • GOOGLE-EARTH • GOOGLE-SUPL • GOOGLE-CODE • YOUTUBE-COMMENT • GOOGLE-TRANSLATE • YOUTUBE-KIDS • GOOGLE-DOCS-WORD-DOCUMENT • YOUTUBE • GOOGLE-BLOG • GOOGLE-ACCOUNTS • GOOGLE-SPRAYSCAPE • GOOGLE-DOCS-PRESENTATION • GOOGLE-ONE • GOOGLE-PLUS 	<ul style="list-style-type: none"> • GOOGLE-VIDEO • GOOGLE-SPACES • GOOGLE-MOBILE-MAPS-APP • GOOGLETALK • GSUITE • GOOGLE-SKYMAP • GOOGLE-GEN • GOOGLE-STATIC • GOOGLE-API • GOOGLE-SYNDICATION • GOOGLE-SAFEBROWSE-SUB • GOOGLE-DOCS • GOOGLE-APPENGINE • GOOGLE-DOCS-DRAWING • GOOGLE-CLASSROOM • GOOGLE-PAY • GOOGLE-TRUSTED-STORE • GOOGLE-MAPS • GOOGLE-CACHE • GOOGLE • GOOGLE-GROUPS-POST

Table 260: Secure Edge Policy—Dependent Applications for CASB Supported Cloud Applications
(Continued)

CASB Supported Cloud Applications	Dependent Applications When Configuring Secure Edge Policy	
	<ul style="list-style-type: none"> • GOOGLE-ADS • GOOGLE-PHOTOS • GOOGLE-BOOKS • GOOGLE-SAFEBROWSE-UPDATE • GOOGLE-TAGS • GOOGLE-MESSAGES • GOOGLE-DOCS-FORM • GOOGLE-ANALYTICS-TRACKING • GOOGLE-TOOLBAR • GOOGLE-UPDATE • GOOGLE-WEBCHAT • GOOGLEBOT • GOOGLE-STADIA • YOUTUBE-MUSIC 	<ul style="list-style-type: none"> • GOOGLE-PLAY-MUSIC • GOOGLE-LOCALGUIDES • ANDROID-MARKETPLACE-DOWNLOAD • GMAIL • GMAIL-BASIC • GMAIL-DRIVE • GMAIL-MOBILE • GCP

Table 260: Secure Edge Policy—Dependent Applications for CASB Supported Cloud Applications (Continued)

CASB Supported Cloud Applications	Dependent Applications When Configuring Secure Edge Policy	
Microsoft OneDrive and SharePoint	<ul style="list-style-type: none"> • MICROSOFT • MICROSOFT-EXCHANGE • MICROSOFT-LIVE-SERVICES • MICROSOFT-LYNC • MICROSOFT-UPDATE • OFFICE365-CREATE-CONVERSATION • OFFICE-DOCS 	<ul style="list-style-type: none"> • ONEDRIVE • SHAREPOINT • SHAREPOINT-ADMIN • SHAREPOINT-BLOG • SHAREPOINT-CALENDAR • SHAREPOINT-DOCUMENT • SHAREPOINT-ONLINE
Slack	SLACK	

To create a new CASB profile:

1. Select *Secure Edge* > *Security Subscriptions* > *CASB* > *CASB Profiles*.

The CASB Profiles page opens.

2. Click + to create a CASB profile.

The Create CASB Profile page opens.

3. Complete the configuration according to the guidelines provided in [Table 261 on page 730](#).

4. Click *OK*.

Table 261: Fields on the Create CASB Profile Page

Setting	Guideline
Name	Enter a unique string of alphanumeric characters; special characters other than -_!@\$&*~: are not allowed. No spaces are allowed; maximum length is 29 characters.

Table 261: Fields on the Create CASB Profile Page *(Continued)*

Setting	Guideline
Activity logging	<p>Define activity logging for the CASB profile. For example, Login, Download, and Chat.</p> <p>By default, all the options are selected.</p>

RELATED DOCUMENTATION

[About the CASB Profiles Page | 724](#)

[Edit and Delete a CASB Profile | 731](#)

[Add Rules to a CASB Profile | 735](#)

[Edit and Delete a CASB Rule | 739](#)

Edit and Delete a CASB Profile

IN THIS SECTION

- [Edit a CASB Profile | 731](#)
- [Delete a CASB Profile | 732](#)

You can edit and delete CASB profiles from the CASB page. This topic has the following sections:

Edit a CASB Profile

To edit a CASB profile:

1. Select **Secure Edge > Security Subscriptions > CASB > CASB Profiles**.

The CASB Profiles page opens.

2. Select an existing CASB profile to edit and click the pencil icon.

The Edit CASB Profile page opens.

3. Edit the CASB profile fields.
4. Click **OK** to save your changes.

The CASB Profiles page displays a confirmation message indicating the status of the edit operation.

Delete a CASB Profile

To delete a CASB profile:

1. Select **Secure Edge > Security Subscriptions > CASB > CASB Profiles**.

The CASB Profiles page opens.

2. Select an existing CASB profile to delete and click the delete icon.

A message asking you to confirm the delete operation is displayed.

3. Click **Yes** to delete the CASB profile.

A confirmation message is displayed indicating the status of the delete operation.

RELATED DOCUMENTATION

[About the CASB Profiles Page | 724](#)

[Create a CASB Profile | 726](#)

[Add Rules to a CASB Profile | 735](#)

[Edit and Delete a CASB Rule | 739](#)

About the CASB Rules Page

IN THIS SECTION

- [Default Rule Settings | 733](#)
- [Common Operations on a CASB Rule | 733](#)
- [Add, Edit, and Delete a CASB Profile Rule | 734](#)
- [Add and Hide Advanced Filter | 734](#)

You must configure Cloud Access Security Broker (CASB) rules to control specific actions on each cloud application to secure your data. After you assign the CASB profile to a Secure Edge policy, the profile ensures that the traffic flows between cloud providers and organizational users (either on-premises or roaming) complies with the Secure Edge policy.

Default Rule Settings

To configure default rule settings for the CASB profile:

1. Select **Secure Edge > Security Subscriptions > CASB > CASB Profiles**.

The CASB Profiles page opens.

2. Click **Add Rules** or on the rule number available next to the column of your CASB profile name.

The CASB rules page opens.

3. Click **Default Rule Settings**.

The Default Rule Settings window opens.

4. Select the **Permit** or **Deny** actions to control the application actions when no rule matches the traffic for a CASB profile. By default, Permit is selected.

5. Enable or disable **Action logging** for the CASB profile rule.

6. Click **OK**.

Common Operations on a CASB Rule

To perform common operations on a CASB rule from the CASB Rules page:

1. On the CASB Profiles page, click **Add Rules** or on the rule number available next to the column of your CASB profile name.

The CASB Rules page opens.

2. Select an existing CASB rule and click **More**.

The list shows common operations for a CASB rule.

3. Complete the configuration according to the guidelines provided in [Table 262 on page 734](#).

Table 262: Common Operations on the CASB Rules Page

Field	Description
Add Rule Before	Add a rule before an existing rule.
Add Rule After	Add a rule after an existing rule.
Clone	Create a copy of an existing rule.
Move	Move the rule by selecting one of the following options: <ul style="list-style-type: none"> • Move Top • Move Up • Move Down • Move Bottom
Clear All Selections	Clear the selections for the rules.

Add, Edit, and Delete a CASB Profile Rule

For information on adding, editing, and deleting a CASB profile rule, see ["Edit and Delete a CASB Rule" on page 739](#) and ["Add Rules to a CASB Profile" on page 735](#) .

Add and Hide Advanced Filter

To add filters:

1. Click the filter icon and then select **Show advanced filter**.

The Add Criteria window opens.

2. Select the values for Field and Condition from the list.
3. Enter the value for the selected field and conditions.
4. Click **Add**.

5. Click **Save**.

The Save Filter page opens.

6. Enter a filter name. If you want to make this saved filter as default, then enable **Set as default**.

The filter is saved.

NOTE: Click **X** to clear the saved filters.

7. Click **Close** once the successful message is displayed.

To hide a filter, click the filter icon and then select **Hide advanced filter**.

Add Rules to a CASB Profile

Configure rules for a Cloud Access Security Broker (CASB) profile to control specific actions that can be performed on each cloud application. Once you create the rules, associate the CASB profile with a Secure Edge policy. You can edit, delete, or clone a CASB profile rule. For more information on the common operations that you can perform on the CASB Rules Page, see ["About the CASB Rules Page" on page 732](#).

[Table 263 on page 735](#) lists the Juniper Secure Edge supported cloud applications and their activities.

Table 263: Juniper Secure Edge Supported Cloud Applications and their Activities

Cloud Application	Supported Activities
Box	Login, Upload, Download, and Share
Dropbox	Login, Upload, Download, and Share
Gmail	Login, Read, Compose, Send, Upload Attachment, and Download Attachment
Google Docs	Login, Upload, Download, and Share
Microsoft OneDrive	Login, Upload, Download, and Share

Table 263: Juniper Secure Edge Supported Cloud Applications and their Activities (Continued)

Cloud Application	Supported Activities
Salesforce	Login, Upload, Download, and Share
SharePoint	Login, Upload, Download, and Share
Slack	Login, Chat, Audio/Video, and FileTransfer

To add a rule to a CASB profile:

1. Select **Secure Edge > Security Subscriptions > CASB > CASB Profiles**.
The CASB Profiles page opens.
2. Click **+** to create a CASB profile.
The Create CASB Profile page opens.
3. Click **Add Rules** or on the rule number available next to the column of your CASB profile name.
The CASB Rules page opens.
4. Complete the configuration according to the guidelines provided in [Table 264 on page 736](#).
5. Click the tick icon on the right-side of the row once done with the configuration.
After you create the rules, assign the associated CASB profile with a Secure Edge policy.

Table 264: Fields on the CASB Rules Page

Setting	Guideline
Seq	Displays the rule number order.
Name	Enter a rule name. Name must begin with an alphanumeric character; colons, periods, slashes, dashes, and underscores are allowed; cannot exceed 29 characters.

Table 264: Fields on the CASB Rules Page (Continued)

Setting	Guideline
Cloud Applications	<p>a. Click + to configure rules to control access to the cloud applications for the CASB profile.</p> <p>The Cloud Applications window appears.</p> <p>b. Enter the following details:</p> <ul style="list-style-type: none"> • Cloud application group—Select Any to match all cloud application groups or select File Sharing to control data sharing permissions. • Cloud applications—Select Any to match all cloud applications or select Specific to choose one or more cloud applications from the list for the CASB profile rule. For example, Box, Dropbox, or Salesforce.
Application Instance	<p>a. Click + to configure the application instance for the CASB profile.</p> <p>The Application Instance window appears.</p> <p>b. Application instance names—Select an application instance from the list.</p> <p>To add a new instance, click Create application instance. For more information on the fields, see "Create an Application Instance" on page 742 .</p> <p>c. Click OK.</p>

Table 264: Fields on the CASB Rules Page (Continued)

Setting	Guideline
Activities	<p>a. Click + to configure the activities for the CASB profile.</p> <p>The Activities window appears.</p> <p>b. Activities—Select Any to match all the activities. To add a specific activity, click Specific and then select the respective activity.</p> <p>c. Share—Select one or more domain names from the list and then click the right arrow.</p> <p>To add a new name:</p> <p>i. Click +.</p> <p>The Add Share window appears.</p> <p>ii. Enter a domain name (for example, yahoo.com).</p> <p>The name must begin with an alphanumeric character. Spaces and special characters except for - : . are not allowed. The maximum length is 63 characters.</p> <p>iii. Click OK.</p> <p>d. To move an existing domain name, select the domain name and use the right arrow to move it to next column.</p> <p>e. Click OK.</p>
Action	Select Deny or Permit to take an action when traffic matches the criteria.
Options	Enable or disable the activity logging option.

RELATED DOCUMENTATION

[Edit and Delete a CASB Rule | 739](#)

[About the CASB Profiles Page | 724](#)

[Create a CASB Profile | 726](#)

[Edit and Delete a CASB Profile | 731](#)

Edit and Delete a CASB Rule

IN THIS SECTION

- [Edit a CASB Rule | 739](#)
- [Delete a CASB Rule | 739](#)

You can edit and delete CASB rules from the CASB Rules page. This topic has the following sections:

Edit a CASB Rule

To edit a CASB rule:

1. Select **Secure Edge > Security Subscriptions > CASB > CASB Profiles**.

The CASB Profiles page opens.

2. Click **Add Rules** or on the rule number available next to the column of the CASB profile name.

The CASB Rules page opens.

3. Select an existing CASB rule to edit and click the pencil icon.

4. Edit the CASB rule fields.

5. Click the tick icon on the right-side of the row once done with the configuration.

The CASB Rule page displays a confirmation message indicating the status of the edit operation.

Delete a CASB Rule

To delete a CASB rule:

1. Select **Secure Edge > Security Subscriptions > CASB > CASB Profiles**.

The CASB Profiles page opens.

2. Click **Add Rules** or on the rule number available next to the column of the CASB profile name.

The CASB Rules page opens.

3. Select an existing CASB rule to delete and click the delete icon.

A message asking you to confirm the delete operation is displayed.

4. Click **Yes** to delete the CASB profile.

A confirmation message indicating the status of the delete operation is displayed.

RELATED DOCUMENTATION

[Add Rules to a CASB Profile | 735](#)

[About the CASB Profiles Page | 724](#)

[Create a CASB Profile | 726](#)

[Edit and Delete a CASB Profile | 731](#)

About the Application Instances Page

IN THIS SECTION

- [Tasks You Can Perform | 741](#)
- [Field Descriptions | 741](#)

To access this page, select **Secure Edge > Security Subscriptions > CASB > Application Instances**.

When an organization supports Software as a Service (SaaS) applications, the following are the requirements:

- You must need access to the SaaS applications using your corporate email IDs. This helps you in accessing all the subscribed application services

- You must need a unique URL that organization users or external users (for example, third party partners) can use to access data based on permissions. As Dropbox and Google Docs are generic URLs, you do not need a unique URL.

To differentiate between corporate and non-corporate SaaS application instances, administrators need to configure access policies using the instance parameter. Use the Application Instances page to configure the application instance for a CASB profile.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create an application instance. See ["Create an Application Instance" on page 742](#) .
- Edit or delete an application instance. See ["Edit and Delete an Application Instance" on page 745](#) .
- Search for an application instance. Click the search icon in the top-right corner of the page. You can enter partial text or full text of the keyword in the text box, and press Enter. The search results are displayed on the same page.
- Filter rules—Click the filter icon (funnel) and specify one or more filtering criteria. The filtered results are displayed on the same page.

NOTE: Filtering is applicable only to some fields.

- Show or hide columns. Click the Show/Hide Columns icon at the top right corner of the page.

Field Descriptions

[Table 265 on page 741](#) describes the fields on the Application Instances page.

Table 265: Application Instances Fields

Field	Description
Name	Displays the application instance name.
Application Instance ID	Displays the application instance ID.
Domain	Displays the user login domain for the application.

Table 265: Application Instances Fields (Continued)

Field	Description
Type	Displays if the cloud application access type is unclassified, work, or personal.
Tag	Displays if the application instance is untagged, sanctioned, or unsanctioned.

RELATED DOCUMENTATION

[CASB Overview](#) | 722

Create an Application Instance

For CASB, to differentiate between corporate and non-corporate SaaS application instances, administrators need to configure access policies using the instance parameter. To identify an instance, CASB requires instance ID, domain, and/or type. And, to monitor logs, tagging that are mapped with instances is used.

Use the Create Application Instance Page to configure application instances.

To create a new application instance:

1. Select **Secure Edge > Security Subscriptions > CASB > Application Instances**.

The Application Instances page opens.

2. Click **+** to create an application instance.

The Create Application Instance page.

3. Complete the configuration according to the guidelines provided in [Table 266 on page 743](#).

4. Click **OK**.

An application instance is created, which you can associate with a CASB profile.

Table 266: Creating Application Instance Settings

Setting	Guideline
Name	<p>Enter a new application instance name. For example, dropbox123.</p> <p>The instance name must begin with an alphanumeric character. Spaces and special characters except for - : . are not allowed. The maximum length is 63 characters.</p>
Application instance ID	<p>A unique URL to access SaaS service. Instance ID comes in packet data of all SaaS application activities, such as, upload, download, and share. You use this Instance ID to apply in the Security policies.</p> <p>Enter an application instance ID.</p> <p>Each application can have its own instance ID. For the following example URLs, consider a common string acmecorp07 as the instance ID within the application's SaaS URLs:</p> <ul style="list-style-type: none"> • Box URL—acmecorp07.app.box.com • Microsoft OneDrive or SharePoint URL—acmecorp07ms-my.sharepoint.com • Salesforce URLs: <ul style="list-style-type: none"> • acmecorp07.my.salesforce.com • acmecorp07.lightning.force.com <p>For example, Slack URL is acmecorp-zoy8730.slack.com for the instance ID acmecorp-zoy8730.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • Dropbox URL is dropbox.com • Google Docs URL is docs.google.com • Gmail URL is mail.google.com <p>As these are generic URLs, instance ID is not applicable.</p>

Table 266: Creating Application Instance Settings (Continued)

Setting	Guideline
Domain	<p>An email domain. During login activity, you get an email domain in packets, and it is part of instance.</p> <p>Enter the domain address.</p> <p>For example, acmecorp07.com is an organization domain. Then, Box, Dropbox, Google Docs, Salesforce, Microsoft OneDrive, Sharepoint, Gmail, and Slack uses the same domain for all the users.</p>
Type	<p>Select a value from the list to map a type with an application instance:</p> <ul style="list-style-type: none"> • Unclassified • Work • Personal <p>NOTE: You must configure the type of value for Dropbox. For other applications, this configuration is optional.</p>
Tag	<p>Select a value from the list to map a tagging with an application instance:</p> <ul style="list-style-type: none"> • Untagged—Default value for the application instances that you have not tagged. • Sanctioned—Application instances sanctioned by your organization. • Unsanctioned—Application instances unsanctioned by your organization.

RELATED DOCUMENTATION

[Edit and Delete an Application Instance | 745](#)

[About the Application Instances Page | 740](#)

Edit and Delete an Application Instance

IN THIS SECTION

- [Edit an Application Instance | 745](#)
- [Delete an Application Instance | 745](#)

You can edit and delete application instances for CASB profiles from the Application Instance page. This topic has the following sections:

Edit an Application Instance

To edit an application instance:

1. Select **Secure Edge > Security Subscriptions > CASB > Application Instances**.

The Application Instances page opens.

2. Select an existing application instance to edit and click the pencil icon.

The Edit Application Instance page opens.

3. Edit the application instance fields.

4. Click **OK** to save your changes.

The Application Instances page displays a confirmation message indicating the status of the edit operation.

Delete an Application Instance

To delete an application instance:

1. Select **Secure Edge > Security Subscriptions > CASB > Application Instances**.

The Application Instances page opens.

2. Select an existing application instance to delete and click the delete icon.

A message asking you to confirm the delete operation is displayed.

3. Click **Yes** to delete the application instance.

A confirmation message is displayed indicating the status of the delete operation.

RELATED DOCUMENTATION

[About the Application Instances Page | 740](#)

[Create an Application Instance | 742](#)

About the Application Tagging Page

IN THIS SECTION

- [Field Descriptions | 746](#)

To access this page, select **Secure Edge > Security Subscriptions > CASB > Application Tagging**.

Use application instance tagging for a CASB profile to reflect whether or not your organization approves the cloud application. By default, all the application instances are tagged as **Untagged**.

Field Descriptions

[Table 267 on page 746](#) describes the fields on the Application Tagging page.

Table 267: Application Tagging Fields

Field	Description
Application Name	Displays the cloud application name for which you are tagging the instance.

Table 267: Application Tagging Fields (*Continued*)

Field	Description
Application Tag	<p>Select one of the options to tag an application instance for a CASB profile:</p> <ul style="list-style-type: none"> • Untagged—Default value for the application instances that you have not tagged. • Sanctioned—Application instances sanctioned by your organization. • Unsanctioned—Application instances unsanctioned by your organization.

RELATED DOCUMENTATION

[About the CASB Profiles Page | 724](#)

Content Filtering Policies Overview

Content filtering policies determine the file type based on the file content and not based on the file extensions. The content filtering policies analyze the file content to accurately determine the file type. Juniper Secure Edge filters the content based on the file type, application, and direction.

NOTE: The content filtering policy evaluates traffic before all other content security policies. Therefore, if traffic meets criteria configured in the content filter, the content filter acts first upon this traffic.

About the Content Filtering Policies Page

IN THIS SECTION

- [Tasks You Can Perform | 748](#)
- [Field Descriptions | 749](#)

To access this page, select **Secure Edge >Security Subscriptions > Content Filtering**. Use the Content Filtering Policies page to view and to manage content filtering policies.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a content filtering policy—See "[Create a Content Filtering Policy](#)" on page 749 .
- Edit and delete a content filtering policy—See "[Edit and Delete a Content Filtering Policy](#)" on page 751 .
- Edit, clone, or delete a content filtering policy rule—See "[Edit, Clone, and Delete a Content Filtering Policy Rule](#)" on page 752 .
- Search for content filtering policies by using keywords and policy name—Click the search icon, enter the search term in the text box, and press Enter. The search results are displayed on the same page.
- Filter rules—Click the filter icon (funnel), and specify one or more filtering criteria. The filtered results are displayed on the same page.
- Filter information based on select criteria. You can add filters, save the filters, and set any of the filters as default. To add a filter:
 1. Click the filter icon on the top-right corner of the page, and select **Add Filter** to open the Add Criteria page.
 2. Set the filter conditions, and click **Add**.

The filter is saved and applied on the data.

To remove the filter, click the filter icon, and select Hide Filter.

Field Descriptions

Table 268 on page 749 describes the fields on the Content Filtering Policies page.

Table 268: Fields on the Content Filtering Policies Page

Field	Description
Name	The name of the content filtering policy.
Rules	The number of rules associated with the content filtering policy.
Description	The description of the content filtering policy.

Create a Content Filtering Policy

Use the Create Content Filtering Policies page to configure content filtering policies.

1. Select **Secure Edge > Security Subscriptions > Content Filtering**.
The Content Filtering Policies page opens.
2. Click **+** to create a content filtering policy.
The Create Content Filtering Policy page opens.
3. Complete the configuration according to the guidelines provided in [Table 269 on page 749](#).
4. Click **OK**.

Table 269: Fields on the Content Filtering Policies Page

Setting	Guideline
Name	Enter a unique name containing maximum 29 characters for the content filtering policy.
Description	Enter a description containing maximum 255 characters for the content filtering policy.

The Content Filtering Policies page opens displaying the new content filtering policy.

Next, add rules to the content filtering policy.

Add Rules in a Content Filtering Policy

1. Select **Secure Edge > Security Subscriptions > Content Filtering**.

The Content Filtering Policies page opens.

2. Click the content filtering policy to which you want to add the rule.

The *Content-Filtering-Policy-Name* page opens.

3. Click **+**, and complete the configuration according to the guidelines provided in [Table 270 on page 750](#).

4. Click **✓**.

Table 270: Fields on the Content Filtering Policy Rule Page

Setting	Guideline
Name	Enter a unique name containing maximum 29 characters for the content filtering rule.
Direction	Select the direction of the content traffic to filter. <ul style="list-style-type: none"> • Any • Download • Upload
File Types	Click + to open the Files Types page, and select the types of files to filter.

Table 270: Fields on the Content Filtering Policy Rule Page *(Continued)*

Setting	Guideline
Action	<p>Select the action to be taken on the selected types of files in the content filtering rule.</p> <ul style="list-style-type: none"> • No Action • Block • Close Client • Close Server • Close Client and Server
Options	<p>Do the following:</p> <ul style="list-style-type: none"> • Click the Event logs toggle button to enable logging for the content filter. • Click the End user notification toggle button to enable notifications to users, and enter a custom notification message containing maximum 512 characters.

Edit and Delete a Content Filtering Policy

IN THIS SECTION

- [Edit a Content Filtering Policy | 751](#)
- [Delete a Content Filtering Policy | 752](#)

Edit a Content Filtering Policy

You cannot modify the default policies.

1. Select **Secure Edge>Security Subscriptions>Content Filtering**.

The Content Filtering Policies page opens displaying the existing content filtering policies.

2. Select the custom content filtering policy to edit, and click the pencil icon.

The Edit Content Filtering Policies page opens.

3. Edit the content filtering policy fields.

4. Click **OK** to save your changes.

The Content Filtering Policies page opens with a confirmation message indicating the status of the edit operation.

Delete a Content Filtering Policy

Before deleting a content filtering policy, ensure that the policy is not used in a Content Security profile, which is used in a firewall policy rule. If you try to delete a content filtering policy that is used in a firewall policy rule, an error message is displayed.

1. Select **Secure Edge>Security Subscriptions>Content Filtering**.

The Content Filtering Policies page opens displaying the existing content filtering policies.

2. Select the custom content filtering policies to delete, and click the delete icon.

A message asking you to confirm the delete operation is displayed.

3. Click **Yes** to delete the selected content filtering policies.

A confirmation message indicating the status of the delete operation is displayed.

Edit, Clone, and Delete a Content Filtering Policy Rule

IN THIS SECTION

- [Edit a Content Filtering Policy Rule | 753](#)
- [Clone a Secure Edge Policy Rule | 753](#)
- [Delete a Secure Edge Policy Rule | 753](#)

You can edit, clone, and delete content filtering policy rules from the **Secure Edge > Security Subscriptions > Content Filtering** page.

Edit a Content Filtering Policy Rule

1. Select **Secure Edge > Security Subscriptions > Content Filtering**.

The Content Filtering Policies page opens displaying the list of content filtering policies.

2. Click the content filtering policy name.

The content filtering policy page opens displaying the list of rules included in the policy.

3. Select the content filtering policy rule, and click the pencil icon.

4. Modify the parameters, and click ✓ to save the changes.

The content filtering policy page displays the modified rule.

Clone a Secure Edge Policy Rule

1. Select **Secure Edge > Security Subscriptions > Content Filtering**.

The Content Filtering Policies page opens displaying the list of content filtering policies.

2. Click the content filtering policy name.

The content filtering policy page opens displaying the list of rules included in the policy.

3. Select the content filtering policy rule, and click **More > Clone**.

The content filtering policy page displays the cloned rule.

4. Update the cloned content filtering policy rule as required.

5. Click ✓ to save the changes.

The content filtering policy page displays the modified rule.

Delete a Secure Edge Policy Rule

1. Select **Secure Edge > Security Subscriptions > Content Filtering**.

The **Content Filtering Policies** page opens displaying the list of content filtering policies.

2. Click the content filtering policy name.

The content filtering policy page opens displaying the list of rules included in the policy.

3. Select the content filtering policy rule, and click the delete icon.

An alert message asking you to confirm the delete operation is displayed.

4. Click **Yes** to delete the selected policy rule.

SecIntel Profiles Overview

Juniper Networks Security Intelligence (SecIntel) provides carefully curated and verified threat intelligence from industry-leading threat feeds to Juniper Secure Edge. This enables blocking malicious and unwanted traffic such as Command and Control (C&C) communications, GeolIP, Attacker IPs, and more with minimum latency. SecIntel delivers real-time threat intelligence by enabling automatic and responsive traffic filtering.

Configure SecIntel profiles to work with security intelligence feeds, such as C&C, DNS, and infected hosts. The Security Intelligence process is responsible for downloading the security intelligence feeds and parsing from the feed connector or ATP Cloud feed server. Anything that matches these scores is considered malware or an infected host.

About SecIntel Profiles

IN THIS SECTION

- [Tasks You Can Perform | 754](#)
- [Field Description | 755](#)

To access this page, select **Secure Edge** > **Security Subscriptions** > **SecIntel** > **Profiles**.

Use the SecIntel Profiles page to manage Command & Control (C&C), DNS, and Infected Hosts profile.

Tasks You Can Perform

You can perform the following tasks from this page:

- View the list of C&C, DNS, and infected hosts profiles. To do this, click **View by** list and select Command & Control, DNS, or Infected Hosts profile.
- Create a command and control profile—See "[Create Command and Control Profile](#)" on page 755 .
- Create a DNS profile—See "[Create DNS Profile](#)" on page 757 .
- Create an infected hosts profile—See "[Create Infected Hosts Profile](#)" on page 759 .
- Edit, clone, or delete SecIntel profile—See "[Edit, Clone, and Delete SecIntel Profile](#)" on page 761 .
- Show or hide columns in the SecIntel 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.
- Reset Preference—Reset the displayed columns to the default set of columns for each tab in the table.

Hover over the More Options (vertical ellipsis) and select **Reset Preference**.

Field Description

Table 271 on page 755 describes the fields on the SecIntel Profiles page.

Table 271: Fields on the SecIntel Profiles Page

Field	Description
Name	Displays the SecIntel profile name.
Type	Displays if the SecIntel profile is a C&C, a DNS, or an infected hosts profile.
Block action	Displays the notification action taken with the block action. For example, Close session, Drop packet, and Sinkhole.
Description	Displays the description of the SecIntel profile.

Create Command and Control Profile

Create a Command and Control (C&C) profile to provide information on C&C servers that have attempted to contact and compromise hosts on your network. A C&C server is a centralized computer that issues commands to botnets of compromised networks of computers and receives reports back from them.

To create a C&C profile:

1. Click **Secure Edge > Security Subscriptions > SecIntel > Profiles**.
The SecIntel Profiles page opens.
2. Select **Create > Command & Control**.
The Create Command & Control Profile page appears.
3. Complete the configuration according to the guidelines provided in [Table 272 on page 756](#).
4. Click **OK** to save the changes. To discard your changes, click **Cancel**.

Once you create the C&C profile, you can associate it with the SecIntel profile groups.

Table 272: Fields on the Create Command & Control Profile page

Field	Action
Name	<p>Enter a name for the C&C profile.</p> <p>The name must be a unique string of alphanumeric and special characters; 63-character maximum. Special characters < and > are not allowed.</p>
Description	Enter a description for the C&C profile.
Default action for all feeds	<p>Drag the slider to change the action to be taken for all the feed types. Actions are Permit (1 - 4), Log (5-6), and Block (7 - 10).</p> <p>Log will have the permit action and also logs the event.</p>
Specific action for feeds	<p>Do the following:</p> <ol style="list-style-type: none"> a. Click + to define feeds and threat score for the C&C profile. <ul style="list-style-type: none"> The Add Feeds window appears. b. Enter the following details: <ol style="list-style-type: none"> i. Feeds—Select one or more feeds that are known command and control for botnets from the Available column and move it to the Selected column. ii. Threat score—Drag the slider to change the action to be taken based on the threat score. c. Click OK.

Table 272: Fields on the Create Command & Control Profile page (Continued)

Field	Action
Block action	<p>Select one of the following block actions from the list:</p> <ul style="list-style-type: none"> • Drop Packets—Device silently drops the session's packet and the session eventually times out. • Close session options—Device sends a TCP RST packet to the client and server and the session is dropped immediately.
Close session options	Select one of the following options from the list: None, Redirect URL, or Redirect message.
Redirect URL	Enter a remote file URL to redirect users when connections are closed.
Redirect message	Enter a custom message to send to the users when connections are closed.

Create DNS Profile

Create a DNS profile to configure feeds and threat score to list the domains that are known to be connected to malicious activity.

To create a DNS profile:

1. Click **Secure Edge > Security Subscriptions > SecIntel > Profiles**.
The SecIntel Profiles page appears.
2. Select **Create > DNS**.
The Create DNS Profile page appears.
3. Complete the configuration according to the guidelines provided in [Table 273 on page 758](#).
4. Click **OK** to save the changes. To discard your changes, click **Cancel**.
Once you create the DNS profile, you can associate it with the SecIntel profile groups.

Table 273: Fields on the Create DNS Profile Page

Field	Action
Name	<p>Enter a name for the DNS profile.</p> <p>The name must be a unique string of alphanumeric and special characters; 63-character maximum. Special characters such as < and > are not allowed.</p>
Description	<p>Enter a description for the DNS profile.</p>
Default action for all feeds	<p>Drag the slider to change the action to be taken for all the feed types. Actions are Permit (1 - 4), Log (5-6), and Block (7 - 10).</p> <p>Log will have the permit action and also logs the event.</p>
Specific action for feeds	<p>Do the following:</p> <ol style="list-style-type: none"> a. Click + to define feeds and threat score to the DNS profile. <ul style="list-style-type: none"> The Add Feeds window appears. b. Enter the following details: <ol style="list-style-type: none"> i. Feeds—Select one or more feeds from the Available column and move it to the Selected column to associate with the DNS profile. ii. Threat score—Drag the slider to change the action to be taken based on the threat score. c. Click OK.

Table 273: Fields on the Create DNS Profile Page (*Continued*)

Field	Action
Block action	<p>Select one of the following block actions from the list:</p> <ul style="list-style-type: none"> • Drop Packets—Device silently drops the session’s packet and the session eventually times out. • Sinkhole—DNS sinkhole action for malicious DNS queries.

Create Infected Hosts Profile

Create an Infected Hosts profile to configure feeds and threat score to list the IP address or IP subnet of the compromised host. Infected hosts indicate local devices that are potentially compromised because they appear to be part of a C&C network or exhibit other symptoms.

To create an Infected Hosts profile:

1. Click **Secure Edge > Security Subscriptions > SecIntel > Profiles**.
The SecIntel Profiles page appears.
2. Select **Create > Infected Hosts**.
The Create Infected Hosts Profile page appears.
3. Complete the configuration according to the guidelines provided in [Table 274 on page 759](#).
4. Click **OK** to save the changes. To discard your changes, click **Cancel**.

Once you create the Infected Hosts profile, you can associate it with the SecIntel profile groups.

Table 274: Fields on the Create Infected Hosts Profile Page

Field	Action
Name	<p>Enter a name for the Infected Hosts profile.</p> <p>The name must be a unique string of alphanumeric and special characters; 63-character maximum. Special characters such as < and > are not allowed.</p>

Table 274: Fields on the Create Infected Hosts Profile Page (*Continued*)

Field	Action
Description	Enter a description for the Infected Hosts profile.
Default action for all feeds	<p>Drag the slider to change the action to be taken for all the feed types. Actions are Permit (1 - 4), Log (5-6), and Block (7 - 10).</p> <p>Log will have the permit action and also logs the event.</p>
Specific action for feeds	<p>Do the following:</p> <ol style="list-style-type: none"> a. Click + to define feeds and threat score to the Infected Hosts profile. The Add Feeds window appears. b. Enter the following details: <ol style="list-style-type: none"> i. Feeds—Select one or more feeds from the Available column and move it to the Selected column to associate with the Infected Hosts profile. ii. Threat score—Drag the slider to change the action to be taken based on the threat score. c. Click OK.
Block action	<p>Select one of the following block actions from the list:</p> <ul style="list-style-type: none"> • Drop Packets—Device silently drops the session's packet and the session eventually times out. • Close session options—Device sends a TCP RST packet to the client and server and the session is dropped immediately.
Close session options	<p>Select one of the following options from the list: None, Redirect URL, or Redirect message.</p>

Table 274: Fields on the Create Infected Hosts Profile Page (*Continued*)

Field	Action
Redirect URL	Enter a remote file URL to redirect users when connections are closed.
Redirect message	Enter a custom message to send to the users when connections are closed.

Edit, Clone, and Delete SecIntel Profile

IN THIS SECTION

- [Edit a SecIntel Profile | 761](#)
- [Clone a SecIntel Profile | 762](#)
- [Delete a SecIntel Profile | 762](#)

Edit a SecIntel Profile

To edit a SecIntel profile:

1. Select **Secure Edge > Security Subscriptions > SecIntel > Profiles**.
The SecIntel Profiles page appears.
2. Select a profile, and click the edit (pencil) icon.
The Edit Profile page appears.
3. Modify the profile fields. See "[Create Command and Control Profile](#)" on page 755 , "[Create DNS Profile](#)" on page 757 , or "[Create Infected Hosts Profile](#)" on page 759 .
4. Click **OK** to save your changes.

The SecIntel Profiles page opens with a message that the profile was successfully updated.

If the SecIntel profile is referenced in a firewall policy intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.

Clone a SecIntel Profile

Cloning enables you to easily create a new SecIntel profile based on an existing one. You can clone a SecIntel profile and modify the parameters.

To clone a SecIntel profile:

1. Select **Secure Edge > Security Subscriptions > SecIntel > Profiles**.

The SecIntel Profiles page appears.

2. Select a profile and select **More > Clone**.

The Clone Profile page appears.

3. Modify the profile fields. See "[Create Command and Control Profile](#)" on page 755 , "[Create DNS Profile](#)" on page 757 , or "[Create Infected Hosts Profile](#)" on page 759 .

4. Click **OK** to save your changes.

The SecIntel Profiles page opens with a message that the IPS profile was successfully created.

Delete a SecIntel Profile

To delete a SecIntel profile:

1. Select **Secure Edge > Security Subscriptions > SecIntel > Profiles**.

The SecIntel Profiles page appears.

2. Select one or more SecIntel profiles, and click the delete (trash can) icon.

A warning message asking you to confirm the deletion is displayed.

3. Click **Yes** to proceed with the deletion.

The SecIntel Profiles page opens with a message indicating the status of the delete operation.

About SecIntel Profile Groups

IN THIS SECTION

● [Tasks You Can Perform | 763](#)

● [Field Description | 763](#)

To access this page, select **Secure Edge > Security Subscriptions > SecIntel > Profile Groups**.

Configure a SecIntel profile group to add SecIntel profiles, such as C&C, DNS, and infected hosts. Once created, you can assign this group to the security policy.

Use the SecIntel Profiles page to manage SecIntel profile groups.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a SecIntel profile group—See ["Create SecIntel Profile Group" on page 764](#) .
- Edit, clone, or delete SecIntel profile group—See ["Edit, Clone, and Delete SecIntel Profile Group" on page 765](#) .
- Show or hide columns in the SecIntel 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.
- Reset Preference—Reset the displayed columns to the default set of columns for each tab in the table.

Hover over the More Options (vertical ellipsis) and select **Reset Preference**.

Field Description

[Table 275 on page 763](#) describes the fields on the SecIntel Profiles page.

Table 275: Fields on the SecIntel Profile Groups Page

Field	Description
Name	Displays the SecIntel profile group name.
Command & Control	Displays the C&C profile that you have associated with the SecIntel profile group.
DNS	Displays the DNS profile that you have associated with the SecIntel profile group.
Infected Hosts	Displays the infected hosts profile that you have associated with the SecIntel profile group.
Description	Displays the description of the SecIntel profile group.

Create SecIntel Profile Group

Create a SecIntel profile group with SecIntel profiles, such as C&C, DNS, and infected hosts. Once created, you can assign this group to the security policy.

To create a SecIntel profile group:

1. Click **Secure Edge > Security Subscriptions > SecIntel > Profile Groups**.
The SecIntel Profile Groups page appears.
2. Click **+** on the upper-right corner of the SecIntel Profile Groups page.
The Create SecIntel Profile Groups page appears.
3. Complete the configuration according to the guidelines provided in [Table 276 on page 764](#).
4. Click **OK** to save the changes. To discard your changes, click **Cancel**.

Once you create the SecIntel profile group, you can associate it with the security policies.

Table 276: Fields on the Create SecIntel Profile Groups Page

Field	Action
Name	Enter a name for the SecIntel profile group. The name must be a unique string of alphanumeric, special characters and 64-character maximum. Special characters such as & ()] ? " # < > are not allowed.
Description	Enter description for the SecIntel profile group.
Command & Control	Select a C&C profile from the list to associate with the SecIntel profile group. Click Create New to create a new C&C profile inline. For more information on a new C&C profile, see "Create Command and Control Profile" on page 755 .
DNS	Select a DNS profile from the list to associate with the SecIntel profile group. Click Create New to create a new DNS profile inline. For more information on a new DNS profile, see "Create DNS Profile" on page 757 .

Table 276: Fields on the Create SecIntel Profile Groups Page (Continued)

Field	Action
Infected Hosts	<p>Select a infected hosts profile from the list to associate with the SecIntel profile group.</p> <p>Click Create New to create a new infected hosts profile inline. For more information on a new infected hosts profile, see "Create Infected Hosts Profile" on page 759 .</p>

Edit, Clone, and Delete SecIntel Profile Group

IN THIS SECTION

- [Edit a SecIntel Profile Group | 765](#)
- [Clone a SecIntel Profile Group | 766](#)
- [Delete a SecIntel Profile Group | 766](#)

Edit a SecIntel Profile Group

To edit a SecIntel profile group:

1. Select **Secure Edge > Security Subscriptions > SecIntel > Profile Groups**.
The SecIntel Profile Groups page appears.
2. Select a profile group, and click the edit (pencil) icon.
The Edit SecIntel Profile Group page appears.
3. Modify the profile fields. See "[Create SecIntel Profile Group](#)" on [page 764](#) .
4. Click **OK** to save your changes.

The SecIntel Profile Groups page opens with a message that the profile was successfully updated.

If the SecIntel profile group is referenced in a firewall policy intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.

Clone a SecIntel Profile Group

Cloning enables you to easily create a new SecIntel profile group based on an existing one. You can clone a SecIntel profile group and modify the parameters.

To clone a SecIntel profile group:

1. Select **Secure Edge > Security Subscriptions > SecIntel > Profile Groups**.

The SecIntel Profile Groups page appears.

2. Select a SecIntel profile group and select **More > Clone**.

The Create SecIntel Profile Group page appears.

3. Modify the profile fields. See "[Create SecIntel Profile Group](#)" on page 764 .

4. Click **OK** to save your changes.

The SecIntel Profile Groups page opens with a message that the IPS profile was successfully created.

Delete a SecIntel Profile Group

To delete a SecIntel profile group:

1. Select **Secure Edge > Security Subscriptions > SecIntel > Profile Groups**.

The SecIntel Profile Groups page appears.

2. Select one or more SecIntel profile groups, and click the delete (trash can) icon.

A warning message asking you to confirm the deletion is displayed.

3. Click **Yes** to proceed with the deletion.

The SecIntel Profile Groups page opens with a message indicating the status of the delete operation.

Anti-malware Profiles Overview

Juniper Secure Edge uses intelligence provided by Juniper Advanced Threat Prevention Cloud (Juniper ATP Cloud) to remediate malicious content using security policies. If configured, security policies block the content before it is delivered to the destination address.

The anti-malware profile defines the content to scan for any malware and the action to be taken when malware is detected. Juniper ATP Cloud uses a pipeline approach to analyzing and detecting malware. If an analysis reveals that the file is malware, it is not necessary to continue the pipeline to further examine the malware.

About Anti-malware Profiles

IN THIS SECTION

- [Tasks You Can Perform | 767](#)
- [Field Descriptions | 767](#)

To access this page, select **Secure Edge > Security Subscriptions > SecIntel > Antimalware**.

Configure antimalware profile and associate the profile with security policies.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create an anti-malware profile. See "[Create Anti-malware Profile](#)" on page 768 .
- Edit, clone or delete an anti-malware profile. See "[Edit, Clone, and Delete Anti-malware Profile](#)" on page 771 .
- View the configured parameters of an anti-malware profile. Click the details icon that appears when you hover over the name of an address or address group or select **More > Detailed View**.
- Clear the selected anti-malware profile—Click **More > Clear All Selections** to clear any anti-malware profile that you might have selected.
- Show or hide columns in the Anti-malware table. To do this, use the Show Hide Columns icon in the upper-right corner of the page, and select the options to show or deselect to hide options on the page.
- Reset Preference—Reset the displayed columns to the default set of columns for each tab in the table.

Hover over the More Options (vertical ellipsis) and select **Reset Preference**.

Field Descriptions

[Table 277 on page 768](#) describes the fields on the Anti-malware page.

Table 277: Fields on the Anti-malware Page

Field	Description
Name	Displays the anti-malware profile name.
Verdict threshold	Displays the threshold value to determine when a file is considered malware.
HTTP	Displays whether the HTTP protocol is enabled or not.
Logs	Displays whether the additional logs configured are files under verdict threshold, Allowlist, and/or Blocklist.

Create Anti-malware Profile

Configure the anti-malware profiles for Juniper Secure Edge. The profile lets you define which files to send to the ATP cloud for inspection and the action to be taken when malware is detected.

To create an anti-malware profile:

1. Select **Secure Edge > Security Subscriptions > Anti-malware**.
The Anti-malware page appears.
2. Click **+** on the upper-right corner of the Anti-malware page.
The Create Anti-malware Profile page appears.
3. Complete the configuration according to the guidelines provided in [Table 278 on page 769](#).
4. Click **OK** to save the changes. To discard your changes, click **Cancel**.

Once you create the anti-malware profile, you can associate it with the security policies.

Table 278: Fields on the Create Anti-malware Profile Page

Field	Action
Name	<p>Enter a name for the anti-malware profile.</p> <p>The name must be a unique string of alphanumeric, special characters and 64 characters maximum. Special characters such as & ()] ? " # are not allowed.</p>
Verdict threshold	<p>Select a threshold value from the list.</p> <p>The threshold value determines when a file is considered malware. If the cloud service returns a file verdict equal to or higher than the configured threshold, then that file is considered as malware.</p>
Protocols	
HTTP	<p>Enable this option to inspect advanced anti-malware (AAMW) files downloaded by hosts through HTTP protocol. The AAMW files are then submitted to Juniper ATP Cloud for malware screening.</p>
Inspection profile	<p>Select a Juniper Advanced Threat Prevention (ATP) Cloud profile name from the list. The ATP Cloud profile defines the types of files to scan.</p> <p>To view the default and other inspection profiles on Juniper Secure Edge, your device must be enrolled with Juniper ATP Cloud.</p>
Action	<p>Select Permit or Block action from the list based on the known verdict of the detected malware.</p>
Action (unknown verdict)	<p>Select Permit or Block action from the list based on the detected malware having a verdict of "unknown."</p>

Table 278: Fields on the Create Anti-malware Profile Page (*Continued*)

Field	Action
Client Notification	<p>Select one of the following options to permit or block actions based on detected malware:</p> <ul style="list-style-type: none"> • None • Redirect URL—Enter HTTP URL redirection for a customized client notification based on detected malware with the block action. • Redirect message—Enter the message for a customized client notification based on detected malware with the block action. <p>Range: 1 through 1023</p>
Log files that meet verdict threshold	Click the toggle button to create a log entry when attempting to download a file that meets the verdict threshold.
Additional Logging	
Files below verdict threshold	Enable this option to create a log entry when attempting to download a file that is below the verdict threshold.
Blocklist hits	Enable this option to create a log entry when attempting to download a file from a site listed in the blocklist file.
Allowlist hits	Enable this option to create a log entry when attempting to download a file from a site listed in the allowlist file.

Edit, Clone, and Delete Anti-malware Profile

IN THIS SECTION

- [Edit an Anti-malware Profile | 771](#)
- [Clone an Anti-malware Profile | 771](#)
- [Delete an Anti-malware Profile | 772](#)

Edit an Anti-malware Profile

To edit an anti-malware profile:

1. Select **Secure Edge > Security Subscriptions > Anti-malware**.
The Anti-malware page appears.
2. Select an anti-malware profile, and click the edit (pencil) icon.
The Edit Anti-malware Profile page appears.
3. Modify the profile fields. See "[Create Anti-malware Profile](#)" on page 768 .
4. Click **OK** to save your changes.

The Anti-malware Profile page opens with a message that the profile was successfully updated.

If the anti-malware profile is referenced in a firewall policy intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.

Clone an Anti-malware Profile

Cloning enables you to easily create a new anti-malware profile based on an existing one. You can clone an anti-malware profile and modify the parameters.

To clone an anti-malware profile:

1. Select **Secure Edge > Security Subscriptions > Anti-malware**.
The Anti-malware page appears.
2. Select an anti-malware profile and select **More > Clone**.
The Create Anti-malware profile page appears.
3. Modify the profile fields. See "[Create Anti-malware Profile](#)" on page 768 .
4. Click **OK** to save your changes.

The Anti-malware profile page opens with a message that the anti-malware profile was successfully created.

Delete an Anti-malware Profile

To delete an Anti-malware profile:

1. Select **Secure Edge > Security Subscriptions > Anti-malware**.

The Anti-malware page appears.

2. Select one or more anti-malware profile, and click the delete (trash can) icon.

A warning message asking you to confirm the deletion is displayed.

3. Click **Yes** to proceed with the deletion.

The Anti-malware Profile page opens with a message indicating the status of the delete operation.

Create a DNS Security Profile

Create a DNS security profile for Domain Generation Algorithm (DGA) detection and tunnel detection.

1. Select **Secure Edge > Security Subscriptions > DNS Security**.

The DNS Security Profile page opens.

2. Complete the configuration according to the guidelines provided in [Table 279 on page 772](#).

3. Click **Save**.

Table 279: Fields on the DNS Security Profile Page

Setting	Guideline
DGA detection	Enable this option for DNS DGA to generate random domain names that are used as rendezvous points with potential command.
Action	Specify the action that Juniper Secure Edge must perform when malicious traffic is detected. <ul style="list-style-type: none"> • Permit: Permits the tunnel session. • Deny: Drops the tunnel session. • Sinkhole: Drops the tunnel sessions and sinkholes the domain.

Table 279: Fields on the DNS Security Profile Page *(Continued)*

Setting	Guideline
Logs	<p>Select the logging action that Juniper Secure Edge must perform when malicious traffic is detected.</p> <ul style="list-style-type: none"> • Log detections: Generated logs for malicious DNS detections. • Log everything: Generates logs for each DNS request and DNS detection.
Tunnel detection	<p>Enable this option to detect DNS Tunneling which is a cyber-attack method that encodes the data of other programs or protocols in DNS queries and responses. It indicates that DNS traffic is likely to be subverted to transmit data of another protocol or malware beaconing.</p>
Action	<p>Specify the action that Juniper Secure Edge must perform when malicious traffic is detected.</p> <ul style="list-style-type: none"> • Permit: Permits the tunnel session. • Deny: Drops the tunnel session. • Sinkhole: Drops the tunnel sessions and sinkholes the domain.
Logs	<p>Select the logging action that Juniper Secure Edge must perform when malicious traffic is detected.</p> <ul style="list-style-type: none"> • Log detections: Generated logs for malicious DNS detections. • Log everything: Generates logs for each DNS request and DNS detections.

Create an Encrypted Traffic Insights Profile

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

1. Select **Secure Edge > Security Subscriptions > ETI**.

The ETI Profile page opens.

2. Complete the configuration according to the guidelines provided in [Table 280 on page 774](#).
3. Click **Save**.

Table 280: Fields on the ETI Profile Page

Setting	Guideline
Encrypted Traffic Insights (ETI)	Enable this option to detect malicious threats hidden in an encrypted traffic without intercepting and decrypting the traffic.
Logs	<p>Select the action that Juniper Secure Edge must take when malicious traffic is detected.</p> <ul style="list-style-type: none"> • Log detections: Generated logs for malicious traffic detections. • Log everything: Generates logs for each encrypted traffic session and malicious traffic detections.

Service Administration

IN THIS CHAPTER

- [Certificate Management Overview | 776](#)
- [About the Certificate Management Page | 776](#)
- [Generate a Certificate | 778](#)
- [Upload and Download a Certificate | 780](#)
- [Regenerate and Delete a Certificate | 781](#)
- [Add Juniper Clouds Root CA Certificate on Microsoft Windows | 782](#)
- [Add Juniper Clouds Root CA Certificate on MacOS | 783](#)
- [Add Juniper Clouds Root CA Certificate in Google Chrome | 783](#)
- [Add Juniper Clouds Root CA Certificate in Mozilla Firefox | 784](#)
- [Proxy Auto Configuration Files Overview | 784](#)
- [About the PAC Files Page | 786](#)
- [Edit, Clone, and Delete a Proxy Auto Configuration File | 788](#)
- [Distribute a Proxy Auto Configuration File URL to Web Browsers | 791](#)
- [Manually Add a Proxy Auto Configuration File URL to a Web Browser | 793](#)
- [Configure an Explicit Proxy Profile | 795](#)
- [Create a URL Category | 795](#)
- [Create a URL Pattern | 796](#)
- [About the Addresses Page | 798](#)
- [Create Addresses or Address Groups | 800](#)
- [Edit, Clone, and Delete Addresses and Address Groups | 804](#)
- [Decrypt Profiles Overview | 806](#)
- [About the Decrypt Profiles Page | 810](#)
- [Create a Decrypt Profile | 812](#)
- [Edit, Clone, and Delete a Decrypt Profile | 814](#)

Certificate Management Overview

Typically, users gain access to resources from an application or system on the basis of their username and password. You can also use certificates to authenticate and authorize sessions among various servers and users. Certificate-based authentication over a Secure Sockets Layer (SSL) connection is the most secure type of authentication. The certificates can be stored on a smart card, a USB token, or a computer's hard drive.

Certificate Management manages 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.

SSL proxy acts as an intermediary, performing SSL encryption and decryption between the client and the server. Better visibility into application usage can be made available when SSL forward proxy is enabled. SSL proxy relies on certificates and private-public key exchange pairs to provide the secure communication. Transport Layer Security (TLS) evolved from SSL, hence the terms TLS and SSL are sometimes used interchangeably in the document.

About the Certificate Management Page

IN THIS SECTION

- [Tasks You Can Perform | 777](#)

To access this page, select **Secure Edge > Service Administration > Certificate Management**.

You must manage the device certificates to establish Transport Layer Security (TLS) or Secure Socket Layer (SSL) sessions. TLS or SSL uses public-private key technology that requires a paired private key and an authentication certificate. SSL encrypts communication between the web browser and web server with a session key negotiated by the SSL server certificate. Device certificates are required for both on-premises users and roaming users. The certificate generation is a one-time activity and you must do it before deploying the security policies.

Use this page to manage TLS/SSL certificate that is used to establish secure communications between Secure Edge and user endpoints. The certificates may be signed by your own Certificate Authority (CA) or by Juniper's CA. You may create a new certificate signing requests (CSR) that can be used to generate a new certificate by your own CA or you can have Juniper Networks create a new certificate.

Tasks You Can Perform

You can perform the following tasks from this page:

- Generate a CSR or a Juniper Networks issued certificate. See ["Generate a Certificate" on page 778](#) .
- Upload a certificate. See ["Upload and Download a Certificate" on page 780](#) .
- Download a certificate. See ["Upload and Download a Certificate" on page 780](#) .
- Regenerate a certificate. See ["Regenerate and Delete a Certificate" on page 781](#) .
- Delete a certificate. See ["Regenerate and Delete a Certificate" on page 781](#) .
- View details of a certificate. To do this, select an existing certificate and click **More > Detail**. The details of the certificate appears on the right-hand side of the page. Also, when you hover over the certificate name, a Detailed View icon appears before the certificate name. You can also use this icon to view the certificate details.
- Search for a text in a certificate. To do this, click 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: Enter partial text or full text of the keyword in the search bar and click the search icon. The search results are displayed. Click X next to a search keyword or click Clear All to clear the search results.
- Show or hide columns in the Certificate Management 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 281 on page 777](#) provides the details of the fields of the Certificate Management page.

Table 281: Fields on the Certificate Management Page

Field	Description
Name	<p>Displays the name of the certificate.</p> <p>Certificate name is unique across the device. This will be used to create a key pair along with the algorithm to associate with the key.</p>
Type	<p>Displays the certificate type:</p> <ul style="list-style-type: none"> • Custom—new certificate signing request (CSR) • Juniper issued certificate

Table 281: Fields on the Certificate Management Page (*Continued*)

Field	Description
Expiry Date	Displays certificate expiration date.
Encryption Type	Displays whether the algorithm of the certificate is RSA, DSA, or ECDSA encryption.

Generate a Certificate

You can create a new Certificate Signing Request (CSR) or Juniper Networks issued certificate from the Certificate Management page.

- **CSR**—Choose CSR if your company maintains a Private Key Infrastructure (PKI) and certificate authority (CA), and can generate its own certificates. By issuing a CSR on Security Director Cloud, you will not need to upload the private key of the certificate to Juniper Security Director Cloud. After the CSR is generated by Juniper Secure Edge, download the CSR and submit it to your CA to generate a new certificate. Once generated, click **Upload** to upload the certificate on the Certificate Management page.
- **Juniper issued certificate**—Choose Juniper Networks Issued Certificate if your company does not have its own CA. Juniper Networks will generate and keep the certificate on the system. Once the certificate has been generated, click **Download** to download the certificates. The CA certificate will be downloaded. Distribute the certificates to your managed devices.

To generate a certificate:

1. Select **Secure Edge > Service Administration > Certificate Management**.
The Certificate Management page appears.
2. Select **Generate > Certificate signing request or Juniper issued certificate..**
The Generate Certificate Signing Request or Generate Juniper Issued Certificate page appears.
3. Complete the configuration according to the guidelines in [Table 282 on page 779](#) .

NOTE: Fields marked with an asterisk (*) are mandatory.

Table 282: Generate Certificate Settings

Setting	Guideline
Name	Displays the name of the certificate. For example, jsec-ssl-proxy-root-cert. For a CSR, the certificate name is jsec-ssl-proxy-root-cert(CSR Request).
Common name	Enter a common name for the certificate.
Organization name	Enter the organization name that you want to associate with the certificate.
Organization unit name	Enter the organization unit or department that you want to associate with the certificate.
Email address	Enter the e-mail address of the certificate holder.
Country	Select the country from where you are creating this certificate.
State or province	Select the state or region from where you are creating this certificate.
Locality	Select the locality from where you are creating this certificate.
Cryptographic Settings	
Algorithm	Displays the algorithm or encryption type used to sign the certificate.
No. of bits	Displays the bit length size for the algorithm.
Digest	Displays the digests available for the certificate.

Table 282: Generate Certificate Settings (Continued)

Setting	Guideline
Expiration	Displays the validity period of the certificate.

4. Click **OK**.

The Certificate Management page opens with a message indicating that the certificate is created successfully.

Upload and Download a Certificate

IN THIS SECTION

- [Upload a Certificate | 780](#)
- [Download a Certificate | 781](#)

You can upload and download a certificate from the Certificate Management page. This topic has the following sections:

Upload a Certificate

Manually upload the selected CSR signed certificate or an externally generated certificate to the device. Only certificate with .pem format and RSA algorithm are supported. Before you proceed, make sure that the signed certificate is available on your local system.

To upload a signed certificate:

1. Select **Secure Edge > Service Administration > Certificate Management**.

The Certificate Management page appears.

2. Select a CSR certificate or an externally generated certificate and click **Upload**.

The Upload Certificate page appears.

3. Click **Browse** and navigate to the location of the signed certificate file on your local system.

NOTE: Ensure that the uploaded .pem file exactly matches with the selected certificate. If there is a mismatch, then the traffic processing will fail at Juniper Secure Edge.

4. Select the signed certificate and click **Open**.
5. Click **OK**.

You are taken to the Certificate Management page. If the certificate content that you imported is validated successfully, a confirmation message is displayed; if not, an error message is displayed.

After uploading a signed certificate, you can use it when you create an SSL proxy profile.

Download a Certificate

To download a certificate:

1. Select **Secure Edge > Service Administration > Certificate Management**.
The Certificate Management page appears.
2. Select a CSR certificate or an externally generated certificate and click **Download**.
The certificate is downloaded to your system.

Regenerate and Delete a Certificate

IN THIS SECTION

- [Regenerate a Certificate | 781](#)
- [Delete a Certificate | 782](#)

You can regenerate or delete an existing certificate from the Certificate Management page. This topic has the following sections:

Regenerate a Certificate

You can regenerate a certificate a few days in advance if the certificate is about to expire. You can either regenerate a Juniper issued certificate or a CSR for customer issued certificate.

To regenerate a certificate:

1. Select **Secure Edge > Service Administration > Certificate Management**.

The Certificate Management page appears.

2. Select a CSR certificate or an externally generated certificate and click **Regenerate**.
A message indicating the status of the regenerate certificate operation is displayed.

Delete a Certificate

You delete a certificate when you do not want to trust a certificate authority in Juniper Secure Edge.

To delete a certificate:

1. Select **Secure Edge > Service Administration > Certificate Management**.
The Certificate Management page appears.
2. Select the certificate that you want to delete.
3. On the upper right side of the Certificate Management page, click the delete icon (trash can).
A confirmation window appears.
4. Click **Yes** to delete.

NOTE: You must delete a certificate before you delete a tenant.

Add Juniper Clouds Root CA Certificate on Microsoft Windows

1. Double-click the Juniper Clouds Root CA certificate file.
Microsoft Windows displays a security warning.
2. Click **Open**.
The Certificate page opens.
3. Click **Install Certificate...**
The Certificate Import Wizard opens.
4. Select one of the following options, and click **Next**:
 - **Current User**
 - **Local Machine**
5. Select **Place all certificates in the following store**, and click **Browse**.
The Select Certificate Store page opens.
6. Select **Trusted Root Certification Authorities**, and click **OK**.
7. Click **Next**.
8. Click **Finish**.
The Certificate Import Wizard displays a confirmation message about the certificate import.

9. Click **OK**.

Add Juniper Clouds Root CA Certificate on MacOS

1. Start the Keychain Access app on your Mac.
2. Click **System** on the left pane.
3. Click the **Certificates** tab.
4. Drag the Juniper Clouds certificate file onto the Keychain Access app.
5. If you are asked for login credentials, type the administrator login credentials of your Mac.
The Juniper Clouds Root CA certificate is installed on your Mac.
6. Double-click the Juniper Clouds certificate.
The Juniperclouds Root CA 2022 page opens.
7. Select **Always Trust** in **When using this certificate** of the Trust section.

Add Juniper Clouds Root CA Certificate in Google Chrome

1. Start Google Chrome.
2. Click the vertical ellipsis on the top-right of the page, and click **Settings**.
The Settings page opens.
3. Click **Privacy & Security** on the left pane.
4. Click **Security**.
The Security page opens.
5. Click **Manage Certificates**.
The Certificates page opens.
6. Click the **Trusted Root Certification Authorities** tab.
7. Click **Import...**
The Certificate Import Wizard opens.
8. Click **Next**.
9. Browse to the certificate, and click **Open**.
10. Click **Next**.
11. Click **Finish**.
Google Chrome displays a security warning to confirm the certificate import.
12. Click **Yes**.
Google Chrome displays a message confirming that the certificate import is successful.
13. Click **OK** to close the Certificate Import Wizard.

14. Click **Close**.

The Juniper Clouds Root CA certificate is added to Google Chrome.

Add Juniper Clouds Root CA Certificate in Mozilla Firefox

1. Start Mozilla Firefox.
2. Click the hamburger menu on the top-right of the page, and click **Settings**.
The Settings page opens.
3. Click **Privacy & Security** on the left pane.
4. Click **View Certificates...** in the Certificates section.
The Certificate Manager page opens.
5. Click the **Authorities** tab.
6. Click **Import...**, navigate to the certificate, and click **Open**.
The Downloading Certificate page opens.
7. Select the following options:
 - **Trust this CA to identify websites**
 - **Trust this CA to identify email users**
8. Click **OK** to close the Downloading Certificate page.
9. Click **OK** to close the Certificate Manager page.

The Juniper Clouds Root CA certificate is added to Mozilla Firefox.

Proxy Auto Configuration Files Overview

IN THIS SECTION

- [Proxy Auto Configuration File URL Distribution | 785](#)

A proxy auto configuration file instructs a web browser to forward traffic to a proxy server instead of the destination server. Depending on the proxy auto configuration file configuration, the traffic destination can be a proxy server or a real content server.

A proxy auto configuration file contains several mappings between the source, destination and the next hop, such as:

- Source IP subnets and their proxy servers.
- Destination domains and URLs and their proxy servers.
- Source IP subnets that are not to be proxied.
- Destination domains and URLs that are not to be proxied.

The file might also contain other parameters that specify when and under what circumstances a web browser forwards traffic to the proxy server. For example, a proxy auto configuration file can contain instructions about specific days and hours when traffic is sent to the proxy server, along with the domains and URLs for which the traffic is not sent to the proxy server.

All web browsers support proxy auto configuration files. You can configure the URL of a proxy configuration file in web browsers using which the web browsers fetch the file and execute the instructions specified in the file. Proxy auto configuration files can be hosted on a computer, an internal server, or on an external server. Juniper Security Director Cloud hosts a default, recommended PAC file that uses geolocation technology to forward traffic to Juniper Secure Edge.

When you create a new organization in Juniper Security Director Cloud, a recommended proxy auto configuration file is automatically generated. You can download the configuration file or clone and edit the file. You cannot edit the original, recommended proxy auto configuration file, but you can delete the recommended file and generate new recommended files.

Proxy Auto Configuration File URL Distribution

You can distribute or configure the proxy auto configuration file URL through either of the two following methods:

- Use Group Policy Objects of Microsoft Windows to distribute the proxy auto configuration file URL to all domain-joined Microsoft Windows devices. Your organization must use Active Directory to link Group Policy Objects.
- Manually add the proxy auto configuration file URL in a web browser on Microsoft Windows or MacOS computers.

RELATED DOCUMENTATION

[Distribute a Proxy Auto Configuration File URL to Web Browsers | 791](#)

[Manually Add a Proxy Auto Configuration File URL to a Web Browser | 793](#)

About the PAC Files Page

IN THIS SECTION

- [Tasks You Can Perform | 786](#)
- [Field Descriptions | 787](#)

To access the PAC Files page, click **Secure Edge>Service Administration>PAC Files**.

Use the PAC Files page to download proxy auto configuration files, generate new proxy auto configuration files, clone the configuration files, and edit the cloned files.

Tasks You Can Perform

You can perform the following tasks from this page:

- Edit, clone, or delete a proxy auto configuration file—See "[Edit, Clone, and Delete a Proxy Auto Configuration File](#)" on page 788 .
- Generate new default proxy auto configuration files with the latest Juniper-recommended configurations—

1. Click **Generate New PAC**.

An alert message asking you to confirm the new proxy auto configuration file generation is displayed.

2. Click **Yes**.

The new proxy auto configuration file is generated and listed on the PAC Files page.

The new proxy auto configuration files you generate contain the latest configurations recommended by Juniper. These recommendations might be different from the configurations recommended in the past.

- View the details of a proxy auto configuration file—Select the configuration file to view the details, and click **More>Detail**. The Details page opens.[Fields on the PAC Files Page on page 787](#)

[Table 283 on page 787](#) describes the fields on this page.

- Search for proxy auto configuration files using keywords—Click the search icon, enter the search term in the text box, and press **Enter**. The search results open on the same page.

Field Descriptions

Table 283 on page 787 describes the fields on the PAC Files page.

Table 283: Fields on the PAC Files Page

Field	Description
Name	The name of the proxy auto configuration file.
Predefined/Custom	Indicates whether the proxy auto configuration file is automatically generated or edited.
URL	The URL of the proxy auto configuration file.
Description	The description of the proxy auto configuration file.
Created Time	The time when the proxy auto configuration file is created.

Table 284: Details Page Fields

Field	Description
Basic	
Exclude by domain	<p>The traffic to these domains bypasses Juniper Secure Edge.</p> <p>If the client domain matches any of these domains, the proxy auto configuration file is not used.</p>
Exclude by destination prefix	<p>The traffic to these destination prefixes bypasses Juniper Secure Edge.</p> <p>If the client IP address any of these IP prefixes, the proxy auto configuration file is not used.</p>

Table 284: Details Page Fields (Continued)

Field	Description
Exclude by source prefix	<p>The traffic to these source IP prefixes bypasses Juniper Secure Edge.</p> <p>If the client IP address matches any of these IP prefixes, the proxy auto configuration file is not used.</p>
On-premises servers	<p>The servers designated as on-premises servers.</p> <p>You can configure the FQDNs of maximum three servers as on-premises servers. If the FQDNs for any of these on-premises servers return a valid DNS response, the client is considered to be on premises and the proxy auto configuration file configuration is not utilized.</p>
Advanced	
Name	The name of the proxy auto configuration file.
Description	The description of the proxy auto configuration file.
URL	The location of the proxy auto configuration file.
XML Code	The XML-based code in the proxy auto configuration file.

Edit, Clone, and Delete a Proxy Auto Configuration File

IN THIS SECTION

- [Edit a Proxy Auto Configuration File | 789](#)

- [Clone a Proxy Auto Configuration File | 790](#)
- [Delete Proxy Auto Configuration Files | 790](#)

You can edit, clone, and delete proxy auto configuration files from the PAC Files page.

Edit a Proxy Auto Configuration File

You cannot edit the default, recommended proxy auto configuration file. You must first clone the recommended file, then edit the cloned file.

You also cannot edit the URL of a proxy auto configuration file.

NOTE: Ensure that the proxy auto configuration file has two proxy servers configured as a fallback mechanism if the first proxy server is unresponsive. If both the proxy servers are unavailable, the request will be directly sent to the web page.

1. Click **Secure Edge>Service Administration>PAC Files**.
2. Select a proxy auto configuration file, and click the edit (pencil) icon.
The Edit PAC <PAC file name> page opens.
3. On the Basic tab, configure the following fields:
 - **Exclude by Domain**—Click +, and add domains so that the traffic to those domains bypass Juniper Secure Edge. If the client domain matches any of these domains, the proxy auto configuration file is not used.
 - **Exclude by Destination Prefix**—Click +, and add destination prefixes so that the traffic to those prefixes bypass Juniper Secure Edge. If the client IP address matches any of these IP prefixes, the proxy auto configuration file is not used.
 - **Exclude by Source Prefix**—Click +, and add source IP prefixes so that the traffic to those prefixes bypass Juniper Secure Edge. If the client IP address matches any of these IP prefixes, the proxy auto configuration file is not used.
 - **On-premises Servers**—Click +, and add maximum three server FQDNs to designate as on-premises servers. If the FQDNs for any of these on-premises servers return a valid DNS response, the client is considered to be on premises and the PAC file configuration is not utilized. This field supports only FQDNs.

NOTE: Your on-premises protected subnets are already excluded from being directed to Juniper Secure Edge, so you don't need to add the subnets to any of the excluded components list.

4. Click the **Advanced** tab, and configure the following:
 - **Name**—Enter a unique string of maximum 31 alphanumeric characters, dashes, and underscores without spaces.
 - **Description**—Enter a description for the proxy auto configuration file containing maximum 255 characters.
 - **XML Code**—Use the code field to directly modify the configuration of the proxy auto configuration file.
5. Click **OK**.

The changes are saved, and the PAC Files page opens.

Clone a Proxy Auto Configuration File

1. Click **Secure Edge>Service Administration>PAC Files**.
The PAC Files page opens.
2. Select a proxy auto configuration file, and click **Clone**.
3. Edit the parameters as described in "[Edit a Proxy Auto Configuration File](#)" on page 789 .
You cannot edit the URL of a proxy auto configuration file.
4. Click **OK**.

The changes are saved, and the PAC Files page opens with a confirmation message indicating the status of the clone operation.

Delete Proxy Auto Configuration Files

Before you delete a proxy auto configuration file that is in use, ensure that you migrate users to another file.

1. Click **Secure Edge>Service Administration>PAC Files**.
2. Select the proxy auto configuration files to delete, and click the delete icon.
A message asking you to confirm the delete operation is displayed
3. Click **Yes** to delete the selected files.

A confirmation message is displayed indicating the status of the delete operation.

Distribute a Proxy Auto Configuration File URL to Web Browsers

IN THIS SECTION

- [Create a Group Policy Object | 791](#)
- [Distribute the Proxy Auto Configuration File URL | 792](#)
- [Update Organization Group Policy | 792](#)
- [Verify the Proxy Auto Configuration File URL Distribution | 792](#)

You can use the Group Policy Management Console to create a new Group Policy Object for distributing a proxy auto configuration file URL to the Microsoft Windows devices in your organization.

To access Group Policy Management Console from a Microsoft Windows server core, you need a Microsoft Windows computer (Professional, Enterprise, Education or Ultimate editions only) that has Remote Server Administration Tools.

NOTE: Ensure that your Microsoft Windows computer is compatible with your Microsoft Server version and has the appropriate administrative permissions on your domain.

On a Microsoft Windows server with Desktop Experience, the Global Policy Management Console is already installed.

When you configure Internet Explorer to use a proxy auto configuration file, web browsers such as Microsoft Edge, Google Chrome, and Opera use the same configuration. These procedures apply to all web browsers except Mozilla Firefox.

Create a Group Policy Object

1. Open the Group Policy Management Console.
2. In the Group Policy management tree, navigate to the forest, domain or organizational unit to which you are applying the Group Policy Object.
3. Right-click the forest, domain or organizational unit, and select **Create a GPO in this domain, and Link it here**.
The New GPO window opens.
4. In the New GPO window, enter a name for the Group Policy Object.
Leave the **Source Starter GPO** field blank.
5. Right-click the new Group Policy Object, and select the following:

- **Enforced**
- **Link Enabled**

6. Click **OK**.

Distribute the Proxy Auto Configuration File URL

You can use the Group Policy Results wizard to verify the policy settings of the users or computers in the domain.

1. Open the Group Policy Management Console.
2. Navigate to the domain or organizational unit to which you applied the Group Policy Object and expand it.
3. Right-click the newly created Group Policy Object, and select **Edit**.
4. Select **User Configuration>Preferences> Control Panel Settings**.
5. Right-click **Internet Settings**, and select **New>Internet Explorer 10**.
6. On the Connections tab, click **LAN settings**.
7. Enter the proxy auto configuration file URL in the **Address** field.
If you see a red dotted line in the **Address** field, place your cursor in the text box, and press the **F6** function key. This enables the field which is indicated by a solid green line.
8. Click **OK**.
9. Optional: If you want to apply the Group Policy Object to the entire computer irrespective of the signed in user, do the following:
 - a. Select **Computer Configuration>Policies>Administrative Templates>Windows Components >Internet Explorer** in the Global Policy Management Console.
 - b. From the Internet Explorer folder, double-click **Make proxy settings per-machine (rather than per-user)**.
The Make proxy settings per-machine (rather than per-user) window opens.
 - c. Under **Make proxy settings per-machine (rather than per-user)**, select **Enabled**.
 - d. Click **OK**.

Update Organization Group Policy

1. Open the Microsoft Windows command prompt.
2. Run the following command to update the group policy: `gpupdate` or `gpupdate /force`

Verify the Proxy Auto Configuration File URL Distribution

1. Log in to the Microsoft Windows user computer using the domain login.
2. Open Internet Explorer.

3. Click Settings > Connections > LAN Settings.
4. Check that the Address field contains the proxy auto configuration file URL.
5. If the Address field does not contain the proxy auto configuration file URL, the group policy might not be updated. Do the following to update the policy:
 - a. Open the command prompt, and run the following command to update the group policy: `gpupdate` or `gpupdate /force`

Manually Add a Proxy Auto Configuration File URL to a Web Browser

IN THIS SECTION

- [Add a Proxy Auto Configuration File URL to Google Chrome in Microsoft Windows | 793](#)
- [Add a Proxy Auto Configuration File URL to Mozilla Firefox in Microsoft Windows | 794](#)
- [Add a Proxy Auto Configuration File URL to Microsoft Edge on Microsoft Windows | 794](#)
- [Add a Proxy Auto Configuration File URL to Safari on MacOS | 794](#)

The following procedures explain steps to manually add a proxy auto configuration file to web browsers in Microsoft Windows and MacOS.

Add a Proxy Auto Configuration File URL to Google Chrome in Microsoft Windows

Before you begin, get the URL of the proxy auto configuration file to add to Google Chrome.

You can copy the URL of the default, recommended proxy auto configuration files on the **Secure Edge > Service Administration > PAC Files** page of Juniper Security Director Cloud.

1. Open Google Chrome.
2. Go to the **Settings** page.
3. Click **System**.
4. In the search result, click **Open your computer's proxy settings**.
The Proxy page opens.
5. Enable **Use setup script**, and paste the PAC file URL in **Script address**.
6. Click **Save**.

Add a Proxy Auto Configuration File URL to Mozilla Firefox in Microsoft Windows

Before you begin, get the URL of the proxy auto configuration file to add to Mozilla Firefox.

You can copy the URL of the default, recommended proxy auto configuration files on the **Secure Edge > Service Administration > PAC Files** page of Juniper Security Director Cloud.

1. Open Mozilla Firefox.
2. Go to the **Settings** page.
3. On the General tab, click **Settings...** in Network Settings.
The Connection Settings page opens.
4. Select **Automatic proxy configuration URL**, and paste the proxy auto configuration file URL.
5. Click **OK**.

Add a Proxy Auto Configuration File URL to Microsoft Edge on Microsoft Windows

Before you begin, get the URL of the proxy auto configuration file to add to Microsoft Edge.

You can copy the URL of the default, recommended proxy auto configuration files on the **Secure Edge > Service Administration > PAC Files** page of Juniper Security Director Cloud.

1. Open Microsoft Edge.
2. Click the ellipsis on the top right, and click **Settings**.
3. On the left pane, click **System and performance**.
4. Click **Open your computer's proxy settings** in **System**.
The Proxy page opens.
5. Click **Set up** in **Automatic proxy setup**.
The Edit setup script page opens.
6. Enable **Use setup script**, and paste the proxy auto configuration file URL in **Script address**.
7. Click **Save**.

Add a Proxy Auto Configuration File URL to Safari on MacOS

To know more about proxy settings on MacOS, see [here](#).

Before you begin, get the URL of the proxy auto configuration file to add to Microsoft Edge.

You can copy the URL of the default, recommended proxy auto configuration files on the **Secure Edge > Service Administration > PAC Files** page of Juniper Security Director Cloud.

1. Open Safari.
2. Click **Safari > Preferences**.
3. Click **Advanced**.
4. Click **Change Settings...** in **Proxies**.

The Network window opens.

5. Select **Automatic Proxy Configuration**, and paste the proxy auto configuration file URL.
6. Click **OK**.
7. Restart Safari to commit the changes.

Configure an Explicit Proxy Profile

The explicit proxy profile tells Secure Edge which port to listen to for the client-side traffic and which traffic to decrypt or bypass.

A Secure Edge explicit forward proxy deployment provides an easy way to handle web requests from the remote users. You can configure the client browsers to point to a forward proxy server.

1. Select **Secure Edge > Service Administration > Explicit Proxy**.

The Explicit Proxy Profile page opens.

2. Complete the configuration according to the guidelines in [Table 285 on page 795](#)

Table 285: Fields on the Explicit Proxy Profile Page

Setting	Guideline
Port	Enter a proxy port number between 8000 to 9999.
Decrypt profile	<p>Select a decrypt profile from the list.</p> <p>A decrypt profile is a set of certificates that are used to decrypt the incoming SSL traffic to Secure Edge. If a decrypt profile is unavailable, click Create Decrypt Profile to create a new profile. See "Create a Decrypt Profile" on page 812 .</p>

3. Click **Save**.

Create a URL Category

Use this page to create URL categories. A URL category is a list of URL patterns grouped under a single title.

1. Select **Shared Services > Objects > URL Categories**.

The URL Categories page opens.

2. Click +.

The Create URL Category page opens.

3. Complete the configuration according to the guidelines provided in [Table 286 on page 796](#).

NOTE: Fields marked with * are mandatory.

4. Click OK.

Table 286: Fields on the Create URL Categories Page

Settings	Guidelines
Name	<p>Enter a unique name containing maximum 59 characters.</p> <p>The name must begin with a letter or an underscore and can contain alphanumeric characters and special characters such as dashes and underscores</p>
Description	<p>Enter a description containing maximum 255 characters.</p>
URL Patterns	<p>Select minimum one URL pattern to add in your URL category.</p> <p>NOTE: You can also add URL patterns by clicking + to open the Create URL Pattern page. See "Create a URL Pattern" on page 796.</p>

A new URL category is created and the URL Categories page opens.

Create a URL Pattern

Use this page to create URL patterns. You can also assign URL patterns to a URL category.

1. Select **Shared Services > Objects > URL Patterns**.

The URL Patterns page opens.

2. Click +.

The Create URL Pattern page opens.

3. Complete the configuration according to the guidelines provided in [Table 287 on page 797](#).

NOTE: Fields marked with * are mandatory.

4. Click **OK**.

Table 287: Fields on the Create URL Patterns Page

Settings	Guidelines
Name	<p>Enter a unique name containing maximum 27 characters.</p> <p>The name must begin with a letter or an underscore and can contain alphanumeric characters and special characters such as dashes and underscores.</p>
Description	<p>Enter a description containing maximum 255 characters.</p>

Table 287: Fields on the Create URL Patterns Page (*Continued*)

Settings	Guidelines
Add URLs	<p>Click +, and enter URLs in the text box.</p> <ul style="list-style-type: none"> • The following wildcard characters are supported in the text box: <ul style="list-style-type: none"> • asterisk (*)—Can only be used at the beginning of a URL and must be followed by a period (.). • period (.) • square brackets ([]) • question mark (?)—Can only be used at the end of a URL. • All URL patterns containing wildcard characters must begin with http://. • The following types of wildcard syntaxes are supported: http://*.example.net, http://www.example.ne?, and http://www.example.n??. • The following types of wildcard syntaxes are not supported: *.example.???, http://*example.net, http://?, and www.example.ne?. <p>The URLs are displayed in the URL list.</p>

A new URL pattern is created and the URL Patterns page opens.

About the Addresses Page

IN THIS SECTION

- [Tasks You Can Perform | 799](#)
- [Field Descriptions | 800](#)

To access this page, select **Shared Services > Objects > Addresses**.

An address specifies an IP address or a host name. You can create addresses that can be used across all policies. Addresses are used in firewall and NAT services and apply to the corresponding policies. If you know only the host name, you enter it into the **Hostname** field and use the address resolution option to resolve it to an IP address. You can also resolve an IP address to the corresponding host name.

Juniper Secure Edge manages its address book at the global level, assigning objects to devices that are required to create policies. An address book is a collection of addresses and address groups that are available in a security zone. If the device is capable of using a global address book, Juniper Secure Edge pushes address objects used in the policies to the global address book of the device.

Use this page to create, edit, clone, and delete addresses and address groups. Addresses and address groups are used in firewall and NAT services. After you create an address, you can combine it with other addresses to form an address group. Address groups are useful when you want to apply the same policy to multiple services.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create an address or address group. See "[Create Addresses or Address Groups](#)" on page 800 .
- Modify, clone, or delete an address or address group. See "[Edit, Clone, and Delete Addresses and Address Groups](#)" on page 804 .
- View the configured parameters of an address or address group. Click the details icon that appears when you hover over the name of an address or address group or select **More > Detailed View**.
- Show or hide columns about the address or address group. Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Filter information based on select criteria. You can add filters, save the filters, and set any of the filters as default. To add a filter:
 1. Click on the filter icon on the top-right corner of the page and select **Add Filter** to open the Add Criteria page.
 2. Set the filter conditions and click **Add**.

The filter is saved and the filter is applied on the data on the page. Filter can be saved and can mark any one filter as default.

To remove the filter, click on the filter icon and select **Hide Filter**.

- Search for an address or address group. Click the Search icon in the top right corner of the page to search for an address or address group.

You can enter partial text or full text of the keyword in the text box and press Enter.

The search results are displayed on the same page.

Field Descriptions

[Table 288 on page 800](#) provides guidelines on using the fields on the Addresses page.

Table 288: Fields on the Addresses Page

Field	Description
Name	The name of the address or address group.
Type	The type of the address object.
Hostname	The host name of the address.
IP Address	The IP address associated with the address.
Description	The description of the address or address group.

Create Addresses or Address Groups

Use this page to create addresses and address groups. After you create an address, you can combine it with other addresses to form an address group. Address groups are useful when you want to apply the same policy to multiple services.

1. Select [Shared Services](#) > [Objects](#) > [Addresses](#).

The **Addresses** page opens.

2. Click +.

The **Create Address** page opens.

3. Complete the configuration according to the guidelines provided in [Table 289 on page 801](#) and [Table 290 on page 803](#).

4. Click OK.

Table 289: Fields on the Create Addresses Page

Field	Description
Name	<p>Enter a unique name containing maximum 63 characters.</p> <p>The name must begin with an alphanumeric character and can contain alphanumeric characters and special characters such as colons, hyphens, slashes, periods, and underscores.</p>
Description	<p>Enter a description containing maximum 900 characters.</p> <p>The description can contain alphanumeric characters and special characters except ampersand, angular brackets, or a new line.</p> <p>You should make this description as useful as possible for all administrators.</p>
Object Type	<p>Select Address or Address Group.</p> <p>If you select Address Group, the screen changes for you to select the addresses to include in your address group. Table 290 on page 803 describes address group configuration parameters.</p>

Table 289: Fields on the Create Addresses Page (Continued)

Field	Description
Type	<p>Select one of the following address types and configure the corresponding fields:</p> <ul style="list-style-type: none"> • Host <ul style="list-style-type: none"> • Host IP—Enter the IPv4 host IP address. For example, 192.0.2.0. If you don't know the IP address, you can enter the host name, and click Look up hostname. • Hostname—Enter a host name containing maximum 63 characters. The host name must begin with an alphanumeric character and can contain special characters such as dashes and underscores. For example, www.company.com. If you don't know the host name, you can enter the IP address, and click Look up IP address. The host name lookup is supported for IPv4 addresses. • Range <ul style="list-style-type: none"> • Start Address—Enter a starting IPv4 address along with the classless inter-domain routing (CIDR) for the address range. For example, 192.0.2.0/24. • End Address—Enter an ending IPv4 address for the address range. <p>The address range is validated after you enter the addresses.</p> <p>NOTE: An address range is configured on a managed device as an address set with one or more network address objects covering the specified address range.</p> • Network

Table 289: Fields on the Create Addresses Page (Continued)

Field	Description
	<ul style="list-style-type: none"> • Network—Enter the network IP address. For example, 192.0.2.0 for an IPv4 or 2001:db8:4136:e378:8000:63bf:3fff:fdd2 for an IPv6 address. • Subnet Mask—Enter the subnet mask for the network range. For example, 192.0.2.0/24 for an IPv4 netmask or 2001:db8::/32 for an IPv6 prefix. The subnet mask is validated as you enter it. You must enter the correct subnet mask based on the network value. • DNS Host DNS Name—Enter the DNS name containing maximum 63 characters. The DNS name must end with an alphanumeric character and can contain alphanumeric characters and special characters such as dashes and periods.

Table 290: Fields on the Address Group Page

Field	Description
Name	<p>Enter a unique name containing maximum 63 characters.</p> <p>The name must begin with an alphanumeric character and can contain alphanumeric characters and special characters such as colons, hyphens, slashes, periods, and underscores.</p>

Table 290: Fields on the Address Group Page (Continued)

Field	Description
Description	<p>Enter a description containing maximum 900 characters.</p> <p>The description can contain alphanumeric characters and special characters except ampersand, angular brackets, or a new line.</p> <p>You should make this description as useful as possible for all administrators.</p>
Object Type	<p>Select Address Group.</p> <p>The screen changes for you to select the addresses to include in your address group.</p>
Addresses	<p>Select the addresses to include in your address group.</p> <p>You can use the fields at the top of each column to search for addresses.</p>

A new address or address group with your configurations is created.

Edit, Clone, and Delete Addresses and Address Groups

IN THIS SECTION

- [Edit Addresses and Address Groups | 805](#)
- [Clone Addresses and Address Groups | 805](#)
- [Delete Addresses and Address Groups | 805](#)

You can edit, clone, and delete addresses and address groups from the **Addresses** page.

NOTE: You cannot edit or delete predefined addresses.

Edit Addresses and Address Groups

If you edit an address that is deployed as part of a policy, you must redeploy the policy for the changes to take effect.

1. Select **Shared Services > Objects > Addresses**.

The Addresses page opens.

2. Select the address or address group to edit, and click the pencil icon.

The Edit Address page opens.

3. Edit the parameters according to the guidelines provided in ["Create Addresses or Address Groups" on page 800](#).

NOTE: You cannot edit Address Name and Object Type.

4. Click **OK**.

The changes are saved, and the modified address or address group is displayed on the Addresses page.

Clone Addresses and Address Groups

1. Select **Shared Services > Objects > Addresses**.

The Addresses page opens.

2. Select the address or address group, and click **More > Clone**.

The Clone Address page opens.

3. Edit the parameters according to the guidelines provided in ["Create Addresses or Address Groups" on page 800](#).

4. Click **OK**.

The changes are saved, and the cloned address or address group is displayed on the Addresses page.

Delete Addresses and Address Groups

You can delete only addresses or address groups that are not referenced in any policy.

1. Select **Shared Services > Objects > Addresses**.

The Addresses page opens.

2. Select the addresses or address groups to delete, and click the delete icon.

A message asking you to confirm the delete operation is displayed

3. Click **Yes** to delete the addresses or address groups.

A confirmation message is displayed indicating the status of the delete operation. If the addresses or address groups are referenced in a policy, an error message is displayed.

Decrypt Profiles Overview

IN THIS SECTION

- [Server Authentication | 807](#)
- [Root CA | 808](#)
- [Trusted CA List | 808](#)
- [Session Resumption | 808](#)
- [SSL Proxy Logs | 808](#)

Juniper Secure Edge attempts to decrypt all SSL/TLS traffic by default. Decrypt profiles allow you to define the types of traffic that should be exempted from decryption.

SSL is an application-level protocol that provides encryption technology for the Internet. SSL, also called TLS, ensures the secure transmission of data between a client and a server through a combination of privacy, authentication, confidentiality, and data integrity. SSL relies on certificates and private–public key exchange pairs for this level of security.

Server authentication guards against fraudulent transmissions by enabling a Web browser to validate the identity of a Web server. Confidentiality mechanisms ensure that communications are private. SSL enforces confidentiality by encrypting data to prevent unauthorized users from eavesdropping on electronic communications. Finally, message integrity ensures that the contents of a communication have not been tampered with.

SSL proxy performs SSL encryption and decryption between the client and the server, but neither the server nor the client can detect its presence. SSL proxy ensures that it has the keys to encrypt and decrypt the payload:

- For the server, SSL proxy acts as a client—SSL proxy generates the shared pre-master key, it determines the keys to encrypt and decrypt.
- For the client, SSL proxy acts as a server—SSL proxy first authenticates the original server and replaces the public key in the original server certificate with a key that is known to it. It then

generates a new certificate by replacing the original issuer of the certificate with its own identity and signs this new certificate with its own public key (provided as a part of the proxy profile configuration). When the client accepts such a certificate, it sends a shared pre-master key encrypted with the public key on the certificate. Because SSL proxy replaced the original key with its own key, it is able to receive the shared pre-master key. Decryption and encryption take place in each direction (client and server), and the keys are different for both encryption and decryption.

SSL proxy uses the following services:

- SSL-T-SSL terminator on the client side.
- SSL-I-SSL initiator on the server side.

This topic has the following sections:

Server Authentication

Implicit trust between the client and the device (because the client accepts the certificate generated by the device) is an important aspect of SSL proxy. It is extremely important that server authentication is not compromised; however, in reality, self-signed certificates and certificates with anomalies are in abundance. Anomalies can include expired certificates, instances of common name not matching a domain name, and so forth.

You can specify that the SSL proxy should ignore server authentication completely. In this case, SSL proxy ignores errors encountered during the server certificate verification process (such as CA signature verification failure, self-signed certificates, and certificate expiry).

You can specify whether the SSL proxy should ignore server authentication errors or not during the creation of an SSL proxy profile.

- If you specify that server authentication errors should *not* be ignored, the following scenarios occur:
 - If authentication succeeds, a new certificate is generated by replacing the keys and changing the issuer name to the issuer name that is configured in the root CA certificate in the proxy profile.
 - If authentication fails, the connection is dropped.
- If you specify that server authentication errors should be ignored, the following scenarios occur:

NOTE: We do not recommend that you configure 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.

- If the certificate is self-signed, a new certificate is generated by replacing the keys only. The issuer name is not changed. This ensures that the client browser displays a warning that the certificate is not valid.
- If the certificate has expired or if the common name does not match the domain name, a new certificate is generated by replacing the keys and changing the issuer name to `SSL-PROXY: DUMMY_CERT:GENERATED DUE TO SRVR AUTH FAILURE`. This ensures that the client browser displays a warning that the certificate is not valid.

Root CA

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.

Trusted CA List

SSL proxy ensures secure transmission of data between a client and a server. Before establishing a secure connection, SSL 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.

Session Resumption

An SSL session refers to the set of parameters and encryption keys that are created when a full handshake is performed. A connection is the conversation or active data transfer that occurs within the session. The computational overhead of a complete SSL handshake and generation of primary keys is considerable. In short-lived sessions, the time taken for the SSL handshake can be more than the time for data transfer. To improve throughput and still maintain an appropriate level of security, SSL session resumption provides a mechanism for caching sessions. This way, session information, such as the pre-master secret key and agreed-upon ciphers, can be cached for both the client and the server. A session ID identifies the cached information. In subsequent connections, both parties agree to use the session ID to retrieve the information rather than create pre-master secret key. Session resumption shortens the *handshake* process and accelerates SSL transactions.

SSL Proxy Logs

When logging is enabled in a decrypt profile, the SSL proxy can generate the messages shown in [Table 291 on page 809](#) .

Table 291: SSL Proxy Logs

Log Type	Description
All	All logs are generated.
Warning	Logs used for reporting warnings.
Info	Logs used for reporting general information.
Error	Logs used for reporting errors.
Session Whitelisted	Logs generated when a session is allowed.
Session Allowed	Logs generated when a session is processed by SSL proxy even after encountering some minor errors.
Session Dropped	Logs generated when a session is dropped by SSL proxy.

All logs contain similar information; the message field contains the reason for the log generation. One of three prefixes shown in [Table 292 on page 809](#) identifies the source of the message. Other fields are descriptively labeled.

Table 292: SSL Proxy Log Prefixes

Prefix	Description
system	Logs generated because of errors related to the device or an action taken as part of the decrypt profile. Most logs fall into this category.
openssl error	Logs generated during the <i>handshake</i> process if an error is detected by the openssl library.

Table 292: SSL Proxy Log Prefixes (*Continued*)

Prefix	Description
certificate error	Logs generated during the handshake process if an error is detected in the certificate (X.509 related errors).

About the Decrypt Profiles Page

IN THIS SECTION

- [Tasks You Can Perform | 810](#)
- [Field Descriptions | 810](#)

To access this page, click **Secure Edge > Service Administration > Decrypt Profiles**. Use the Decrypt Profiles page to view and to manage decrypt profiles.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a decrypt profile—See "[Create a Decrypt Profile](#)" on page 812
- Edit, clone, or delete a decrypt profile—See "[Edit, Clone, and Delete a Decrypt Profile](#)" on page 814 .
- View the details of a decrypt profile—Select the decrypt profile to view the details, and from the More or right-click menu, select **Detailed View**. The View decrypt profile Details page opens. [Table 293 on page 811](#) describes the fields on this page.
- Search for decrypt profiles using keywords—Click the search icon and enter the search term in the text box, and press Enter. The search results open on the same page.

Field Descriptions

[Table 293 on page 811](#) describes the fields on the Decrypt Profiles page.

Table 293: Fields on the Decrypt Profiles Page

Field	Description
Name	The name of the decrypt profile.
Exempted Address	The addresses that are exempted from decrypt processing.
Description	The description of the decrypt profile.
Root Certificate	The root certificate associated with the decrypt profile.

Table 294: View Decrypt Profile Details Page Fields

Field	Description
General Information	
Name	The name of the decrypt profile.
Description	The description of the decrypt profile.
Root certificate	Displays the root certificate authorities associated with the root certificate.
Exempted address	The addresses that are exempted from decrypt processing.
Exempted URL categories	The URL categories that are exempted from decrypt processing.

Create a Decrypt Profile

Use this page to configure decrypt profiles. The decrypt profile is enabled as an application service within a security policy.

NOTE: Ensure that you have a root certificate imported for the organization before you create a decrypt profile. You can import SSL certificates (root and trusted) from the Certificate Management page (**Secure Edge > Service Management > Certificate Management**) and associate the certificates with decrypt profiles.

1. Select **Secure Edge > Service Administration > Decrypt**.
The Decrypt Profiles page opens.
2. Click **+**.
The Create Decrypt Profile page opens.
3. Complete the configuration according to the guidelines provided in [Table 295 on page 812](#).
Fields marked with an asterisk (*) are mandatory.
4. Click **OK**.

Table 295: Fields on the Decrypt Profile Page

Setting	Guideline
General Information	
Name	Enter a unique name without spaces containing maximum 63 characters. The name can contain alphanumeric characters and special characters such as hyphens and underscores.
Description	Enter a description containing maximum 255 characters.

Table 295: Fields on the Decrypt Profile Page *(Continued)*

Setting	Guideline
Root certificate	<p>Select or add a root certificate. In a public key infrastructure (PKI) hierarchy, the root certificate authority (CA) is at the top of the trust path.</p> <p>NOTE: To select the root certificate from the device, you must ensure that at least one trusted certificate is installed on the device.</p>
Exempted URL categories	<p>Select the previously defined URL categories to create allowlists that bypass decrypt processing. The selected URL categories are exempted during SSL inspection.</p> <p>NOTE: You can also add URL categories by clicking + to open the Create URL Category page. See "Create a URL Category" on page 795 .</p>
Exempted addresses	<p>Select the previously defined addresses to create allowlists that bypass decrypt processing. The selected addresses are exempted during SSL inspection.</p> <p>Because SSL encryption and decryption are complicated and expensive procedures, network administrators can selectively bypass decrypt processing for some sessions.</p> <p>Such sessions typically 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> <p>NOTE: You can also add addresses by clicking + to open the Create Addresses page. See "Create Addresses or Address Groups" on page 800 .</p>

An decrypt profile is created, and the Decrypt Profiles page opens displaying a confirmation message.

Edit, Clone, and Delete a Decrypt Profile

IN THIS SECTION

- [Edit a Decrypt Profile | 814](#)
- [Clone a Decrypt Profile | 814](#)
- [Delete a Decrypt Profile | 814](#)

You can edit, clone, and delete decrypt profiles from the Decrypt Profiles page.

Edit a Decrypt Profile

1. Select **Secure Edge > Service Administration > Decrypt Profiles**.
The Decrypt Profiles page opens displaying the existing decrypt profiles.
2. Select the decrypt profile, and click the pencil icon.
The Edit Decrypt Profile page opens.
3. Edit the parameters according to the guidelines provided in ["Create a Decrypt Profile" on page 812](#).
4. Click **OK**.

The changes are saved, and the Decrypt Profiles page opens.

Clone a Decrypt Profile

Cloning enables you to easily create a decrypt profile based on an existing one.

1. Select **Secure Edge > Service Administration > Decrypt Profiles**.
The Decrypt Profiles page opens displaying the existing decrypt profiles.
2. Select the decrypt profile, and select **More > Clone**.
The Clone decrypt profile page opens.
3. Edit the parameters according to the guidelines provided in ["Create a Decrypt Profile" on page 812](#).
4. Click **OK**.

The changes are saved, and the Decrypt Profiles page opens with a confirmation message indicating the status of the clone operation.

Delete a Decrypt Profile

1. Select **Secure Edge > Service Administration > Decrypt Profiles**.
The Decrypt Profiles page opens displaying the existing decrypt profiles.

2. Select the decrypt profiles to delete, and click the delete icon.

A message asking you to confirm the delete operation is displayed

3. Click **Yes** to delete the selected decrypt profiles.

A confirmation message is displayed indicating the status of the delete operation.

Identity

IN THIS CHAPTER

- [End User Authentication Overview | 816](#)
- [About the End User Authentication Page | 817](#)
- [Add an End User Profile | 829](#)
- [Edit and Delete an End User Profile | 830](#)
- [Add a Group | 831](#)
- [Edit and Delete a Group | 832](#)
- [Juniper Identity Management Service Overview | 833](#)
- [About the JIMS Page | 835](#)
- [JIMS Collector Onboarding Overview | 837](#)
- [Onboard JIMS Collector | 837](#)
- [Create JIMS Collector Service Accounts | 838](#)
- [Install JIMS Collector | 840](#)
- [Configure JIMS Collector to Get Information from the Directory Service | 841](#)
- [Configure JIMS Collector to Get Microsoft Event Logs | 842](#)
- [Configure JIMS Collector to Probe Unknown IP Addresses | 844](#)
- [Delete JIMS Collector | 844](#)

End User Authentication Overview

Juniper Secure Edge provides end user authentication service that is tenant-aware and internet-facing. The authentication service is responsible for authenticating users using the preferred authentication methods configured by the administrator.

Administrators must authenticate the remote (roaming) users using any one of the following supported authentication methods:

- Hosted Database—Use a database hosted on Juniper Secure Edge for authentication and authorization.
- SAML— Connect to an identity provider (IdP) of your choice over the Internet for authentication. You use the Security Assertion Markup Language (SAML) 2.0 framework for authentication using an IdP.
- LDAP—Connect to your organization's Active Directory service over the Internet for authentication. For user-based firewall policies using group membership, You must first install a Juniper Identity Management Service (JIMS) Collector on your network: See "[Juniper Identity Management Service Overview](#)" on page 833 .

Based on the authentication methods configured by the tenant administrator, the user will be re-directed to the login page with those configured authentication methods.

When all three authentication methods are configured, the user can authenticate using the method of their choice. For SAML authentication, click **Single Sign-On (SSO)** and for Hosted DB and LDAP authentication, click **E-mail/Password** button. In case both Hosted DB and LDAP are configured, and the user enters the username and password, then order of authentication is: (1) Hosted DB, (2) LDAP.

About the End User Authentication Page

IN THIS SECTION

- [Tasks You Can Perform | 817](#)
- [Create a SAML Profile | 818](#)
- [Create an LDAPS Profile | 824](#)
- [Manage the Hosted Database | 827](#)

To access this page, select **Secure Edge>Identity>User Authentication**.

Configure authentication profiles to authenticate the end users.

Tasks You Can Perform

You can perform the following tasks from this page:

- ["Create a SAML Profile" on page 818](#) .
- ["Create an LDAPS Profile" on page 824](#)

- ["Manage the Hosted Database" on page 827](#)

Create a SAML Profile

To create a SAML profile:

1. Select **Secure Edge > Identity > User Authentication** .

The End User Authentication page appears with the SAML profile tab.

2. Complete the configurations according to the guidelines in [Table 296 on page 821](#)

NOTE: Fields marked with an asterisk (*) are mandatory.

Figure 21: SAML Profile

Secure Edge ▾ / Identity ▾ / User Authentication ▾

End User Authentication ?

SAML ? LDAPS ? Hosted Database ?

SAML Profile * ?

ACS Urls ? [View ACS Urls](#)

Identity Provider (IdP) Configuration

Directory Synchronization ?

Identity Provider * ? ▾

Security API Token * ? 🔗

Tenant Domain * ?

Validate ? [Validate](#)

IdP Settings ?

- Import settings
- Enter settings manually
- Enter metadata URL

Figure 22: IdP Attributes

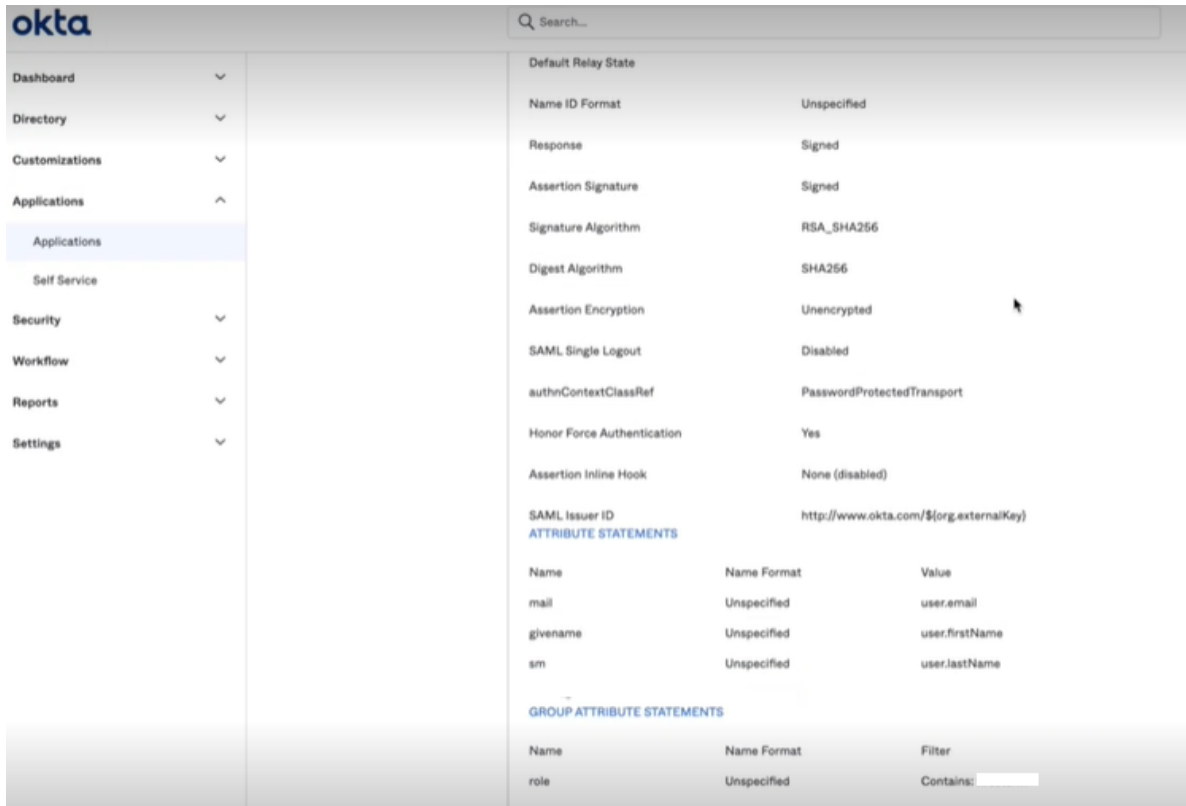
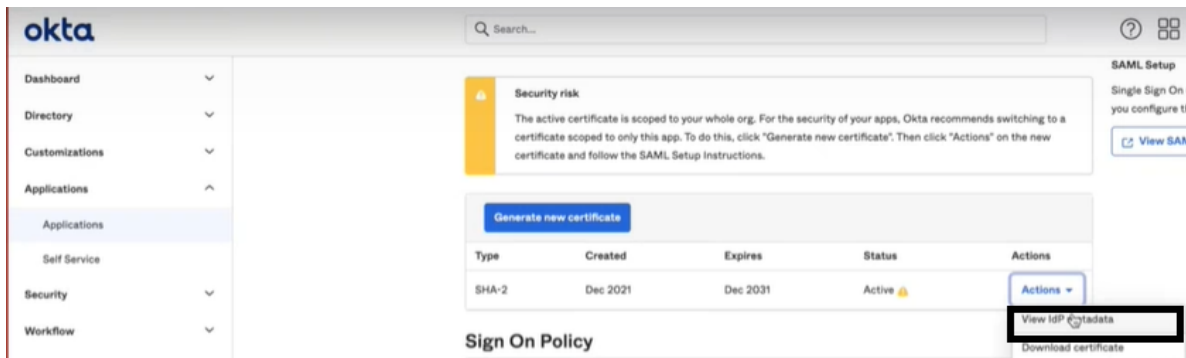


Figure 23: IdP Metadata URL



3. Click OK.

Table 296: Fields on the SAML profile tab

Field	Description
SAML Profile	
SAML Profile	Enable or disable SAML authentication.
ACS URLs	View the Assertion Consumer Service (ACS) URLs. The ACS URL directs your IdP where to send its SAML response after authenticating a user.
Directory Synchronization	Enable to use the user groups from your IdP directories in Secure Edge policy. Supported IdPs are Okta and Entra ID (Azure AD).
Identity Provider (IdP) Configuration	
Identity Provider	Select an IdP. Available IdPs for directory synchronization are Okta and Entra ID (Azure AD).
Okta Configurations	
Security API Token	<p>Enter the Okta API token created using the API > Token > Create token menu on Okta admin console for Juniper Secure Edge. API token is valid for 30 days.</p> <p>If SAML profile or directory synchronization is made inactive/disabled for more than 30 days, it is revoked and cannot be used again. For reconfiguration, you need to create a new token.</p>
Tenant Domain	Enter the domain configured in Okta. Locate the Okta domain by clicking your username in the top-right corner of the Okta admin console. The domain appears in the dropdown menu.
Validate	Click validate button to test the validity of the configurations.

Table 296: Fields on the SAML profile tab (Continued)

Field	Description
Entra ID Configurations	
Application ID	Enter the Application (client) ID assigned to you after completing App registrations on Microsoft Entra admin center for Juniper Secure Edge.
Directory (tenant) ID	Enter the Directory (tenant) ID assigned to you after completing App registrations on Microsoft Entra admin center for Juniper Secure Edge.
Client Secret	Enter the client secret generated using Certificates & secrets > Client secrets menu on Microsoft Entra admin center for Juniper Secure Edge. Microsoft Entra generates client secret with expiry date, so update client secret before expiry date.
Validate	Click validate button to test the validity of the configurations.
IdP Settings	<ul style="list-style-type: none"> • Select Import Settings to import the IdP metadata in one go. The metadata file must be in XML format. • To manually configure the IdP settings, select Enter settings manually. • To copy the settings from an URL, select Enter metadata URL.
Metadata URL	Enter the IdP metadata URL. The Service Provider (SP) uses the metadata URL to validate that the SAML assertions are issued from the correct IdP.
Service Provider (SP)	

Table 296: Fields on the SAML profile tab (Continued)

Field	Description
Entity ID	Displays the unique identifier for the SAML Profile.
Username attribute	<p>Enter the username attribute for SAML.</p> <p>Username attribute is mandatory and must be in e-mail address format. The username attribute is mapped to the user data, which is provided by IdP in the SAML assertion response.</p>
Sign auth requests	<p>Enable the toggle button to sign the SAML authentication requests sent from Juniper Secure Edge to IdP. If you enable sign authentication requests, you must provide both private key and public key certificate.</p>
Private key	<p>Enter the private key that you have generated locally. In Juniper Secure Edge, the private key is used to sign SAML authentication request. The private key is not shared with IdP.</p>
Public key	<p>Enter the public key that you have generated locally. The public key certificate is generated locally by the user. You must upload the same public key certificate in the IdP portal. In IdP, the public key certificate is used to validate the SAML authentication request sent by Juniper Secure Edge.</p>
Group attribute	<p>Enter the group attribute which the end-user belongs to which is then filtered and sent to IDP.</p>
First name attribute	<p>Enter the first name attribute of the SAML user.</p> <p>The first name attribute is used to create an user profile.</p>

Table 296: Fields on the SAML profile tab (Continued)

Field	Description
Last name attribute	Enter the last name attribute of the SAML user. The last name attribute is used to create an user profile.

NOTE:

- For SAML, the retries and the locking period is configurable in SAML server.
- By default, directory synchronization runs at regular intervals.

Create an LDAPS Profile

LDAPS profile configuration supports high availability (HA). You must configure both primary and secondary LDAPS servers. If you enable SSL encryption, the default SSL LDAP port number is 636. If you are not using SSL, the default port number is 389.

To create an LDAPS profile:

1. Select **Secure Edge > Identity > User Authentication** .

The End User Authentication page appears.

2. Click **LDAPS** tab.
3. Complete the configurations according to the guidelines in [Table 297 on page 826](#)

NOTE: Fields marked with an asterisk (*) are mandatory.

Figure 24: LDAPS Profile

Secure Edge / Identity / User Authentication

End User Authentication

SAML Profile | **LDAPS Profile** | Hosted Database

i Be sure to allow all LDAP traffic from Secure Edge IPs — — on your firewalls.

Primary Server

Server address*

SSL certificate* **Browse**

Port number*

Secondary Server

Secondary Server

Server address*

SSL certificate* **Browse**

Port number*

Test LDAP Servers Connection

LDAP Authentication

Base domain name*

Bind domain name*

Bind password* **Test Authentication**

User Options

User attribute

User filter

Cancel **Save**

4. Click **OK**.

Table 297: Fields on the LDAPS profile tab

Field	Description
Primary Server	
Server address	Enter the IP address of LDAP authentication server. The server address is a unique IPv4 or IPv6 address that is assigned to a particular LDAP server and used to route information to the server.
SSL certificate	The client certificate for LDAP client to establish an LDAP over SSL connection. If you plan to use SSL encryption with your LDAP server, you must import the SSL certificate from the LDAP server. Click Browse , select the SSL certificate and click Open .
Port number	Specify a port on the LDAP server to which the LDAP client can connect to.
Secondary Server (Optional)	
Server address	Enter the IP address of secondary LDAP authentication server. The server address is a unique IPv4 or IPv6 address that is assigned to a particular LDAP server and used to route information to the server.
SSL certificate	The client certificate for LDAP client to establish an LDAP over SSL connection. If you plan to use SSL encryption with your secondary LDAP server, you must import the SSL certificate from the LDAP server. Click Browse , select the SSL certificate and click Open .
Port number	Specify a port on the secondary LDAP server to which the LDAP client can connect to.
Test LDAP Servers Connection	Click Test LDAP Servers Connection to check if the connection is established.

Table 297: Fields on the LDAPS profile tab (Continued)

Field	Description
LDAP Authentication	
Base domain name	Enter the distinguished name (DN) of the search base. Configure the distinguished name of the search base (LDAP base) that specifies the base of user directory. Every entry in the directory has a distinguished name (DN). The DN is the name that uniquely identifies an entry in the directory.
Bind domain name	Enter the distinguished name of the proxy account of the LDAP client to bind to the server with. Configure the distinguished name to bind the LDAP client with the LDAP server.
Bind password	Enter the credentials of the LDAP client to bind with the LDAP server. Configure the public key password. Click Test Authentication to check if the credentials are bound for authentication.
User Options	
User attribute	Enter the username attribute that is used for comparing user entries. The username attribute has permissions to access the LDAP server.
User filter	Enter a value to use for the search parameter filter in LDAP.

Manage the Hosted Database

End users can be authenticated against a hosted database consisting of user's username (email address) and passwords. Administrators can use the Juniper Secure Edge portal to configure and activate the users in hosted database. Once the users are configured in the Juniper Secure Edge portal, the user will receive an e-mail consisting of their credentials (username and password). Once the user has this information, they can use their email address and password as credentials to authenticate.

Use the Hosted Database tab to add, modify, and delete an end user profile or group profiles.

You can perform the following tasks from this page:

- Add an end user profile. See ["Add an End User Profile" on page 829](#) .
- Edit or delete end user profile. See ["Edit and Delete an End User Profile" on page 830](#) .
- Add a group.
- Edit or delete groups.
- View details about end user profiles. See [Table 298 on page 828](#) .

NOTE: Hosted database supports maximum five retry attempts after which the user is locked. The number of retries is not configurable. Once a user is locked, they can only be unlocked by the administrator.

Table 298: Fields on the Hosted Database tab

Field	Description
End users	
Name	Displays the name of the user who is a part of the tenant.
Email	Displays the email address of the user. E-mail is the username, which will be used by the user for authentication.
Groups	Displays the groups to which the user belongs to. Group name is displayed in domain:groupname format.
Groups	
Name	Displays the name of the group.

Table 298: Fields on the Hosted Database tab (Continued)

Field	Description
Username	Click on Show users to view the list of users in the group. Username for a user is the email address of the user.
Domain	Displays the domain to which the group belongs to.
Description	Displays the description of the group.

Add an End User Profile

You can add up to 50 users per group. You cannot create a user without tagging them to a group.

NOTE: You must create at least one group to create a user.

To add an end user profile:

1. Select **Secure Edge > Identity > User Authentication.**

The End User Authentication page appears.

2. Click the **Hosted Database tab.**

The End Users tab appears.

3. Click the add icon (+).

The Create End User Profile page appears.

4. Configure the parameters according to the guidelines provided in [Table 299 on page 830](#) .

NOTE: Fields marked with * are mandatory.

Table 299: End User Profile Settings

Setting	Guideline
Name	Enter the name of the user. The name can contain alphanumeric characters, underscore, period, and space.
Email	Enter the email address of the user.
Groups	Select the groups to which you want to assign the user and click >. NOTE: You can add users to multiple groups but belonging to a single domain.

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

Once you click **OK**, the new password will be sent to the email address of the user. You will see the new profile in the **Hosted Database > End users** tab.

Edit and Delete an End User Profile

IN THIS SECTION

- [Edit an End User Profile | 830](#)
- [Delete an End User Profile | 831](#)

You can edit and delete end user profiles from the Hosted Database tab. This topic has the following sections:

Edit an End User Profile

To modify the parameters configured for an end user:

1. Select **Secure Edge > Identity > User Authentication**.

The End User Authentication page appears.

2. Click the **Hosted Database** tab and select the end user profile you want to edit. Click the edit icon (pencil symbol) on the right top corner of the page.
3. The **Edit End User Profile** page appears, displaying the same options that are displayed when creating a new End User Profile.

NOTE: You can only edit the name of a user and the groups to which the user belongs to. You cannot edit the e-mail address of the user.

4. Modify the parameters according to the guidelines provided in [Table 299 on page 830](#).
5. Click **OK** to save your changes. If you want to discard your changes, click **Cancel**.
If you click **OK**, you will see the modified profiles in the **Hosted Database** tab.
6. To reset the password for the end user, select the end user profile and click **Reset Password**. An alert message appears, verifying that you want to reset the password. Once you click **Yes**, the new password will be sent to the email address of the user. Only administrators can reset the password.

Delete an End User Profile

To delete an user profile:

1. Select **Secure Edge > Identity > User Authentication**.
The End User Authentication page appears.
2. Click the **Hosted Database** tab and select the end user profile you want to delete and then click the delete icon (trash can).
An alert message appears, verifying that you want to delete the user profile.
3. Click **Yes** to delete the user profile. If you do not want to delete, click **Cancel** instead.
If you click **Yes**, the selected user profile is deleted.

Add a Group

You can add up to 50 groups for a single tenant. Each group can contain up to 50 users. A user can only be present in groups having the same domain name.

To add a group profile:

1. Select **Secure Edge > Identity > User Authentication**.
The End User Authentication page appears.
2. Click the **Hosted Database** tab.
3. Click the **Groups** tab.
4. Click the add icon (+).

The Create Group page appears.

5. Configure the parameters according to the guidelines provided in [Table 300 on page 832](#).

NOTE: Fields marked with * are mandatory.

Table 300: Group Settings

Setting	Guideline
Name	Enter the name of the group. The name can contain alphanumeric characters, underscore, period, and space.
Description	Enter the description for the group.
Domain	Enter the domain to which the group belongs to.
End users	Select the users whom you want to assign to the group and click >.

6. Click **OK** to save your changes. If you want to discard your changes, click **Cancel**.
If you click **OK**, you will see the new group in the **Hosted Database > Groups** tab.

Edit and Delete a Group

IN THIS SECTION

- [Edit a Group | 832](#)
- [Delete a Group | 833](#)

You can edit and delete groups from the Hosted Database tab. This topic has the following sections:

Edit a Group

To modify the parameters configured for a group:

1. Select **Secure Edge > Identity > User Authentication**.

The End User Authentication page appears.

2. Click the **Hosted Database > Groups** tab and select the group you want to edit.

3. Click the edit icon (pencil symbol) on the right top corner of the page.

The **Edit Group** page appears, displaying the same options that are displayed when creating a new group.

NOTE: You can only edit the description of a group and the users who are added to the group. You cannot edit the group name or the domain of the group.

4. Modify the parameters according to the guidelines provided in [Table 300 on page 832](#).

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

If you click **OK**, you will see the modified parameters in the **Hosted Database > Groups** tab.

Delete a Group

To delete a group:

1. Select **Secure Edge > Identity > User Authentication**.

The End User Authentication page appears.

2. Click the **Hosted Database > Groups** tab and select the group you want to delete and then click the delete icon (trash can).

An alert message appears, verifying that you want to delete the group.

3. Click **Yes** to delete the group. If you do not want to delete, click **Cancel** instead.

If you click **Yes**, the selected group is deleted.

Juniper Identity Management Service Overview

Juniper Identity Management Service (JIMS) is a standalone service application that runs on Microsoft Windows. The JIMS application has the following two components:

- **JIMS Collector**—Collects and maintains an in-memory cache of user, device, and group information from Active Directory domains or from a syslog client.

JIMS Collector monitors and collects data from Active Directory every 30 seconds. After collecting the data, JIMS Collector automatically pushes this data to the local JIMS Server and Juniper Secure Edge when JIMS Collector is onboarded on Juniper Secure Edge.

- **JIMS Server**—Is installed with JIMS Collector and manages on-premises SRX Series Firewalls. When you use Juniper Secure Edge, JIMS Collector pushes identity information to Juniper Secure Edge when configured.

Juniper Secure Edge supports JIMS Collector Release 1.7.0 or later.

[Table 301 on page 834](#) lists the ports JIMS Collector uses to connect to various servers.

Table 301: JIMS Collector Communication Ports

Connection	Port
JIMS Collector connects to directory services, such as Microsoft Active Directory, using LDAP or LDAPS.	<ul style="list-style-type: none"> • LDAP—TCP port 389 • LDAPS—TCP port 636
JIMS Collector connects to identity Producers, such as Microsoft Domain Controllers or Microsoft Exchange Server, using MSRPC.	TCP port 135
JIMS Collector connects to the SYSLOG server identity producer using internal communications. The SYSLOG server listens to TCP and UDP port for incoming syslog messages.	TCP and UDP port 514
JIMS Collector connects to the PC Probe identity producers using internal communications. PC Probe sends outbound Windows Management Instrumentation (WMI) requests to computers using TCP ports.	TCP ports range 49152 to 65535
JIMS Collector pushes data to Juniper Secure Edge using TLS over a TCP port.	TCP port 443
On-premises SRX Series Firewalls pull data from the local JIMS Server.	<ul style="list-style-type: none"> • TCP port 443 • TCP port 591 for JWeb support

About the JIMS Page

IN THIS SECTION

- [Tasks You Can Perform | 835](#)
- [Field Descriptions | 835](#)

To access this page, select **Secure Edge > Identity > JIMS**.

Use the JIMS page to add and manage JIMS Collectors and view the JIMS Collector statistics.

Tasks You Can Perform

You can perform the following tasks from this page:

- Onboard JIMS Collectors. See ["Onboard JIMS Collector" on page 837](#) .
- Delete JIMS Collectors. See ["Delete JIMS Collector" on page 844](#) .
- View the configured parameters of JIMS Collectors. Select **More > Detailed View**, or click the details icon that is displayed when you hover over the JIMS Collector identifier.

NOTE: The detailed view displays the number of times JIMS Collector connected to the JIMS server to push identity-related data, such as domains, users, device, groups, and sessions.

- Show or hide columns about the address or address group. Click the vertical ellipsis on the top-right corner, click **Show Hide columns**, and select the columns to view on the page.
- Reset the custom view settings on the JIMS page to the default settings. Click the vertical ellipsis on the top-right corner, and click **Reset Preferences**.

Field Descriptions

[Table 302 on page 836](#) provides guidelines on using the fields on the JIMS page.

NOTE: The widgets on the top section of the JIMS page display the number of times identity-related statistics, such as domains, users, device, groups, and sessions, is collected from JIMS Collector.

Table 302: Fields on the JIMS Page

Field	Description
Domains	The number of domains.
Users	The number of active users.
Devices	The number of active devices.
Groups	The number of groups.
Sessions	The number of active sessions.
JIMS Collectors	
Collector Identifier	The name of the Microsoft Windows server where JIMS Collector is installed.
Version	The version of JIMS Collector that is installed on the Microsoft Windows server.
Current State	The current state of JIMS Collector.
Description	The user description that the JIMS Collector UI displays.
Last Update	The timestamp when JIMS Collector last connected to the JIMS server for an update.

JIMS Collector Onboarding Overview

Onboarding JIMS Collector involves multiple tasks that requires installation and configuration in Juniper Secure Edge, Active Directory, and the JIMS Collector administrative interface.

You will need to onboard JIMS Collector in Juniper Secure Edge, create service accounts with limited privileges in Active Directory, and configure JIMS Collector using its administrative interface.

The following list describes the tasks required to install and configure JIMS Collector:

1. Onboard JIMS Collector in Juniper Secure Edge.
 - a. Download JIMS Collector.
 - b. Install the Root CA certificate.
 - c. Generate the JIMS Collector base configuration.
2. Create the following service accounts with limited privileges in Active Directory for JIMS Collector in Active Directory—JIMS-EventSource, JIMS-DirectoryService, and JIMS-PCProbe.
 - a. Configure user accounts with limited permission.
 - b. Configure the properties of the user accounts.
 - c. Add the user accounts to Active Directory groups.
 - d. Define group policies for the user accounts.
3. Install JIMS Collector and verify the the JIMS Collector connectivity.
4. Configure JIMS Collector to get information from the directory service.
5. Configure JIMS Collector to get Microsoft event logs.
6. Configure JIMS Collector to probe unknown IP addresses.

Onboard JIMS Collector

Juniper Secure Edge supports JIMS Collector Release 1.7.0 or later.

1. Log in to Juniper Secure Edge.
2. Select **Secure Edge>Identity>JIMS**.
The JIMS page opens.
3. Click **+**.
The JIMS Collector Onboarding page opens.

4. Click **Download**.

You can save the JIMS Collector setup file on your computer.

5. Click **Download Certificate** to install the Root CA certificate.

6. Click **Generate - Collector Configuration**, and save the generated XML configuration file on your computer.

You can also change the description of JIMS Collector before generating the JIMS Collector configuration file. The JIMS page displays the description in the list of JIMS Collectors.

Downloading the XML configuration file also automatically generates a secret key to decrypt the configuration in the file in JIMS Collector. A new secret key is generated every time you generate the XML configuration file.

7. Copy the secret key generated after the XML configuration file is downloaded.

You will need to load the secret key into JIMS Collector after installing the application.

Juniper Secure Edge displays the onboarded JIMS Collector in the Pending state. The state changes to Active after you install JIMS Collector.

Create JIMS Collector Service Accounts

IN THIS SECTION

- [Configuring Limited Permission User Accounts | 839](#)
- [Configuring Properties for Limited Permission User Accounts | 839](#)
- [Adding Limited Permission User Accounts to Active Directory Groups | 839](#)
- [Defining Group Policies for Limited Permission User Accounts | 839](#)

Create the following service accounts with limited privileges in Active Directory to ensure these service accounts have permission only to execute their tasks.

- JIMS-EventSource; Used to get Microsoft event logs.
- JIMS-DirectoryService: Used to get username, devices, and groups from the directory service.
- JIMS-PCProbe: Used to probe a Microsoft Windows computer in your Active Directory domain.

You will need to add the service accounts on JIMS Collector. Perform the following procedures to configure each service account.

Configuring Limited Permission User Accounts

For each new user account:

1. From the Start menu, select **Active Directory Users and Computers**.
2. Navigate to the forest's Users container.
3. Right-click **Users** and select **New Users**.
4. Specify a descriptive first and middle name and any username or pre-Windows 2000 username.
5. Specify a password according to your organization's password policy.
6. Clear the **User must change password at next login** check box.
7. Select the **User cannot change password** check box.
8. Select the **Password never expires** check box.

Configuring Properties for Limited Permission User Accounts

To set properties for each new user account:

1. Right-click a user and then select **Properties**.
2. Select the **Remote Control** tab.
3. Clear the **Enable Remote Control** check box.
4. Select **Remote Desktop Services Profile**.
5. Select the **Deny this user's permissions to log onto remote desktop session host server** check box.
6. Select the **Dial-in** tab and select the **Deny Access** check box.

Adding Limited Permission User Accounts to Active Directory Groups

To add each new user account to an Active Directory group:

1. Select **Built-in** under the forest.
2. Select the **Event Log Readers** group and add the JIMS-EventLogRemoteAccess account.
3. Select the **Distributed COM Users** group and add the JIMS-PC-Probe account.
4. Select the **Remote Management Users** group and add the JIMS-PC-Probe account.
5. Select the **Domain Admins** group and add the JIMS-PC-Probe account.

Defining Group Policies for Limited Permission User Accounts

To define group policies for each new user account:

1. From the Start menu, select **Group Policy Management**.
2. In the Group Policy Manager, select the forest, select **Default Domain Policy**, and right-click **Edit**.
3. Select **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment**.

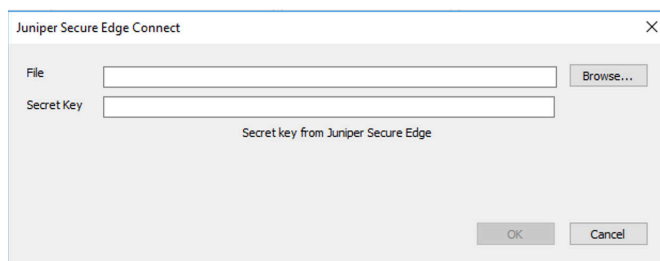
4. Select **Deny Logon locally**, select **Define these policy settings**, and add each new user account.
5. Select **Deny Logon through Remote Desktop Services**, select **Define these policy settings**, and add each new user account.
6. Select **Deny Logon through Terminal Services**, select **Define these policy settings**, and add each new user account.
7. Select **Deny logon as a batch job**, select **Define these policy settings**, and add each new user account.
8. Select **Deny Logon as a service**, select **Define these policy settings**, and add each new user account.

Install JIMS Collector

Juniper Secure Edge supports JIMS Collector Release 1.7.0 or later.

1. Install JIMS Collector on a Microsoft Windows computer
 - Ensure that the computer can connect to Juniper Security Director Cloud and your enterprise's Active Directory.
2. Select **Juniper Networks > JIMS Administrative Interface** from the Start menu of the computer to start the JIMS Collector user interface.
3. Onboard JIMS Collector to Juniper Secure Edge.
 - a. Click **File > Juniper Secure Edge Connect**.
The Juniper Secure Edge Connect page opens.

Figure 25: Juniper Secure Edge Connect Page



- b. Select the downloaded XML configuration file.
 - c. Insert the secret key generated after downloading the XML configuration file.
 - d. Click **OK**.
4. Check whether JIMS Collector has established a connection with Juniper Secure Edge.
 - a. Click **Monitor** on the left pane, and click the **JIMS Servers** tab.

- b. Verify that the **Connection State** column displays **Connected**.

Juniper Secure Edge displays the onboarded JIMS Collector on the JIMS page in the Active state after a connection with Juniper Secure Edge is established.

Configure JIMS Collector to Get Information from the Directory Service

JIMS Collector gets information such as username, devices, and groups from the directory service. JIMS Collector uses this configuration to fetch the user and group mapping information from Active Directory.

1. Log in to the Windows computer where you installed JIMS Collector.
2. Select **Juniper Networks > JIMS Administrative Interface** from the Start menu.
The Juniper Identity Management Service - Administrative Interface opens.
3. Click **Directory Services** on the left pane.
4. Click **Add**.

The Add Active Directory Configuration page opens.

Figure 26: Add Active Directory Configuration Window

5. Complete the configuration according to the guidelines provided in [Table 303 on page 842](#).

Table 303: Fields on the Add Active Directory Configuration Page

Field	Description
Description	Enter a description for the active directory. The description must be useful for all administrators.
Server Hostname or IP Address	Enter an IP address or FQDN of your Active Directory server. We recommend that you enter an FQDN because the IP address might change.
Login ID	Enter the username of the JIMS-DirectoryService service account.
Password	Enter the password of the JIMS-DirectoryService service account.
TLS Connection	Select whether the connection must use TLS as the default encryption protocol. The default setting is No.

6. Click **OK**.

Configure JIMS Collector to Get Microsoft Event Logs

JIMS Collector uses this data to map user and group mapping information from Active Directory with IP addresses.

1. Log in to the Windows computer where you installed JIMS Collector.
2. Select **Juniper Networks > JIMS Administrative Interface** from the Start menu.
The Juniper Identity Management Service - Administrative Interface opens.
3. Click **Identity Producers** on the left pane, and click the **Event Sources** tab.
4. Click **Add**.
The Add EventSource Configuration page opens.

Figure 27: Add EventSource Configuration Page

5. Complete the configuration according to the guidelines provided in [Table 304 on page 843](#).

Table 304: Fields on the Add EventSource Configuration Page

Field	Description
Select a Source	Select one of the following sources to monitor the mapping between the user and IP address: <ul style="list-style-type: none"> • Domain Controller • Exchange Server
Description	Enter a description for the active directory. The description must be useful for all administrators.
Server Hostname or IP Address	Enter the FQDN of your Active Directory server. You can also enter the IP address, but FQDN is better because the IP address might change.
Login ID	Enter the username of the JIMS-EventSource service account.
Password	Enter the password of the JIMS-EventSource service account.

Table 304: Fields on the Add EventSource Configuration Page (*Continued*)

Field	Description
Startup Event History Catchup Time	<p>Enter a time period in hours that the JIMS Collector goes back after a restart and begins collecting event log information from the sources.</p> <p>The valid range is between 1 and 10 hours. The default value is 1 hour.</p>

6. Click **OK**.

Configure JIMS Collector to Probe Unknown IP Addresses

The optional PC Probe configuration enables JIMS Collector to probe an unknown IP address of domain computers for the username domain of the user. PC Probe supports only Microsoft Windows-based computers.

Do not configure PC Probe if your server running JIMS Collector has full Internet access. PC Probe sends Windows Management Instrumentation Command-line (WMIC) commands that could expose your enterprise's service account details to unknown users.

1. Log in to the Windows computer where you installed JIMS Collector.
2. Select **Juniper Networks > JIMS Administrative Interface** from the Start menu.
3. Click **Identity Producers** on the left pane, and click the **PC Probes** tab.
4. Click **Add**.
The PC Probe Configuration page opens.
5. Configure the following fields to add the JIMS-PCProbe service account:
 - **Description**
 - **Login ID**—Enter the username of the JIMS-PCProbe service account.
 - **Password**—Enter the password of the JIMS-PCProbe service account.
6. Click **OK**.

Delete JIMS Collector

You need to delete JIMS Collector from the JIMS Administrator Interface and from Juniper Secure Edge.

1. Log in to the Windows computer where you installed JIMS Collector.
2. Click **Juniper Networks > JIMS Administrative Interface** from the Start menu.
3. Click **JIMS Server** on the left pane.
4. Select the JIMS server, and click **Delete**.
An alert message asking you to confirm the delete operation is displayed.
5. Click **Yes**.
6. Log in to Juniper Secure Edge.
7. Select **Secure Edge > Identity > JIMS**.
The JIMS page opens.
8. Select the JIMS Collectors to delete, and click the delete icon.
An alert message asking you to confirm the delete operation is displayed.
9. Click **Yes**.
A confirmation message indicating the status of the delete operation is displayed.

CASB and DLP

IN THIS CHAPTER

- [About CASB and DLP | 846](#)

About CASB and DLP

Juniper Secure Edge provides full-stack Security Service Edge (SSE) capabilities to protect web, SaaS, and on-premises applications and provide users with consistent and secure access that follows them wherever they go.

Cloud Access Security Broker (CASB) discovers sanctioned and non-sanctioned SaaS applications in use and provides visibility and granular controls to ensure authorized access, actions, threat prevention, and compliance.

Data Loss Prevention (DLP) provides granular visibility and control over data housed in cloud applications and prevents sensitive data from leaving your network either inadvertently or as part of an attack.

For more information on the Juniper CASB and DLP features, see [Juniper Secure Edge CASB and DLP Administration Guide](#).

For more information on the Juniper CASB and DLP Release Notes, see [Juniper Secure Edge CASB and DLP Release Notes](#).



Shared Services

[Firewall Profiles-Rule Options | 848](#)

[Firewall Profiles-Redirect Profiles | 855](#)

[Objects-Addresses | 859](#)

[Objects-GeoIP | 875](#)

[Objects-Services | 881](#)

[Objects-Applications | 898](#)

[Objects-Schedules | 914](#)

[Objects-URL Patterns | 920](#)

[Objects-URL Categories | 927](#)

[Advanced Threat Prevention | 932](#)

[Insights-On-prem Collectors | 978](#)

[Insights-Cloud Collector | 992](#)

[Insights-Rules | 993](#)

[Insights-Settings | 1000](#)

Firewall Profiles-Rule Options

IN THIS CHAPTER

- [About Rule Options Page | 848](#)
- [Create Rule Options | 849](#)
- [Edit, Clone, and Delete Rule Options | 853](#)

About Rule Options Page

IN THIS SECTION

- [Tasks You Can Perform | 848](#)

Use the Rule Options page to create an object to specify redirect options, authentication, TCP-options, and action for destination-address translated or untranslated packets. When a rule options is created, the Juniper Security Director Cloud creates an object in the database to represent the rule options. You can use this object to create security policies.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create rule options. See "[Create Rule Options](#)" on page 849 .
- Edit or delete rule options. See "[Edit, Clone, and Delete Rule Options](#)" on page 853 .
- Search for a rule option. Click the Search icon in the top right corner of the page to search for a firewall policy.

You can enter partial text or full text of the keyword in the text box and press Enter.

The search results are displayed on the same page.

Table 305: Fields on the Rule Options Page

Field	Description
Name	Name of the rule option.
Description	Description of the Rule Option
Definition Type	Number of devices associated with the policy.
Last Updated By	The user who modified the rule option.
Last Updated Time	The date and time when the rule option was modified.

Create Rule Options

When a rule options is created, Juniper Security Director Cloud creates an object in the database to represent the rule options. You can use this object to create security policies.

Use the Rule Options page to create an object that specifies the basic settings of a security policy.

To create rule option:

1. Select **Shared Services > Firewall Profiles > Rule Options**.

The Rule Options page appears.

2. Click the plus icon (+).

The Create Rule Options page appears.

3. Complete the configuration settings according to the guidelines provided in ["About Rule Options Page" on page 848](#).

NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **OK**.

The new rule option is created and a confirmation message is displayed.

Table 306: Fields on the Create Rule Options Page

Field	Description
Name	<p>Enter a unique string of alphanumeric characters that can include spaces and some special characters.</p> <p>The maximum length is 255 characters.</p>
Description	<p>Enter a description for the policy; the maximum length is 255 characters.</p>
General	
Hardware Acceleration	<p>Enable this option to process fast-path packets in the network processor instead of in the Services Processing Unit (SPU). When performing the policy check, the SPU verifies if the traffic is qualified for services offloading.</p>
Redirect Options	<p>Select an option:</p> <ul style="list-style-type: none"> • None • Redirect Wx- Select this option if you want to enable WX redirection for packets that arrive from the LAN. • Reverse Redirect Wx-Select this option if you want to enable WX redirection for the reverse flow of packets that arrive from the WAN.
<p>Authentication</p> <p>NOTE: Authentication is supported only when the permit action is enabled.</p>	
Push Auth Entry to JIMS	<p>Enable Push to JIMS.</p>

Table 306: Fields on the Create Rule Options Page (Continued)

Field	Description
Authentication Type	<p>Select an option to restrict or permit users individually or in groups. Select None if you do not want to use any authentication to restrict or permit clients.</p> <ul style="list-style-type: none"> • Pass Through-Pass-through user authentication is a form of active authentication. The user is prompted to enter a username and password when pass-through authentication is invoked. • Web-Web authentication is an alternative to pass-through user authentication. Instead of pointing to the resource that you want to connect to from your client browser, you point the browser to an IP address on the device that is enabled for Web authentication. This initiates an HTTP session to the IP address hosting the Web authentication feature on the device. The device then prompts you for your username and password and caches the result in the device. Later, when traffic encounters a Web authentication policy, you are allowed or denied access based on the prior Web authentication results. • User Firewall-Firewall authentication policies that restrict and permit access of firewall users to protected resources behind a firewall. • Infranet-Select this option to configure the SRX Series Firewall to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment..
TCP Option	
Syn-check	<p>Enable this option for the device to reject TCP segments with non-SYN flags set unless they belong to an established session.</p>

Table 306: Fields on the Create Rule Options Page (*Continued*)

Field	Description
Sequence Check	Enable this option to monitor the TCP byte sequence counter and to validate the trusted acknowledgment number against the untrusted sequence number.
Window Scale	Enable this option to increase the network transmission speed
Initial TCP MSS	Select the TCP maximum segment size (MSS) for packets arriving at the ingress interface (initial direction). If the value in the packet is higher than the one you select, the configured value overrides the TCP MSS value in the incoming packet. The range is 64 through 65535.
Reverse TCP MSS	Select the TCP maximum segment size (MSS) for packets that match a specific policy and travel in the reverse direction of a session. If the value in the packet is higher than the one you select, the configured value replaces the TCP MSS value. The range is 64 through 65535.
Advanced Settings	
Destination NAT Control	Select an option <ul style="list-style-type: none"> • None • Drop Untranslated-Drop packets with translated destination IP addresses. Traffic permitted by the security policy is limited to packets where the destination IP address has not been translated. • Drop Translated-Drop packets without translated destination IP addresses. Traffic permitted by the security policy is limited to packets where the destination IP address has been translated by means of a destination NAT rule.

RELATED DOCUMENTATION

[About Rule Options Page | 848](#)

[Edit, Clone, and Delete Rule Options | 853](#)

Edit, Clone, and Delete Rule Options

SUMMARY

IN THIS SECTION

- [Edit Rule Options | 853](#)
- [Clone Rule Options | 853](#)
- [Delete Rule Options | 854](#)

You can edit, clone, and delete rule options from the Rule Options page. This topic has the following sections:

Edit Rule Options

To modify the parameters configured for a rule option:

1. Select **Shared Services > Firewall Profiles > Rule Options**.

The Rule Options page appears, displaying the existing rule options.

2. Select the rule option that you want to edit and then select the pencil icon.

The Edit Rule Options page appears, displaying the same fields that are presented when you create a rule option.

3. Modify the rule option fields.

4. Click **OK** to save your changes.

A confirmation message appears, indicating the status of the edit operation.

Clone Rule Options

Cloning enables you to easily create rule option based on an existing one.

To clone a rule option:

1. Select **Shared Services > Firewall Profiles > Rule Options**.

The Rule Options page appears, displaying the existing rule options.

2. Select the rule option that you want to clone and then select **More > Clone**. Alternatively, right-click a profile and select **Clone**.

The Clone Rule Options page appears, displaying the same fields that are presented when you create a rule option.

3. Modify the rule option fields.
4. Click **OK** to save your changes.

A confirmation message appears, indicating the status of the clone operation.

Delete Rule Options

To delete one or more rule options:

1. Select **Shared Services > Firewall Profiles > Rule Options**.

The Rule Options page appears, displaying the existing rule options.

2. Select one or more rule options that you want to delete and then select the delete icon.

An alert message appears, asking you to confirm the delete operation.

3. Click **Yes** to delete the selected rule options.

A confirmation message appears, indicating the status of the delete operation.

RELATED DOCUMENTATION

| [About Rule Options Page | 848](#)

Firewall Profiles-Redirect Profiles

IN THIS CHAPTER

- [About the Redirect Profiles Page | 855](#)
- [Create a Redirect Profile | 856](#)
- [Edit, Clone, and Delete a Redirect Profile | 857](#)

About the Redirect Profiles Page

IN THIS SECTION

- [Tasks You Can Perform | 855](#)
- [Field Descriptions | 856](#)

To access this page, select **Shared Services > Firewall Profiles > Redirect Profiles**.

Use the Redirect Profiles page to create a redirect profile and provide a reason for the policy action or to redirect the user request to an informative webpage. After you configure the redirect profiles for a policy, when a policy blocks HTTP or HTTPS traffic with reject action, a message or redirect URL is sent to the user. You can customize the redirect action by adding the text message or specify the URL to which the user is redirected.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a redirect profile. See ["Create a Redirect Profile" on page 856](#) .
- Edit, Clone, and Delete a redirect profile. See ["Edit, Clone, and Delete a Redirect Profile" on page 857](#) .

Field Descriptions

Table 307 on page 856 provides guidelines on using the fields on the Redirect Profile page.

Table 307: Fields on the Redirect Profile Page

Field	Description
Block Message Type	The message type, that is, Text or Redirect URL.
Block Message/Redirect URL	The custom text or the URL of the webpage to which the user is redirected. If custom-text is specified, both the default block message and the custom-defined block message are displayed. Custom text is inserted below the default message, which includes username, Application Firewall has blocked your request to application <i>application name</i> at <i>dest-ip:dest-port</i> accessed from <i>src-ip:src-port</i> .

Create a Redirect Profile

Use this page to create a redirect profile and configure a custom block message or redirect URL.

To create a redirect profile:

1. Select **Shared Services > Firewall Profiles > Redirect Profiles**.
The Redirect Profiles page appears.
2. Click the add icon (+).
The Create Redirect Profile page appears.
3. Complete the configuration according to the guidelines provided in [Table 308 on page 857](#).

Table 308: Fields on the Redirect Profile Page

Field	Description
Block Message Type	<p>Select the block message type:</p> <ul style="list-style-type: none"> • Text—If custom text is specified, both the default block message and the custom-defined block message are displayed. The maximum length of custom text is 512 characters. • Redirect URL—The URL of the webpage to which the client is redirected. The URL must start with http or https. For example, http://www.juniper.net. The URL must not exceed 1024 characters.
Redirect URL	Enter the block message or redirect URL.

4. Click **OK**.

A profile is created and displayed on the redirect profiles page.

Edit, Clone, and Delete a Redirect Profile

IN THIS SECTION

- [Edit a Redirect Profile | 857](#)
- [Clone a Redirect Profile | 858](#)
- [Delete a Redirect Profile | 858](#)

You can edit, clone, and delete redirect profiles from the Redirect Profiles page.

Edit a Redirect Profile

To modify the parameters configured for a Redirect profile:

1. Select **Shared Services > Firewall Profiles > Redirect Profiles**.

The Redirect Profiles page appears.

2. Select the redirect profile that you want to edit and click the edit icon (pencil).

The Edit Redirect Profile page appears showing the same fields that are presented when you create a Redirect profile.

3. Modify the redirect profile fields as needed.
4. Click **OK** to save your changes.

You are taken to the Redirect Profiles page with the modified redirect profile information.

Clone a Redirect Profile

Cloning enables you to easily create a new redirect profile based on an existing one.

To clone a Redirect profile:

1. Select **Shared Services > Firewall Profiles > Redirect Profiles**.

The Redirect Profiles page appears.

2. Select the redirect profile that you want to clone and select **More > Clone**. Alternatively, right-click a profile and select **Clone**.

The Clone Redirect Profile page appears, showing the same fields that are presented when you create a Redirect profile.

3. Modify the redirect profile fields as needed.
4. Click **OK** to save your changes.

You are taken to the Redirect Profiles page. A confirmation message appears, indicating the status of the clone operation.

Delete a Redirect Profile

1. Select **Shared Services > Firewall Profiles > Redirect Profiles**.

The Redirect Profiles page appears.

2. Select one or more redirect profiles that you want to delete and click the delete icon.

An alert message appears asking you to confirm the delete operation.

3. Click **Yes** to delete the selected redirect profiles.

A confirmation message appears indicating the status of the delete operation.

Objects-Addresses

IN THIS CHAPTER

- [About the Addresses Page | 859](#)
- [Variable Address Overview | 862](#)
- [Create Addresses or Address Groups | 863](#)
- [Import and Export Addresses | 868](#)
- [Merge Duplicate Addresses | 870](#)
- [Replace Addresses in Bulk | 872](#)
- [Edit, Clone, and Delete Addresses and Address Groups | 872](#)

About the Addresses Page

IN THIS SECTION

- [Tasks You Can Perform | 860](#)
- [Field Descriptions | 861](#)

To access this page, select **Shared Services > Objects > Addresses**.

An address specifies an IP address or a hostname. You can create addresses that you can use across all policies. Addresses are used in firewall and NAT services and apply to the corresponding policies. You can also resolve an IP address to the corresponding hostname.

Juniper Security Director Cloud manages its address book at the global level, assigning objects to devices that are required to create policies. An address book is a collection of addresses and address groups. If the device is capable of using a global address book, Juniper Security Director Cloud pushes address objects used in the policies to the global address book of the device.

Use this page to create, edit, clone, and delete addresses and address groups, and manage addresses. Addresses and address groups are used in firewall and NAT services. After you create an address, you can combine it with other addresses to form an address group. Address groups are useful when you want to apply the same policy to multiple services.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create an address or address group. See ["Create Addresses or Address Groups" on page 863](#) .
- Modify, clone, or delete an address or address group. See ["Edit, Clone, and Delete Addresses and Address Groups" on page 872](#) .
- Import and export the addresses data to a CSV file. See ["Import and Export Addresses" on page 868](#) .
- Merge duplicate addresses. See ["Merge Duplicate Addresses" on page 870](#) .
- Replace addresses in bulk. See ["Replace Addresses in Bulk" on page 872](#)
- View the configured parameters of an address or address group. Click **More** > **Detailed View**.
- View duplicate addresses. Click **View** and select **Duplicate addresses** from the drop-down list.
- View the network components associated with an address. Click **View Associations** to open the View Associations page which displays the components, such as NAT policies and SRX policies associated with the address. Hover your cursor over the network component to view the associated objects.
- View all addresses or unused addresses. Select an option in the **View by** drop-down list. You can view the unused addresses to delete specific or all the unused addresses. You can also further search the unused addresses list and filter the list based on your search keywords.
- Show or hide columns about the address or address group. Click the **Show Hide columns** icon in the top-right corner of the page, and select columns to view on the page.
- Filter information based on select criteria. You can add filters, save the filters, and set any of the filters as default.
 1. Click the filter icon on the top-right corner of the page, and select **Add Filter** to open the Add Criteria page.
 2. Set the filter conditions, and click **Add**.

The filter is saved and applied to the data on the page.

To remove the filter, click the filter icon, and select **Hide Filter**.

- Search for an address or address group.
 1. Click the search icon in the top-right corner of the page to search for an address or address group.
 2. Enter keywords or partial keywords in the text box, and press **Enter**.

The search results are displayed on the same page.

Field Descriptions

[Table 309 on page 861](#) provides guidelines on using the fields on the Addresses page.

Table 309: Fields on the Addresses Page

Field	Description
Name	The name of the address or address group.
Type	The type of the address object.
Hostname	The hostname of the address.
IP Address	The IP address associated with the address.
Description	The description about the address or address group which was entered when the address or address group was created.

RELATED DOCUMENTATION

[Create Addresses or Address Groups | 863](#)

[Edit, Clone, and Delete Addresses and Address Groups | 872](#)

[Import and Export Addresses | 868](#)

[Merge Duplicate Addresses | 870](#)

[Replace Addresses in Bulk | 872](#)

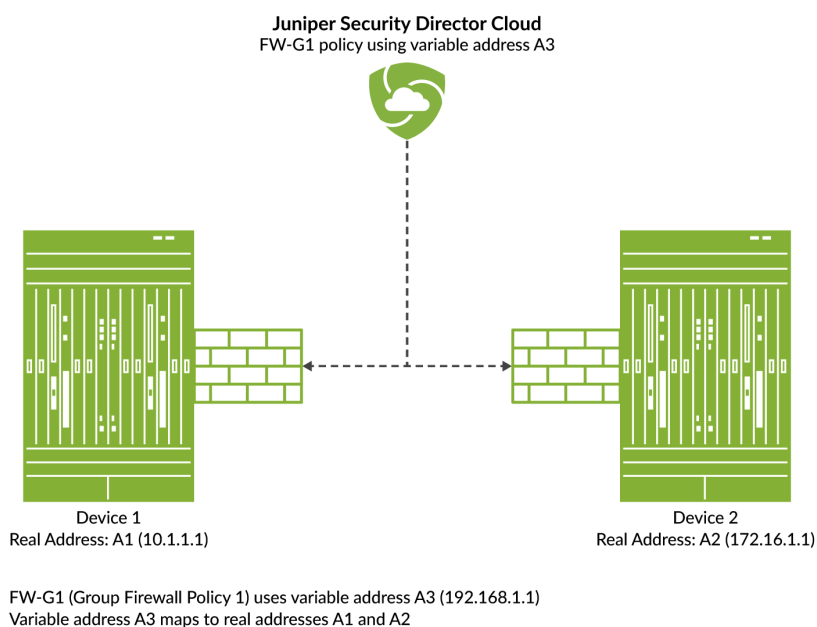
Variable Address Overview

A variable is useful when you want to apply similar rules across devices where only the address might differ. Instead of using static values, you can use variables to create fewer rules and use them more widely. You can achieve this by creating and configuring a variable address for all devices to which you are applying a group policy.

For example:

- Group firewall policy **FW-G1** has two devices, **Dev-1** and **Dev-2**. Each device has its own unique address. **Dev-1** has address *A1*. **Dev-2** has address *A2*.
- You want to apply the same rule to both devices, but you do not want to configure two rules with all the same criteria except for the address. It is more efficient to configure one rule with a variable default address and apply it to both devices.
- You can achieve this by creating an address variable with a default address *A3*, and making *A3* common to **Dev-1** and **Dev-2** in your rule. When you configure default address *A3*, you map it to the real address of each device, *A1* for **Dev-1** and *A2* for **Dev-2**.
- When group firewall policy **FW-G1** is applied, these mappings are used to replace the default address with the real address for each device.
- **NOTE:** Variable addresses are used in group policies only. Variable addresses are not applicable to device policies.

Figure 28: Variable Address Usage



Create Addresses or Address Groups

Use the **Addresses** page to create addresses and address groups. Addresses and address groups are used in firewall and NAT services. After you create an address, you can combine it with other addresses to form an address group. Address groups are useful when you want to apply the same policy to multiple services.

To create an address or address group:

1. Select **Shared Services > Objects > Addresses**.

The **Addresses** page appears.

2. Click the add icon (+).

The **Create Addresses** page appears.

3. Complete the configuration according to the guidelines provided in [Table 310 on page 864](#) and [Table 311 on page 867](#).

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

A new address or address group with your configurations is created. You can use this object in firewall or NAT policies.

Table 310: Fields on the Create Addresses Page

Field	Description
Name	<p>Enter a unique name for the address. The name must begin with an alphanumeric character and can contain alphanumeric characters and some special characters (colons, hyphens, forward slashes, periods, and underscores). The maximum length is 63 characters.</p>
Description	<p>Enter a description for your address. The description can contain alphanumeric characters and special characters (excluding ampersand, lesser than (<) and greater than (>), and newline (\n)). The maximum length is 900 characters.</p> <p>You should make this description as useful as possible for all administrators.</p>
Object Type	<p>Select Address or Address Group. If you select Address Group, then the screen changes so you can select the addresses you want to include in your address group. Table 311 on page 867 describes address group configuration parameters.</p>

Table 310: Fields on the Create Addresses Page (Continued)

Field	Description
Type	<p>Select a type of address and fill in the corresponding fields. Available types are:</p> <ul style="list-style-type: none"> • Host <ul style="list-style-type: none"> • Host IP—Enter the IPv4 host IP address. For example: 192.0.2.0. If you do not know the IP address, you can enter the hostname and click Look up hostname. • Hostname—Enter the hostname. It must begin with an alphanumeric character and cannot exceed 63 characters. Dashes and underscores are allowed. If you do not know the host name, you can enter the IP address and click Look up IP address. For example, enter www.company.com and click Look up IP address. Hostname lookup is supported for IPv4 addresses. • Range <ul style="list-style-type: none"> • Start Address—Enter a starting IPv4 address along with the classless inter-domain routing (CIDR) for the address range. For example: 192.0.2.0/24. • End Address—Enter an ending IPv4 address for the address range. The range is validated after you enter the address. <p>NOTE: An address range is configured on a managed device as an address set with one or more network address objects covering the specified address range.</p> • Network <ul style="list-style-type: none"> • Network—Enter the network IP address. For example: 192.0.2.0. IPv6 is also supported.

Table 310: Fields on the Create Addresses Page (Continued)

Field	Description
	<p>For example: 2001:db8:4136:e378:8000:63bf:3fff:ddd2.</p> <ul style="list-style-type: none"> • Subnet Mask—Enter the subnet mask for the network range. For example, IPv4 netmask: 192.0.2.0/24. IPv6 prefix: 2001:db8::/32 The subnet mask is validated as you enter it. You must enter the correct subnet mask in accordance with the network value. • DNS Host <ul style="list-style-type: none"> • DNS Name—Enter the DNS name. For example: company.com. Only alphanumeric characters, dashes, and periods are accepted. This name cannot exceed 63 characters in length, and must end with an alphanumeric character. • DNS Type—Select the DNS type as IPv4-only or IPv6-only. • Variable <ul style="list-style-type: none"> • Default address—This default address is replaced with the mapped device-specific address when applied to the group firewall policy. • Variable address—Steps to add the variable address: <ul style="list-style-type: none"> a. Click the add icon (+). Create variable page appears. b. Select the check box beside each device to which you want to map this variable address. Click the arrow to move the selected device or devices from the Available column to the Selected column.

Table 310: Fields on the Create Addresses Page (Continued)

Field	Description
	<p>Only devices from the current and child domain are listed. You can use the fields at the top of each column to search for listed devices.</p> <p>c. Select a predefined address by clicking anywhere within this field and choosing an address from the Select Address window. The default address is replaced by this device-specific address when applied to a policy that includes the selected device or device</p> <p>d. Click OK. A new variable with your configurations is created. You can use this variable address in policies. See "Select a Security Policy Rule Source" on page 318 and "Select a Security Policy Rule Destination" on page 319</p> <p>NOTE: Variables addresses are used in group policies only. Variable addresses are not applicable to device policies.</p>

Table 311: Address Group Settings

Field	Description
Name	<p>Enter a unique name for the address group that must begin with an alphanumeric character. The name can contain alphanumeric characters and some special characters (colons, hyphens, forward slashes, periods, and underscores). The maximum length is 63-character.</p>

Table 311: Address Group Settings (Continued)

Field	Description
Description	<p>Enter a description for your address. The description can contain alphanumeric characters and special characters (excluding ampersand, lesser than (<) and greater than (>), and newline (\n)). The maximum length is 900 characters.</p> <p>You should make this description as useful as possible for all administrators.</p>
Object Type	<p>Select Address or Address Group. If you select Address Group, then the screen changes so you can select the addresses you want to include in your address group.</p>
Addresses	<p>Select the check box beside each address you want to include in the address group. Click the greater-than icon (>) to move the selected address or addresses from the Available column to the Selected column. Note that you can use the fields at the top of each column to search for addresses.</p>

RELATED DOCUMENTATION

[About the Addresses Page | 859](#)

[Edit, Clone, and Delete Addresses and Address Groups | 872](#)

[Variable Address Overview | 862](#)

Import and Export Addresses

IN THIS SECTION

[Import Addresses from a CSV File | 869](#)

● Export Addresses to a CSV File | 870

The bulk import and export of addresses feature is a useful tool for managing large-scale networks efficiently. The benefits of such a feature include:

- **Time-saving:** You can create or modify multiple addresses simultaneously. This saves time and effort compared to manually creating or modifying addresses one by one.
- **Accuracy:** By using the import and export feature, you can avoid errors that can occur when manually creating or modifying addresses. With this feature, you can ensure that all addresses are created or modified according to a predefined format, which increases accuracy.
- **Scalability:** As network infrastructures grow larger, it becomes increasingly difficult to manage them effectively. The import and export feature helps you to scale up your network management capabilities to accommodate growing networks.
- **Standardization:** When you create or modify addresses using the import and export feature, you can ensure that you adhere to a predefined set of standards. This helps maintain consistency across the network and avoids potential configuration errors.
- **Flexibility:** You can use the import and export feature to move addresses between different systems or locations, which can be useful when migrating to new systems or consolidating multiple networks.

The bulk import and export of addresses can help you manage large-scale networks more efficiently, accurately, and consistently. This feature can save time, improve accuracy, and facilitate scalability and standardization of addresses across the network.

Import Addresses from a CSV File

1. Click [Shared Services](#)>[Objects](#)>[Addresses](#).

The Addresses page opens.

2. Download the CSV file template, and enter your address data.

a. Click **More > Import addresses from CSV** to open the Import Addresses from CSV page.

b. Click **Download CSV template** to download the CSV template file on to your computer.

c. Add your addresses in the CSV template.

3. Click [More > Import addresses from CSV](#).

4. Do the following:

a. **Upload CSV:** Select the CSV file to import the addresses.

b. **Global Action:** Select one of the following actions for Juniper Security Director Cloud to resolve any conflicts between the imported and existing addresses data:

- **Keep existing:** If you select to keep the existing data, a tick mark identifies the values of the addresses data that will not be imported.
- **Create new object**
- **Overwrite with imported value:** If you select to overwrite the existing data, a tick mark identifies the data that will overwrite the values of the existing addresses.

5. Click **Upload**.

- Before Juniper Security Director Cloud imports the the data from the CSV file, it analyzes the address data for errors. If it detects errors, such as incorrect IP addresses or incorrect address types, it adds a column in the CSV file and indicates the errors against each entry. You can download the updated CSV file and fix the errors.

- If no errors are detected in the CSV file, the file is uploaded to import the address data.

6. Optional: If Juniper Security Director Cloud detects errors in the CSV file, download the updated CSV file, fix the indicated errors, and click **Upload** to upload the file again.

7. Click **OK**.

All data conflicts is resolved based on the actions you select, and the addresses data is imported from the CSV file and displayed on the Addresses page.

Export Addresses to a CSV File

Click **More**, and do one of the following:

- Select the addresses to export, and click **Export selected addresses to CSV**.
- Click **Export all addresses to CSV** to export all addresses.

The addresses data is downloaded to your computer as a CSV file.

Merge Duplicate Addresses

Multiple users create various objects in a network which sometimes results in users creating duplicate objects, such as duplicate addresses. Such duplicate addresses clutter the network space and confuse users. You can optimize network space usage by keeping the network clean and optimizing the resource usage.

Use the duplicate address detection feature to find duplicate addresses and merge the addresses into one address object.

1. Click **Shared Services > Objects > Addresses**.

The Addresses page opens.

2. Click **View** and select **Duplicate addresses** from the drop-down list.

The list of addresses with duplicate entries is displayed.

3. Select the duplicate addresses to merge and click **Merge Duplicate Address**.

The Merge Duplicate Addresses page opens.

4. Select one of the following:

- **Select an existing name**—Select a name from the drop-down list.
- **Enter a new name**—Enter a name and description for the merged address according to the guidelines in [Table 312 on page 871](#).

Table 312: Fields on the Merge Duplicate Addresses Page

Field	Description
Name	<p>Enter a unique name for the address containing maximum 63 characters without spaces.</p> <p>The name must begin with an alphanumeric character and can contain special characters such as colons, hyphens, forward slashes, periods, and underscores.</p>
Description	<p>Enter a description for the address containing maximum 900 characters.</p> <p>The description can contain alphanumeric characters and special characters except ampersand, lesser than sign, greater than sign, or a new line.</p> <p>You should make this description as useful as possible for all administrators.</p>

Juniper Security Director Cloud identifies the usage of the duplicate addresses across all features and displays a message asking for confirmation about the merge operation.

Hover your cursor over the network components to view the objects where the duplicate addresses are used.

5. Click **Yes**.

Juniper Security Director Cloud merges the duplicate addresses and displays the updated list with unique addresses.

RELATED DOCUMENTATION

[About the Addresses Page | 859](#)

[Replace Addresses in Bulk | 872](#)

Replace Addresses in Bulk

Manage addresses in your network efficiently and keep your firewall policies updated with correct addresses by replacing addresses in bulk.

1. Click **Shared Services > Objects > Addresses**.

The Addresses page opens.

2. Select the addresses to replace.

Ensure that the list of addresses is not filtered. Click **View** and select **All addresses**.

3. Click **View > Replace addresses across features**.

The Replace Addresses Across Features page opens.

4. Select an address from the **Replace selected addresses with** drop-down list and click **OK**.

Juniper Security Director Cloud identifies the usage of the selected addresses across all features and displays a message asking for confirmation about the replace operation.

Hover your cursor over the network components to view the objects where the addresses are used.

5. Click **Yes**.

Juniper Security Director Cloud replaces the selected addresses with the new address.

RELATED DOCUMENTATION

[About the Addresses Page | 859](#)

[Merge Duplicate Addresses | 870](#)

Edit, Clone, and Delete Addresses and Address Groups

IN THIS SECTION

- [Edit Addresses and Address Groups | 873](#)

- [Clone Addresses and Address Groups | 873](#)
- [Delete Addresses and Address Groups | 874](#)

You can edit, clone, and delete addresses and address groups from the **Addresses** page.

NOTE:

- You cannot edit or delete predefined addresses.
- You cannot edit or delete the GeolP feeds from the Addresses page. You can edit or delete the GeolP feeds from the **Shared Services > Objects > GeolP** page.

Edit Addresses and Address Groups

To modify the parameters configured for an address or address group:

1. Select **Shared Services > Objects > Addresses**.

The **Addresses** page appears.

2. Select the address or address group that you want to edit and click the edit icon (pencil symbol) at the right top corner of the table.

The **Edit Address** page appears, showing the same options as displayed when you create a new address or address group.

3. Modify the parameters according to the guidelines provided in "[Create Addresses or Address Groups](#)" on page 863 .

NOTE: Address Name and Object Type can not be modified.

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

When you click **OK**, the modified address or address group is displayed on the **Addresses** page.

NOTE: When you edit an address that is a deployed as part of a policy, you will need to redeploy that policy in order for the changes to take effect.

Clone Addresses and Address Groups

To clone an address or address group:

1. Select **Shared Services > Objects > Addresses**.

The **Addresses** page appears.

2. Right-click the address or address group that you want to clone and then click **Clone**, or select **More > Clone**.

The **Clone Address** page appears with editable fields.

3. Modify the parameters according to the guidelines provided in "[Create Addresses or Address Groups](#)" on page 863 .
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.
If you select **OK**, the cloned address or address group is saved.

Delete Addresses and Address Groups

NOTE: Only addresses or address groups that have not been referenced in any policy can be deleted. If you try to delete such an address or address group, an error message will be displayed.

To delete an address or address group:

1. Select **Shared Objects > Objects > Addresses**.

The **Addresses** page appears.

2. Select the address or address group you want to delete and then click the delete icon (trash can).

An alert message appears verifying that you want to delete your selection.

3. Click **Yes** to delete the address or address group. If you do not want to delete, click **Cancel** instead.
If you select **Yes**, the selected address or address group is deleted, unless it is referenced in a policy.

SEE ALSO

[About the Addresses Page | 859](#)

[Create Addresses or Address Groups | 863](#)

Objects-GeoIP

IN THIS CHAPTER

- [About the GeoIP Page | 875](#)
- [Create a GeoIP Feed | 876](#)
- [Edit, Clone, and Delete GeoIP Feeds | 878](#)

About the GeoIP Page

IN THIS SECTION

- [Tasks You Can Perform | 875](#)
- [Field Descriptions | 876](#)

To access this page, select **Shared Services > Objects > GeoIP**

IP-based geolocation (GeoIP) is the method of locating a computer terminal's geographic location by identifying that terminal's IP address. A GeoIP feed is an up-to-date mapping of IP addresses to geographical regions. By mapping an IP address to the sources of attack traffic, geographic regions of origin can be determined, giving you the ability to filter traffic to and from specific locations in the world.

Using Juniper Security Director Cloud, you can create, modify, or delete the GeoIP feeds. You can use the GeoIP feeds in security policy to deny or allow traffic based on source or destination IP address.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a GeoIP feed. See ["Create a GeoIP Feed" on page 876](#) .
- Modify, clone, or delete a GeoIP feed. See ["Edit, Clone, and Delete GeoIP Feeds" on page 878](#) .

- View the configured parameters of GeolIP feed. Click the details icon that appears when you hover over the name of a GeolIP feed or select **More > Detailed View**.
- Show or hide columns about the GeolIP feed. Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Filter information based on select criteria. You can add filters, save the filters, and set any of the filters as default. To add a filter:
 1. Click on the filter icon on the top-right corner of the page and select **Add Filter** to open the Add Criteria page.

2. Set the filter conditions and click **Add**.

The filter is saved and applied on the page. You can save the filter and can mark any one filter as default.

To remove the filter, click the filter icon and select **Hide Filter**.

- Search for a GeolIP feed. Click the Search icon in the top right corner of the page to search for a GeolIP feed. Type partial or full text of the keyword in the text box and press Enter.

You can view the search results on the same page.

Field Descriptions

[Table 313 on page 876](#) provides guidelines on using the fields on the GeolIP page.

Table 313: Fields on the GeolIP Page

Field	Description
Name	View the name of the GeolIP feed.
Description	View the description about the GeolIP feed.
Countries	View the countries included in the GeolIP feed.

Create a GeolIP Feed

You can create GeolIP feeds from the **GeolIP** page.

Before You Begin

- You must have Juniper ATP Cloud account. Make sure you configure the necessary steps for Juniper ATP Cloud before creating a GeolP feed. See [Juniper Advanced Threat Prevention Cloud Installation Overview](#) for more details.
- GeolP filtering is a useful tool when you are experiencing certain types of attacks, such as DDoS from specific geographical locations.
- If you are using Juniper ATP Cloud, you must select your GeolP feed as the source or destination of a security policy rule to apply it.

To create a GeolP feed:

1. Select **Shared Services > Objects > GeolP**.

The **GeolP** page appears.

2. Click the add icon (+).

The **Create GeolP** page appears.

3. Complete the configuration according to the guidelines provided in and ["Create a GeolP Feed" on page 876](#).

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

A new GeolP feed is created and listed as a dynamic address group entry on the **Shared Services > Objects > Addresses** page. You can use this GeolP feed as address group to specify the source or destination address while creating security policy rules.

Table 314: Fields on the Create GeolP Page

Field	Description
Name	Enter a unique name containing maximum 63 characters without spaces. The name must begin with an alphanumeric character and can contain special characters such as colons, periods, dashes, and underscores.
Description	Enter a description that contains alphanumeric characters and special characters (excluding ampersand, lesser than (<) and greater than (>), and newline ()). The maximum length is 900 characters.

Table 314: Fields on the Create GeolP Page (Continued)

Field	Description
Countries	Select the check box beside the countries in the Available list and click the > icon to move to the Selected list. The countries in the Selected list are included in the feed to take action according to their threat level. You can use the search at the top of each column to search for the listed countries.

RELATED DOCUMENTATION

[Edit, Clone, and Delete Addresses and Address Groups | 872](#)

[About the Addresses Page | 859](#)

Edit, Clone, and Delete GeolP Feeds

IN THIS SECTION

- [Edit a GeolP Feed | 878](#)
- [Clone a GeolP Feed | 879](#)
- [Delete a GeolP Feed | 879](#)

You can edit, clone, and delete GeolP feeds from the **GeolP** page.

Edit a GeolP Feed

To modify the parameters configured for a GeolP feed:

1. Select **Shared Services > Objects > GeolP**.
The **GeolP** page appears.
2. Select the GeolP feed to edit and click the edit icon (pencil symbol) at the right top corner of the table.

The **Edit GeolP** page appears, showing the same options as displayed when you create a GeolP feed.

3. Modify the parameters according to the guidelines provided in "[Create a GeolP Feed](#)" on page 876 .
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

When you click **OK**, the modified GeolP feed is displayed on the **GeolP** page.

NOTE: When you edit a GeolP feed that is a deployed as part of a security policy, you must redeploy that policy for the changes to take effect.

Clone a GeolP Feed

To clone a GeolP feed:

1. Select **Shared Services > Objects > GeolP**.

The **GeolP** page appears.

2. Right-click the GeolP feed that you want to clone and then click **Clone**, or select **More > Clone**.

The **Clone GeolP** page appears with editable fields.

3. Modify the parameters according to the guidelines provided in "[Create a GeolP Feed](#)" on page 876 .
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

If you select **OK**, the cloned GeolP feed is saved.

Delete a GeolP Feed

NOTE: You can delete only those GeolP feeds that are not referenced in any policy.

To delete a GeolP feed:

1. Select **Shared Services > Objects > GeolP**.

The **GeolP** page appears.

2. Select the GeolP feed you want to delete and then click the delete icon (trash can).

An alert message appears verifying that you want to delete your selection.

3. Click **Yes** to delete the GeolP feed. If you do not want to delete, click **Cancel** instead.

If you select **Yes**, the selected GeolP feed is deleted, unless it is referenced in a policy.

SEE ALSO

[About the GeolP Page](#) | 875

[Create a GeolP Feed](#) | 876

[About the Addresses Page | 859](#)

[Create Addresses or Address Groups | 863](#)

Objects-Services

IN THIS CHAPTER

- [About the Services Page | 881](#)
- [Create Services and Service Groups | 883](#)
- [Import and Export Services | 886](#)
- [Merge Duplicate Services | 888](#)
- [Replace Services in Bulk | 889](#)
- [Edit, Clone, and Delete Services and Service Groups | 890](#)
- [Create Protocols | 892](#)
- [Edit and Delete Protocols | 896](#)

About the Services Page

IN THIS SECTION

- [Tasks You Can Perform | 882](#)
- [Field Descriptions | 883](#)

To access this page, select **Shared Services > Objects > Services**.

Use the **Services** page to create, modify, clone and delete services or service groups and import and export services to a CSV file. You can also create and manage protocols that you use to create services.

A service refers to an application on a device, such as Domain Name Service (DNS). Services are based on protocols and ports used by an application. When added to a policy, a configured service can be applied across all devices associate with it. The protocols available to create a service include: TCP, UDP, SUN-RPC, MS-RPC, ICMP, ICMPv6, and Other.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a service or service group. See ["Create Services and Service Groups" on page 883](#) .
- Modify, clone or delete a service or service group. See ["Edit, Clone, and Delete Services and Service Groups" on page 890](#) .
- Merge duplicate services. See ["Merge Duplicate Services" on page 888](#) .
- Replace services in bulk. See ["Replace Services in Bulk" on page 889](#)
- View the configured parameters of a service or service group. Click the details icon that appears when you hover over the name of a service or service group, or click **More > Detailed View**.
- Import and export the services data to a CSV file. See ["Import and Export Services" on page 886](#) .
- View the network components associated with a service. Click **View Associations** to open the View Associations page which displays the components, such as NAT policies and SRX policies associated with the service. Hover your cursor over the network component to view the associated objects.
- View all services or unused services. Select an option in the **View by** drop-down list. You can view the unused services to delete specific or all the unused services. You can also further search the unused services list and filter the list based on your search keywords.
- Show or hide columns about the services or service groups. Click the **Show Hide columns** icon in the top- right corner of the page and select columns to view on the page.
- Filter information based on select criteria. You can add filters, save the filters, and set any of the filters as default. To add a filter:
 1. Click on the filter icon on the top-right corner of the page and select **Add Filter** to open the Add Criteria page.
 2. Set the filter conditions and click **Add**.

The filter is saved and is applied on the data on the page. You can mark any one filter as default.

To remove the filter, click the filter icon and select **Hide Filter**.

- Search a specific service or service group. Click the Search icon in the top right corner of the page to search for a service or service group.

You can enter partial text or full text of the keyword in the text box and press Enter.

The search results are displayed on the same page.

Field Descriptions

Table 315 on page 883 provides guidelines on using the fields on the **Services** page.

Table 315: Fields on the Service Page

Field	Description
Name	Name of the service or service group.
Type	Specifies whether the object is a service or service group.
Description	Description about the service or service group.
Predefined/Custom	Indicates whether a service or service group is predefined or custom.

RELATED DOCUMENTATION

[Create Services and Service Groups | 883](#)

[Edit, Clone, and Delete Services and Service Groups | 890](#)

[Merge Duplicate Services | 888](#)

[Replace Services in Bulk | 889](#)

[Create Protocols | 892](#)

[Edit and Delete Protocols | 896](#)

Create Services and Service Groups

Use the **Create Service** page to create a service. You can create services based on protocols and ports used by an application. You can use protocols such as TCP, UDP, MS-RPC, SUN-RPC, ICMP, ICMPv6, and so on, to create services. Once you create a service, you can combine it with other services to form a service group. Service groups are useful when you want to apply the same policy to multiple services.

You can also create or modify service-based protocols from the **Services** page.

To configure a service or service group:

1. Select **Shared Services > Objects > Services**.

The **Services** page appears.

2. Click the add icon (+) to create service or service group.

The **Create Service** page appears.

3. Complete the configuration of a service according to the guidelines provided in [Table 316 on page 884](#).

If you want to configure a service group, see [Table 317 on page 885](#).

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

A new service or service group with the configuration you provided is created. You can use this service or service group as an endpoint in firewall policies.

[Table 316 on page 884](#) provides guidelines on using the fields to create a service.

Table 316: Create Service Settings

Field	Description
Name	Enter a unique name for the service. The name must begin with an alphanumeric character and can contain alphanumeric characters and some special characters (colons, hyphens, forward slashes, periods, and underscores); 63-character maximum.
Description	Enter a description for your service. The description can contain alphanumeric characters and special characters (excluding ampersand, lesser than (<) and greater than (>), and newline (\n)); 900-character maximum. You should make this description as useful as possible for all administrators.
Type	Select Service or Service Group . If you select Service Group , then the page changes so you can select the services you want to include in your service group. See Table 316 on page 884 .

Table 316: Create Service Settings *(Continued)*

Field	Description
Protocols	<p>Select the protocol you want to associate with the service. You can also create a new protocol, or edit existing protocols:</p> <ul style="list-style-type: none"> To create a new protocol, click on the add icon (+). See "Create Protocols" on page 892 . To edit an existing protocol, click on the edit icon (pencil symbol). See "Edit and Delete Protocols" on page 896 .

[Table 317 on page 885](#) provides guidelines on using the fields to create a service group.

Table 317: Service Group Settings

Field	Description
Name	Enter a unique name for the service group. The name must begin with an alphanumeric character and can contain alphanumeric characters and some special characters (colons, hyphens, forward slashes, periods, and underscores); 63-character maximum.
Description	<p>Enter a description for your service group. The description can contain alphanumeric characters and special characters (excluding ampersand, lesser than (<) and greater than (>), and newline (\n)); 900-character maximum.</p> <p>You should make this description as useful as possible for all administrators.</p>
Type	Select Service or Service Group . If you select Service Group , then the screen changes so you can select the services you want to include in your service group.

Table 317: Service Group Settings (Continued)

Field	Description
Services	Select the service you want to include in the service group and click the greater-than icon (>) to move the selected service or services from the Available column to the Selected column. You can use the search field at the top of each column to search for listed services.

RELATED DOCUMENTATION

[About the Services Page | 881](#)

[Edit, Clone, and Delete Services and Service Groups | 890](#)

[Create Protocols | 892](#)

[Edit and Delete Protocols | 896](#)

Import and Export Services

IN THIS SECTION

- [Import Services from a CSV File | 887](#)
- [Export services to a CSV File | 888](#)

The bulk import and export of services feature is a useful tool for managing large-scale networks efficiently. The benefits of such a feature include:

- **Time-saving:** You can create or modify multiple services simultaneously. This saves time and effort compared to manually creating or modifying services one by one.
- **Accuracy:** By using the import and export feature, you can avoid errors that can occur when manually creating or modifying services. With this feature, you can ensure that all services are created or modified according to a predefined format, which increases accuracy.

- **Scalability:** As network infrastructures grow larger, it becomes increasingly difficult to manage them effectively. The import and export feature helps you to scale up your network management capabilities to accommodate growing networks.
- **Standardization:** When you create or modify services using the import and export feature, you can ensure that you adhere to a predefined set of standards. This helps maintain consistency across the network and avoids potential configuration errors.
- **Flexibility:** You can use the import and export feature to move services between different systems or locations, which can be useful when migrating to new systems or consolidating multiple networks.

The bulk import and export of services can help you manage large-scale networks more efficiently, accurately, and consistently. This feature can save time, improve accuracy, and facilitate scalability and standardization of addresses across the network.

Import Services from a CSV File

1. Click **Shared Services>Objects>Services**.

The Services page opens.

2. Download the CSV file template, and enter your services data.

- a. Click **More > Import addresses from CSV**, to open the Import services from CSV page.
- b. Click **Download CSV template** to download the CSV template file on to your computer.
- c. Add your services data in the CSV template.

3. Click **More>Import services from CSV**.

4. Do the following:

- a. **Upload CSV:** Select the CSV file to import the services.
- b. **Global Action:** Select one of the following actions for Juniper Security Director Cloud to resolve any conflicts between the imported and existing services data:
 - **Keep existing:** If you select to keep the existing data, a tick mark identifies the values of the services data that will not be imported.
 - **Create new object**
 - **Overwrite with imported value:** If you select to overwrite the existing data, a tick mark identifies the data that will overwrite the values of the existing services.

5. Click **Upload**.

- Before Juniper Security Director Cloud imports the the data from the CSV file, it analyzes the services data for errors. If it detects errors, such as incorrect IP addresses or incorrect services types, it adds a column in the CSV file and indicates the errors against each entry. You can download the updated CSV file and fix the errors.

- If no errors are detected in the CSV file, the file is uploaded to import the services data.
6. Optional: If Juniper Security Director Cloud detects errors in the CSV file, download the updated CSV file, resolve the errors, and upload the file again.
 7. Click **OK**.

All data conflicts are resolved, and the services data is imported from the CSV file and displayed on the services page.

Export services to a CSV File

1. Click **Shared Services > Objects > Services**.
The Services page opens.
2. Click **More**, and do one of the following:
 - Select the services to export, and click **Export selected services to CSV**.
 - Click **Export all services to CSV** to export all services.

The services data is downloaded to your computer as a CSV file.

Merge Duplicate Services

Multiple users create various objects in a network which sometimes results in users creating duplicate objects, such as duplicate services. Such duplicate services clutter the network space and confuse users. You can optimize network space usage by keeping the network clean and optimizing the resource usage.

Use the duplicate services detection feature to find duplicate services and merge the services into one services object.

1. Click **Shared Services > Objects > Services**.
The Services page opens.
2. Click **View** and select **Duplicate services** from the drop-down list.
The list of services with duplicate entries is displayed.
3. Select the duplicate addresses to merge and to click **Merge Duplicate services**.
The Merge Duplicate Services page opens.
4. Select one of the following:
 - **Select an existing name**—Select a name from the drop-down list.
 - **Enter a new name**—Enter a name and description for the merged address according to the guidelines in [Table 318 on page 889](#).

Table 318: Fields on the Merge Duplicate Services Page

Field	Description
Name	<p>Enter a unique name for the service containing maximum 63 characters without spaces.</p> <p>The name must begin with an alphanumeric character and can contain special characters such as colons, hyphens, forward slashes, periods, and underscores.</p>
Description	<p>Enter a description for the service containing maximum 900 characters.</p> <p>The description can contain alphanumeric characters and special characters except ampersand, lesser than sign, greater than sign, or a new line.</p> <p>You should make this description as useful as possible for all administrators.</p>

Juniper Security Director Cloud identifies the usage of the duplicate services across all features and displays a message asking for confirmation about the merge operation.

Hover your cursor over the network components to view the objects where the duplicate services are used.

5. Click **Yes**.

Juniper Security Director Cloud merges the duplicate services and displays the updated list with unique services.

RELATED DOCUMENTATION

[About the Services Page | 881](#)

[Replace Services in Bulk | 889](#)

Replace Services in Bulk

Manage services in your network efficiently and keep your firewall policies updated with correct services by replacing services in bulk.

1. Click **Shared Services > Objects > Services**.

The Services page opens.

2. Select the services to replace.

Ensure that the list of services is not filtered. Click **View** and select **All services**.

3. Click **View > Replace services across features**.

The Replace Services Across Features page opens.

4. Select the services from the **Replace selected services with** drop-down list and click **OK**.

Juniper Security Director Cloud identifies the usage of the selected services across all features and displays a message asking for confirmation about the replace operation.

Hover your cursor over the network components to view the objects where the services are used.

5. Click **Yes**.

Juniper Security Director Cloud replaces the selected services with the new services.

RELATED DOCUMENTATION

[About the Services Page | 881](#)

[Merge Duplicate Services | 888](#)

Edit, Clone, and Delete Services and Service Groups

IN THIS SECTION

- [Edit Services and Service Groups | 891](#)
- [Clone Services or Service Groups | 891](#)
- [Delete Services and Service Groups | 891](#)

You can edit, clone, and delete services and service groups from the **Services** page.

NOTE:

- You cannot edit or delete predefined services, however, you can clone predefined services.
- You cannot delete services or service groups that are in use.

Edit Services and Service Groups

To modify the parameters configured for a service or service group:

1. Select **Shared Services > Objects > Services**.

The **Services** page appears.

2. Select the service or service group that you want to edit, and click on the edit icon (pencil symbol) on the right top corner of the table.

NOTE: You cannot modify the service or service group Name or the Object Type.

The **Edit Service** page appears, displaying the same options that are displayed when creating a new service or service group.

3. Modify the parameters according to the guidelines provided in "[Create Services and Service Groups](#)" on page 883 .
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.
If you click **OK**, you will see the modified service or service group in the **Services** page.

Clone Services or Service Groups

To clone a service or service group:

1. Select **Shared Services > Objects > Services**.

The **Services** page appears.

2. Right-click on the service or service group that you want to clone and then click **Clone**, or select **More > Clone**.

The **Clone Service** page appears with editable fields. Modify the parameters as required according to the guidelines provided in "[Create Services and Service Groups](#)" on page 883 .

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

If you click **OK**, the cloned service or service group will appear beneath the selected service or service group.

Delete Services and Service Groups

To delete a service or service group:

1. Select **Shared Services > Objects > Services**.
The **Services** page appears.
2. Select the service or service group you want to delete and then click the delete icon (trash can).
An alert message appears, verifying that you want to delete the service or service group.
3. Click **Yes** to delete the service or service group. If you do not want to delete, click **Cancel** instead.
If you click **Yes**, the selected service or service group is deleted.

SEE ALSO

[About the Services Page | 881](#)

[Create Services and Service Groups | 883](#)

[Create Protocols | 892](#)

[Edit and Delete Protocols | 896](#)

Create Protocols

Use the **Create Protocol** page to create TCP, UDP, MS-RPC, SUN-RPC, ICMP, ICMPv6, and other protocols, that can be used in services. A service refers to an application on a device. Services are based on protocols and ports used by an application.

To create a protocol:

1. Select **Shared Services > Objects > Services**.
The **Services** page appears.
2. Click the add icon (+) to create service or service group.
The **Create Services** page appears.
3. Click the add icon (+) that appears above the **Protocols** table.
The **Create Protocol** page appears.
4. Complete the configuration of the protocol according to the guidelines provided in [Table 319 on page 893](#) and [Table 320 on page 894](#) .
5. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.
A new protocol with the configuration you provided is created within the service.

[Table 319 on page 893](#) provides guidelines on using the fields to create a protocol.

Table 319: Fields on Create Protocol Page Settings

Field	Description
General Information	
Name	Enter a unique name for the protocol. The name must begin with an alphanumeric character and can contain alphanumeric characters and some special characters (colons, hyphens, forward slashes, periods, and underscores); 63-character maximum.
Description	Enter a description for your protocol. The description can contain alphanumeric characters and special characters (excluding ampersand, lesser than (<) and greater than (>), and newline (\n)); 900-character maximum. You should make this description as useful as possible for all administrators.
Type	Select the type of the protocol you want to create and fill in the corresponding fields. The available types of protocols are: TCP, UDP, ICMP, SUN-RPC, MS-RPC, ICMPv6, and so on. If you select TCP or UDP, continue with this table. See Table 320 on page 894 for the other protocol types.
Destination Port	Enter a destination port number for TCP. The range is from 0 to 65, 535.
Advanced Settings	
Inactivity Timeout	Enable this option to specify the amount of time the protocol can be inactive before it times out.
Timeout Duration	Enter a timeout value for this protocol. The value range is 4 to 86400 seconds.

Table 319: Fields on Create Protocol Page Settings *(Continued)*

Field	Description
ALG	Select an ALG (Application Layer Gateway) service option if applicable.
Source Ports and Port Ranges	Enter the source port or port range for the protocol.

Table 320 on page 894 includes the settings and guidelines for the various protocol types.

Table 320: Create Protocol Type Settings

Field	Description
ICMP	
ICMP Type	Enter a value from 0 through 225 for the ICMP message type. For example, enter 1 for host unreachable. You can find these values in RFC 792.
ICMP Code	Enter a value from 0 through 225 for the ICMP code. For example, enter 0 for echo reply. You can find these values in RFC 792.
SUN-RPC	
RPC Program Number	Enter a value or value range for the RPC (remote procedure call) service. For example, enter 100,017 for remote execution. You can find these values in RFC 5531.
Protocol Type	Select TCP or UDP for the protocol type.
MS-RPC	

Table 320: Create Protocol Type Settings (Continued)

Field	Description
UUID	Enter the corresponding UUID value for the MS-RPC service. For predefined values, refer to MS-RPC UUID Mappings.
Protocol Type	Select TCP or UDP for the protocol type.
ICMPv6	
ICMP Type	Enter a value from 0 through 225 for the ICMPv6 message type. You can find these values in RFC 4443.
ICMP Code	Enter a value from 0 through 225 for the ICMPv6 code. You can find these values in RFC 4443.
SCTP, RSVP, PIM, OSPF, IPIP, IGMP, GRE, ESP, EGP, AH, and Other	
Protocol Number	Enter a protocol number for the protocol type. This number identifies the service in the next higher level in the protocol stack to which data is passed.

RELATED DOCUMENTATION

[About the Services Page](#) | 881

[Create Services and Service Groups](#) | 883

[Edit, Clone, and Delete Services and Service Groups](#) | 890

[Edit and Delete Protocols](#) | 896

Edit and Delete Protocols

IN THIS SECTION

- [Edit Protocols | 896](#)
- [Delete Protocols | 896](#)

You can edit and delete protocols through the **Services** page.

Edit Protocols

To modify the parameters configured for a protocol:

1. Select **Shared Services > Objects > Services**.

The **Services** page appears.

2. Select the service to which the protocol you want to edit is associated, and click on the edit icon (pencil symbol) on the right top corner of the table.

The **Edit Service** page appears, listing the protocols associated with the service in **Protocols** table.

3. Select the protocol that you want to edit, and then click on the edit icon (pencil symbol) on the right top corner of the **Protocols** table.

The **Edit Protocol** page appears, showing the same fields as those seen when you create a new protocol.

4. Modify the parameters of the protocol according to the guidelines provided in "[Create Protocols](#)" on [page 892](#) .

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

If you click **OK**, the modified protocol appears in the **Protocols** table.

Delete Protocols

To delete a protocol:

1. Select **Shared Services > Objects > Services**.

The **Services** page appears.

2. Select the service to which the protocol you want to delete is associated, and click on the edit icon (pencil symbol) on the right top corner of the table.

The **Edit Service** page appears, listing the protocols associated with the service in **Protocols** table.

3. Select the protocol you want to delete and then click the delete icon (trash can).

An alert message appears, verifying that you want to delete the protocol.

4. Click **Yes** to delete the protocol. If you do not want to delete, click **Cancel** instead.
If you click **Yes**, the selected protocol is deleted.

SEE ALSO

[About the Services Page | 881](#)

[Create Services and Service Groups | 883](#)

[Edit, Clone, and Delete Services and Service Groups | 890](#)

[Create Protocols | 892](#)

Objects-Applications

IN THIS CHAPTER

- [About the Application Signatures Page | 898](#)
- [Add Application Signatures | 901](#)
- [Edit, Clone, and Delete Application Signatures | 908](#)
- [Add Custom Application Signature Groups | 910](#)
- [Edit, Clone, and Delete Application Signature Groups | 911](#)

About the Application Signatures Page

IN THIS SECTION

- [Tasks You Can Perform | 898](#)
- [Field Descriptions | 899](#)

To access this page, select **Shared Services > Objects > Applications**.

Use the **Application Signatures** page to view application signatures that are already downloaded and to create, modify, clone, and delete application signatures and signature groups. The **Application Signatures** page displays the name, object type, category and subcategory, risk associated with, and characteristics of the signature. You can create custom application and application group with a set of similar signatures for consistent reuse when defining policies.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add an application signature. See "[Add Application Signatures](#)" on page 901 .

- Modify, clone, or delete an application signature. See ["Edit, Clone, and Delete Application Signatures" on page 908](#) .
- Add an application signature group. See ["Add Custom Application Signature Groups" on page 910](#) .
- Modify, clone, or delete an application signature group. See ["Edit, Clone, and Delete Application Signature Groups" on page 911](#) .

NOTE: You cannot modify the name of an application signature group.

- View the configured parameters of an application signature or application signature group. Click the details icon that appears when you hover over the name of an image or click **More > Details**.
- Show or hide columns in the **Application Signatures**. Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Search for a specific application signature or application signature group. Click the Search icon in the top right corner of the page to search for an application signature or application signature group.
- Filter the application signature information based on select criteria. You can add filters, save the filters, and set any of the filters as default. To add a filter:
 1. Click on the filter icon on the top-right corner of the page and select **Add Filter** to open the Add Criteria page.
 2. Set the filter conditions and click **Add**.

The filter is saved and the filter is applied on the data on the page. Filter can be saved and can mark any one filter as default.

To remove the filter, click on the filter icon and select **Hide Filter**.

Field Descriptions

[Table 321 on page 900](#) provides guidelines on using the fields on the **Application Signatures** page.

Table 321: Fields on the Application Signatures Page

Field	Description
Name	Enter a unique name for the application signature or application signature group. The name must begin with an alphanumeric character and can contain alphanumeric characters and some special characters (colons, hyphens, forward slashes, periods, and underscores); 63-character maximum.
Type	Signature application or group —either application signature or application signature group.
Category	Category of the application signature. For example, the value of Category can be Messaging, Web, Infrastructure, Remote-Access, Multimedia, and so on
Sub Category	Subcategory of the application signature. For example, the value of Subcategory can be Wiki, File-Sharing, Multimedia, Social-Networking, News, and so on.
Risk	Level of risk associated with the application signature. For example, the value of Risk can be Low, Moderate, Unsafe, High, and Critical.
Characteristics	One or more characteristics of the application signature.
Predefined/Custom	Indicates whether an application signature or signature groups is predefined or custom.
Cacheable	If an application is created with the Cacheable option, the column displays True, otherwise displays --.
Created Version	Version of the application signature.
Order	Order of the application signature.

RELATED DOCUMENTATION

[Add Application Signatures | 901](#)

[Edit, Clone, and Delete Application Signatures | 908](#)

[Add Custom Application Signature Groups | 910](#)

[Edit, Clone, and Delete Application Signature Groups | 911](#)

Add Application Signatures

You can add custom application signatures for applications that are not included in Juniper Networks predefined application database. When you add custom application signatures, make sure that your application signatures are unique, by providing a unique and relevant name.

To create a custom application signature:

1. Select **Shared Services > Objects > Applications**.
2. Click **Create > Signature**.
The Create Application Signature page appears.
3. Complete the configuration according to the guidelines provided in [Table 322 on page 901](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

A new application signature with your configurations is created.

[Table 322 on page 901](#) provides guidelines on using the fields on the **Create Application Signature** page.

Table 322: Fields on the Create Application Signature Page

Field	Description
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.
Description	Enter a description for the application signature; maximum length is 255 characters.
Signature Order and Priority	

Table 322: Fields on the Create Application Signature Page (*Continued*)

Field	Description
Order	<p>Enter the order for the custom application signature in the range between 1 and 50000. A lower order value has higher priority. This option is used when multiple custom application signatures of the same type match the same traffic. However, you cannot use this option to prioritize among different type of applications such as TCP stream-based applications against TCP port-based applications or IP address-based applications against port-based applications.</p> <p>NOTE: Application order must be unique for each application.</p>
Priority	Specify the application signature priority (high or low) over other application signatures.
Signature Classification	
Category	Enter the category of the application signature. For example, Messaging, Web, Infrastructure, Remote-Access, Multimedia, and so on.
Sub Category	Enter the subcategory of the application signature. For example, Wiki, File-Sharing, Multimedia, Social-Networking, News, and so on.
Risk	Select the level of risk associated with the application signature. For example, Low, Moderate, High, Critical, and Unsafe.
Characteristics	Enter one or more characteristics of the application signature. For example, supports file transfer, loss of productivity, and so on.

Table 322: Fields on the Create Application Signature Page (*Continued*)

Field	Description
Application Criteria	<p>Enable one or more application matching criteria:</p> <ul style="list-style-type: none"> • ICMP Mapping • IP Protocol Mapping • Address Mapping • L7 Signature
ICMP Mapping	<p>Click the toggle button to specify the Internet Control Message Protocol (ICMP) value for an application while configuring custom application signatures for application identification.</p> <p>The ICMP mapping technique maps standard ICMP message types and optional codes to a unique application name. The ICMP code and type provide additional specification, for packet matching in an application definition.</p>
ICMP Type	<p>Enter an ICMP value for the application. The ICMP mapping technique maps standard ICMP message types and optional codes to a unique application name.</p> <p>Range is 0-254.</p>
ICMP Code	<p>Enter an ICMP code for the application. The field provides further information (such as RFCs) about the ICMP type field.</p> <p>Range is 0-254.</p>
IP Protocol Mapping	<p>Click the toggle button to specify the IP protocol value for an application. This parameter is used to identify an application based on its IP protocol value and is intended only for IP traffic. To ensure adequate security, use IP protocol mapping only in your private network for trusted servers.</p>

Table 322: Fields on the Create Application Signature Page (*Continued*)

Field	Description
IP Protocol	<p>Enter an IP Protocol number for the application. Standard IP protocol numbers map an application to IP traffic. To ensure adequate security, use IP protocol mapping only in your private network for trusted servers.</p> <p>Range is 0-254.</p> <p>You can find a complete list of industry standard protocol numbers at the IANA website.</p> <p>NOTE: You cannot use IP protocol numbers 1(ICMP), 6(TCP) and 17(UDP) for custom application signature creation. Instead, we recommend you to use L7 signature policies for these protocols.</p>
Address Mapping	<p>Click the toggle button to specify address mapping information. Layer 3 and Layer 4 address mapping defines an application by matching the destination IP address or port range (optional) of the traffic. Use the address mapping option to configure custom applications signatures when the configuration of your private network predicts application traffic to or from trusted servers.</p> <p>Address mapping provides efficiency and accuracy while handling traffic from a known application. For more information, see Table 323 on page 905 .</p> <p>NOTE:</p> <ul style="list-style-type: none"> • You must specify either IP address or TCP/UDP port range for address mapping. • If both IP address and TCP/UDP ports are configured, both should match destination tuples (IP address and port range) of the packet.

Table 322: Fields on the Create Application Signature Page (*Continued*)

Field	Description
L7 Signature	Click the toggle button to specify the Layer 7-based custom application signatures that are required to identify the multiple applications running on the same L7 protocols. For example, applications such as Facebook and Yahoo Messenger can both run over HTTP, but there is a need to identify them as two different applications running on the same Layer 7 protocol. For more information, see Table 324 on page 906 .
Cacheable	Click the toggle button to enable caching of application identification results on the device. Enable this option to True only when L7 signatures are configured alone in a custom signature. This option is not supported for address-based, IP protocol-based, and ICMP-based custom application signatures.

Table 323: Fields on the Add IP Address Mapping Page

Field	Description
Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed; maximum length is 63 characters.
IP Address	Enter the destination IPv4 or IPv6 address of the application.
CIDR	Enter a CIDR value for the IP Address that you assign to the application. Range for IPv4 address is 1-32. Range for IPv6 address is 1-128.

Table 323: Fields on the Add IP Address Mapping Page (*Continued*)

Field	Description
TCP Port range	(Optional) Enter space-separated list of ports or port ranges to match a TCP destination port for Layer 3 and Layer 4 address-based custom applications. The range is 0-65535. Example: 80-82 443.
UDP port range	(Optional) Enter space-separated list of ports or port ranges ranges to match an UDP destination port for Layer 3 and Layer 4 address-based custom applications. The range is 0-65535. Example: 160-162 260.

Table 324: Fields on the Add Signature Page

Field	Description
Over Protocol	Displays the signature to match the application protocol. Example: HTTP.
Signature Name	Enter a unique name that is a string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 63 characters.
Port Range	Enter the port range for the application. Range is 0-65535 Example: 80-82 443
Add Members	Click the plus icon (+) to add the member details.

Table 324: Fields on the Add Signature Page (*Continued*)

Field	Description
Member No.	Displays the member name for a custom application signature. Custom signatures can contain multiple members that define attributes for an application. (The supported member name range is m01–m15.)
Context	<p>Select the service-specific context.</p> <ul style="list-style-type: none"> • For L7 Signatures over HTTP, select any of the following context: <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 • For L7 Signatures over SSL, select the service-specific context as ssl-server-name. • For L7 Signatures over TCP, select the service-specific context as stream. • For L7 Signatures over UDP, select the service-specific context as stream. <p>For possible combinations of context and direction for L7 application creation, refer context (Application Identification).</p>

Table 324: Fields on the Add Signature Page *(Continued)*

Field	Description
Direction	<p>Select the direction of the packet flow to which the signature must be matched.</p> <ul style="list-style-type: none"> • any—The direction of packet flow can either be from client-side to server-side or from server-side to client-side. • client-to-server—The direction of packet flow is from client-side to server-side. • server-to-client—The direction of packet flow is from server-side to client-side.
Pattern	<p>Enter the deterministic finite automaton (DFA) pattern matched on the context. The DFA pattern specifies the pattern to be matched for the signature. Maximum length is 128.</p>

RELATED DOCUMENTATION

[About the Application Signatures Page | 898](#)

[Edit, Clone, and Delete Application Signatures | 908](#)

[Add Custom Application Signature Groups | 910](#)

[Edit, Clone, and Delete Application Signature Groups | 911](#)

Edit, Clone, and Delete Application Signatures

IN THIS SECTION

- [Edit Custom Application Signatures | 909](#)
- [Clone Application Signatures | 909](#)
- [Delete Application Signatures | 910](#)

You can edit, clone, and delete custom application signatures from the **Application Signatures** page.

NOTE:

- You cannot edit or delete predefined application signatures, however, you can clone predefined application signatures.
- You cannot delete application signatures that are in use.

Edit Custom Application Signatures

To modify the parameters configured for a user-created (custom) application signature:

1. Select **Shared Services > Objects > Applications**.

The **Application Signatures** page appears.

2. Select the custom application signature that you want to edit, and then click on the edit icon (pencil), on the top right corner of the table.

The **Edit Application Signature** page appears, showing the same options as those displayed when you create a new application signature.

3. Modify the parameters according to the guidelines provided in ["Add Application Signatures" on page 901](#).
4. Click **Save** to save the changes. If you want to discard your changes, click **Cancel** instead.

The modified application signature appears on the **Application Signatures** page.

Clone Application Signatures

You can clone a application signature when you want to reuse an existing application signature, but with a few minor changes. This way, you can save time recreating the application signature from scratch.

To clone an application signature:

1. Select **Shared Services > Objects > Applications**.

The **Application Signatures** page appears.

2. Select the application signature that you want to clone, and then select **More > Clone**, or right-click the application signature and then select **Clone**.

The **Clone** page appears with editable fields.

3. Modify the fields as required. Refer to the guidelines provided in ["Add Application Signatures" on page 901](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

The cloned application signature is displayed on the **Application Signatures** page.

Delete Application Signatures

To delete a cloned user-created (custom) application signature:

1. Select **Shared Services > Objects > Applications**.

The **Application Signatures** page appears.

2. Select the application signature you want to delete and then click the delete icon.

An alert message appears to verify that you want to delete the selected application signature.

3. Click **Yes** to delete the selected application signature. If you do not want to delete, click **Cancel** instead.

The deleted application signature is removed from the Application Signatures page.

SEE ALSO

[About the Application Signatures Page | 898](#)

[Add Application Signatures | 901](#)

[Add Custom Application Signature Groups | 910](#)

[Edit, Clone, and Delete Application Signature Groups | 911](#)

Add Custom Application Signature Groups

Application identification supports custom application signatures to detect applications as they pass through the device. When you add custom signature groups, make sure that your signature groups are unique, by providing a unique and relevant name.

To add an application signature group:

1. Select **Shared Services > Objects > Applications**.
2. Click **Create > Signature Group**.
3. Complete the configuration according to the guidelines provided in [Table 325 on page 911](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

A new application signature group with your configurations is created.

[Table 325 on page 911](#) provides guidelines on using the fields on the **Create Application Signature Group** page.

Table 325: Fields on the Create Application Signature Group Page

Field	Description
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.
Description	Enter a description for the application signature; maximum length is 255 characters.
Group Members	Click the add icon (+) to add signatures to your application group. On the Add Application Signatures page, select the check boxes next to the signatures you want to add to the group.

RELATED DOCUMENTATION

[About the Application Signatures Page | 898](#)

[Add Application Signatures | 901](#)

[Edit, Clone, and Delete Application Signatures | 908](#)

[Edit, Clone, and Delete Application Signature Groups | 911](#)

Edit, Clone, and Delete Application Signature Groups

IN THIS SECTION

- [Edit Custom Application Signature Groups | 912](#)
- [Clone Application Signature Groups | 912](#)
- [Delete Custom Application Signature Groups | 912](#)

You can edit, clone, and delete application signature groups from the **Application Signatures** page.

Edit Custom Application Signature Groups

To modify the parameters configured for an application signature group:

1. Select **Shared Services > Objects > Applications**.
The **Application Signatures** page appears.
2. Select the application signature group that you want to edit, and click on the edit icon (pencil symbol), on the top right corner of the table.
The **Edit** page appears, showing the same options as those displayed when you create a new application signature group.
3. Modify the parameters according to the guidelines provided in "[Add Custom Application Signature Groups](#)" on page 910 .
4. Click **Save** to save the changes. If you want to discard your changes, click **Cancel** instead.
The modified application signature group appears in the **Application Signatures** page.

Clone Application Signature Groups

You can clone an application signature group when you want to reuse an existing application signature group, but with a few minor changes. This way, you can save time recreating the application signature group from the start.

To clone an application signature group:

1. Select **Shared Services > Objects > Applications**.
The **Application Signatures** page appears.
2. Right-click the application signature group that you want to clone and then select **Clone**, or select **More > Clone**.
The **Clone** page appears with editable fields.
3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.
The cloned application signature group is displayed on the **Application Signatures** page.

Delete Custom Application Signature Groups

To delete a custom application signature group:

1. Select **Shared Services > Objects > Applications**.
The **Application Signatures** page appears.
2. Select the custom application signature group you want to delete and then click the delete icon (trash can).
An alert message appears, verifying that you want to delete the selected item.

3. Click **Yes** to delete the selected application signature group. If you do not want to delete, click **Cancel** instead.

SEE ALSO

[About the Application Signatures Page | 898](#)

[Add Application Signatures | 901](#)

[Edit, Clone, and Delete Application Signatures | 908](#)

[Add Custom Application Signature Groups | 910](#)

Objects-Schedules

IN THIS CHAPTER

- [Schedules Overview | 914](#)
- [About the Schedules Page | 915](#)
- [Create a Schedule | 916](#)
- [Edit, Clone, and Delete a Schedule | 918](#)

Schedules Overview

A schedule allows a policy to be active for a specified duration. If you want a policy to be active during a scheduled time, you must first create a schedule for that policy or link the policy to an existing schedule. When a schedule timeout expires, the associated policy is deactivated and all sessions associated with the policy are also timed out.

If a policy contains a reference to a schedule, that schedule determines when the policy is active. When a policy is active, it can be used as a possible match for traffic. A schedule lets you restrict access to, or remove a restriction from a resource, for a period of time.

A schedule uses the following guidelines:

- A schedule can have multiple policies associated with it; however, a policy cannot be associated with multiple schedules.
- A policy remains active as long as the schedule it refers to is also active.

A schedule can be active during a single time slot, as specified by a start date and time, and a stop date and time.

- A schedule can be active forever (recurrent), but only as specified by the daily schedule. The schedule on a specific day (time slot) takes priority over the daily schedule.
- A scheduler can be active during a time slot, as specified by the weekday schedule.
- A scheduler be active within two different time slots (daily or for a specified duration).

About the Schedules Page

IN THIS SECTION

- [Tasks You Can Perform | 915](#)
- [Field Descriptions | 915](#)

To access this page, click **Shared Services > Objects > Schedules**.

The Schedules page enables you to create, modify, clone, and delete schedules for the security policy. A schedule allows you to restrict access to a resource, or remove a restriction to a resource, for a specified period of time.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a firewall policy schedule group. See ["Create a Schedule" on page 916](#)
- Modify, clone or delete a firewall policy schedule. See ["Edit, Clone, and Delete a Schedule" on page 918](#)
- View the configured parameters of a security policy schedule. Click the details icon that appears when you hover over the name of an image or click **More > Detail**.
- Show or hide columns about the security policy schedule. Click the Show Hide columns icon in the top right corner of the page and select columns that you want to view on the page.
- Search for a specific security policy schedule. Click the Search icon in the top right corner of the page to search for a firewall policy schedule.

You can enter partial text or full text of the keyword in the text box and press Enter.

The search results are displayed on the same page.

Field Descriptions

Provides guidelines on using the fields on the Schedules page.

Field	Description
Name	Name of the schedule; maximum length is 63 characters.
Description	Description for the schedule; maximum length is 900 characters.
Start Date	The date and time from when the schedule comes into effect.
End Date	The date and time from when the schedule ends.
Second Start Date	The second date and time from when the schedule comes into effect.
Second End Date	The second date and time from when the schedule ends.
Schedules	Displays if the schedule is active daily or for any specific days including specific times of the day.

Create a Schedule

Use the **Create Schedules** page to create schedules. A schedule allows you to restrict access to a resource, or remove a restriction to a resource, for a specified period of time.

To configure a schedule:

1. Select **Shared Services > Objects > Schedules**.
The **Schedules** page appears.
2. Click the add icon (+).
The **Create Schedules** page appears.
3. Complete the configuration of the schedule according to the guidelines provided in [Table 326 on page 917](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

A new schedule is created. You can use this schedule to activate security policies for the times and dates configured in your schedules.

[Table 326 on page 917](#) provides guidelines on using the fields to create a schedule.

Table 326: Fields on the Create Schedules Page

Field	Description
General Information	
Name	Required. Enter a unique name for the service. It must begin with an alphanumeric character and cannot exceed 63 characters. Dashes and underscores are allowed.
Description	Enter a description for your service. You should make this description as useful as possible for all administrators.
Dates	
Date Range	<p>Select Ongoing if you want your schedules to always be active.</p> <p>Select Custom to configure two sets of start and end dates for a single schedule. For the first set, enter dates in the Start Date and End Date fields. You must enter the days in MM/DD/YYYY format.</p> <p>For the second set of the schedule, enter the start date in the Second Start Date field and enter the end date in the Second End Date field.</p>
Times	
Time Range	Create a schedule to be active daily or for any specific times of the day.

Table 326: Fields on the Create Schedules Page (*Continued*)

Field	Description
Daily Options	<p>Select Daily to make the schedule applicable daily.</p> <p>Select Custom to enter specific days and times. Click on a specific day to specify time options for an entire day, to exclude a specific day, or to enter time ranges for the selected day. You must enter the time in HH:MM:SS format.</p> <p>For example, if you click on Monday, you get a dialog box that allows you to specify whether you want the schedule to be active all day Monday, exclude Monday from the schedule, or have the schedule be active at specific times.</p>

Edit, Clone, and Delete a Schedule

IN THIS SECTION

- [Edit a Schedule | 918](#)
- [Clone a Schedule | 919](#)
- [Delete a Schedule | 919](#)

You can edit, clone, and delete schedules from the **Schedules** page.

Edit a Schedule

To modify the parameters configured for a schedule:

1. Select **Shared Services > Objects > Schedules**.
The **Schedules** page appears.
2. Select the schedule that you want to edit, and then click on the edit icon (pencil) on the right top corner of the table.
The **Edit Schedules** page appears, showing the same options as when creating a new schedule.
3. Modify the parameters according to the guidelines provided in "[Create a Schedule](#)" on page 916 .

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

The modified schedule appears on the **Schedules** page.

Clone a Schedule

To clone a schedule:

1. Select **Shared Services > Objects > Schedules**.

The **Schedules** page appears.

2. Right-click on the schedule that you want to clone and then click **Clone**, or select **More > Clone**.

The **Clone Schedule** page appears displaying the same fields that are available when you create a schedule.

3. Modify the schedule fields as needed.

4. Click **OK** to save your changes.

The modified schedule appears on the **Schedules** page.

Delete a Schedule

To delete a schedule:

1. Select **Shared Services > Objects > Schedules**.

The **Schedules** page appears.

2. Select the schedule you want to delete and then click the delete icon.

An alert message appears, asking you to confirm the delete operation.

3. Click **Yes** to delete the selection.

A confirmation message appears, indicating the status of the delete operation.

Objects-URL Patterns

IN THIS CHAPTER

- [About the URL Patterns Page | 920](#)
- [Create a URL Pattern | 921](#)
- [Import URL Patterns from a CSV File | 923](#)
- [Edit, Clone, and Delete a URL Pattern | 924](#)

About the URL Patterns Page

IN THIS SECTION

- [Tasks You Can Perform | 920](#)
- [Field Descriptions | 921](#)

A URL pattern is a set of ordered characters that is modeled after an actual URL. Use this page to view, create, edit, clone, and delete URL patterns. The patterns are used to validate inbound and outbound URL requests and allow or block them.

To access this page, select **Shared Services > Objects > URL Patterns**.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a URL pattern—See ["Create a URL Pattern" on page 921](#) .
- Edit, clone, or delete a URL pattern—See ["Edit, Clone, and Delete a URL Pattern" on page 924](#) .

- View the details of a URL pattern—Select the URL pattern for which you want to view the details and from the More or right-click menu, select **Detailed View**. The URL Pattern Details page appears displaying the fields shown in [Table 327 on page 921](#).
- Import URL patterns from a CSV file—"[Import URL Patterns from a CSV File](#)" on page 923
- Clear the selected URL patterns—Click **Clear All Selections** to clear any URL patterns that you might have selected.
- Search for URL patterns using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.

Field Descriptions

[Table 327 on page 921](#) describes the fields on the URL Patterns page.

Table 327: URL Patterns Page Fields

Field	Description
Name	Name of the URL pattern.
URLs	List of URLs in the URL pattern.
Description	Description of the URL pattern.

Create a URL Pattern

Use this page to create URL patterns. You can also assign URL patterns to a URL category.

1. Select **Shared Services > Objects > URL Patterns**.
The URL Patterns page appears.
2. Click the add icon (+) to create a URL pattern.
The Create URL Patterns page is displayed.
3. Complete the configuration according to the guidelines provided in [Table 328 on page 922](#).

NOTE: Fields marked with * are mandatory.

4. Click **OK**.

A new URL pattern is created and you are returned to the URL Patterns page.

Table 328: Create URL Patterns Settings

Settings	Guidelines
Name	<p>Enter a unique name for the URL pattern.</p> <p>The name must begin with a letter or an underscore (_) and can contain alphanumeric characters and some special characters (_ -). The maximum length is 29 characters.</p>
Description	<p>Enter a description for the URL pattern. The maximum length is 255 characters.</p>
URL Category	<p>Select the URL category to which you want to assign the URL pattern. Alternatively, click Create New URL Category to create a URL category, enter the URL category name in the text box, and click Save to assign the URL pattern to the new category.</p>

Table 328: Create URL Patterns Settings (Continued)

Settings	Guidelines
Add URLs	<p>Enter one or more URLs (separated by commas) in the text box, and click Add. The URLs are displayed in the URL List table.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • The following wildcard characters are supported: <ul style="list-style-type: none"> • asterisk (*) • period (.) • square brackets ([]) • question mark (?) • Precede all wildcard characters with http://. • The asterisk (*) can only be used at the beginning of a URL and must be followed by a period (.) • The question mark (?) can only be used at the end of a URL. • The following are examples of wildcard syntaxes that are supported: http://*.example.net, http://www.example.ne?, and http://www.example.n??. • The following are examples of wildcard syntaxes that are not supported: *.example.???, http://*example.net, http://?, and www.example.ne?.

Import URL Patterns from a CSV File

You can import multiple allowed or blocked URL patterns from a CSV file. This enables you to manage large-scale networks more efficiently, accurately, and consistently.

1. Go to **Shared Services > Objects > URL Patterns**.
The **URL Patterns** page is displayed.
2. Click **More > Import URL Patterns from CSV File**.

The **Import URL Patterns from CSV** page is displayed.

3. Click **Download CSV template**.

The CSV template file is downloaded to your computer.

4. In the downloaded file, enter the name, description, and URL patterns that must be allowed or blocked.

5. In the **Import URL Patterns from CSV** page, click **Browse**, select the file, and then click **Upload**.

- Before the data is imported from the CSV file, the data is analyzed. If the name or URL pattern is missing in a row, an error message is displayed. A column is added in the CSV file with information about the error against the corresponding entry.

- If no errors are detected in the CSV file, the file is uploaded to import the data.

6. If an error is detected, download the updated CSV file, fix the errors, and then upload the file again.

- If the imported data contain the same name as existing URL patterns or IP addresses but different values, the **Conflict Resolution** table is displayed with the list of conflicts.

- If no conflicts are detected, the data is imported.

7. If the **Conflict Resolution** table is displayed, select one of the following options to resolve the conflict between the imported and existing data:

- **Keep existing:** If you select to keep the existing data, a tick mark identifies the values of the data that will not be imported.
- **Create new object**
- **Overwrite with imported value:** If you select to overwrite the existing data, a tick mark identifies the data that will overwrite the values of the existing data.

You can also select different resolution options from the Action column drop-down list of each row of conflicting data

8. Click **OK**.

All data conflicts is resolved based on the actions you select, and the data is imported from the CSV file and displayed on the **URL Patterns** page.

Edit, Clone, and Delete a URL Pattern

IN THIS SECTION

- [Edit a URL Pattern | 925](#)
- [Clone a URL Pattern | 925](#)

You can edit, clone, and delete URL patterns from the URL Patterns page. This topic has the following sections:

Edit a URL Pattern

To modify the parameters configured for a URL pattern:

1. Select **Shared Services > Objects > URL Patterns**.

The URL Patterns page appears, displaying the existing URL patterns.

2. Select the URL pattern that you want to edit and click the pencil icon.

The Edit URL Patterns page appears, displaying the same fields that are presented when you create a URL pattern.

3. Modify the URL pattern fields as needed.

4. Click **OK**.

You are taken to the URL Patterns page. A confirmation message appears, indicating the status of the edit operation.

Clone a URL Pattern

Cloning enables you to easily create a new URL pattern based on an existing one.

To clone a URL pattern:

1. Select **Shared Services > Objects > URL Patterns**.

The URL Patterns page appears, displaying the existing URL patterns.

2. Select the URL pattern that you want to clone and then select **More > Clone**.

The Clone URL Patterns page appears, displaying the same fields that are presented when you create a URL pattern.

3. Modify the URL pattern fields as needed.

4. Click **OK** to save your changes.

You are taken to the URL Patterns page. A confirmation message appears, indicating the status of the clone operation.

Delete a URL Pattern

Before deleting a URL pattern, ensure that the URL pattern is not referenced in any content security profiles that are, in turn, used in firewall policy rules or in URL categories referenced in the content security settings. If you try to delete such a URL pattern, an error message is displayed.

To delete one or more URL patterns:

1. Select **Shared Services > Objects > URL Patterns**.

The URL Patterns page appears, displaying the existing URL patterns.

2. Select one or more URL patterns that you want to delete and click the delete icon.

An alert message appears, asking you to confirm the delete operation.

3. Click **Yes** to delete the selected URL patterns.

A confirmation message appears, indicating the status of the delete operation.

Objects-URL Categories

IN THIS CHAPTER

- [About the URL Categories Page | 927](#)
- [Create a URL Category | 928](#)
- [Edit, Clone, and Delete a URL Category | 930](#)

About the URL Categories Page

IN THIS SECTION

- [Tasks You Can Perform | 927](#)
- [Field Descriptions | 928](#)

To access this page, select **Shared Services > Objects > URL Categories**.

Use this page to view, create, edit, clone, and delete URL categories. A URL category is a list of URL patterns grouped under a single title.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a URL category—See ["Create a URL Category" on page 928](#).
- Edit, clone, or delete a URL category—See ["Edit, Clone, and Delete a URL Category" on page 930](#).
- View the details of a URL category—Select the URL category for which you want to view the details and from the More or right-click menu, select **Detailed View**. The URL Category Details page appears, displaying the details of the selected URL category; see [Table 329 on page 928](#) for an explanation of the fields.

- Clear the selected URL categories—Click **Clear All Selections** to clear any URL categories that you might have selected.
- Search for URL categories by using keywords—Click the search icon, enter the search term in the text box, and press Enter. The search results are displayed on the same page.

Field Descriptions

[Table 329 on page 928](#) describes the fields on the URL Categories page.

Table 329: URL Categories Page Fields

Field	Description
Name	Name of the URL category.
URL Pattern	List of URL patterns in the URL category.
Category	List the URL category type: Juniper Enhanced or Juniper NextGen. NOTE: To view the Juniper NextGen URL categories, the Junos OS version must be 23.3R1 or later.
Predefined/Custom	Indicates the type of URL category: <ul style="list-style-type: none"> • Predefined—URL categories that are loaded by default. • Custom—URL categories that are created by the user.
Description	Description of the URL category.

Create a URL Category

Use this page to create URL categories. A URL category is a list of URL patterns grouped under a single title.

To create a URL category:

1. Select **Shared Services > Objects > URL Categories**.

The URL Categories page appears.

2. Click the add icon (+) to create a URL category.

The Create URL Categories page is displayed.

3. Complete the configuration according to the guidelines provided in [Table 330 on page 929](#).

NOTE: Fields marked with * are mandatory.

4. Click **OK**.

A new URL category is created and you are returned to the URL Categories page.

Table 330: Create URL Categories Settings

Settings	Guidelines
Name	<p>Enter a unique name for the URL category.</p> <p>The name must begin with a letter or an underscore (_) and can contain alphanumeric characters and some special characters (_ -). The maximum length is 59 characters.</p>
Description	<p>Enter a description for the URL pattern. The maximum length is 255 characters.</p>
URL Patterns	<p>Select one or more URL patterns in the Available column and click the forward arrow to confirm your selection. The selected URL patterns are displayed in the Selected column.</p> <p>Alternatively, click Create a New Pattern to create a URL pattern and assign it to the URL category. The Create URL Patterns page appears. For more information, see "Create a URL Pattern" on page 921.</p> <p>NOTE: You must select at least one URL pattern.</p>

Edit, Clone, and Delete a URL Category

IN THIS SECTION

- [Edit a URL Category | 930](#)
- [Clone a URL Category | 930](#)
- [Delete a URL Category | 931](#)

You can edit, clone, and delete URL categories from the URL Categories page. This topic has the following sections:

Edit a URL Category

To modify the parameters configured for a URL category:

1. Select **Shared Services > Objects > URL Categories**.

The URL Categories page appears, displaying the existing URL categories.

2. Select the custom URL category that you want to edit and click the pencil icon.

The Edit URL Categories page appears, displaying the same fields that are presented when you create a URL category.

3. Modify the URL category fields as needed.
4. Click **OK** to save your changes.

You are taken to the URL Categories page. A confirmation message appears, indicating the status of the edit operation.

Clone a URL Category

Cloning enables you to easily create a new URL category based on an existing one.

To clone a URL category:

1. Select **Shared Services > Objects > URL Categories**.

The URL Categories page appears, displaying the existing URL categories.

2. Select the URL category that you want to clone and then select **More > Clone**.

The Clone URL Categories page appears, displaying the same fields that are presented when you create a URL category.

3. Modify the URL category fields as needed.
4. Click **OK** to save your changes.

You are taken to the URL Categories page. A confirmation message appears, indicating the status of the clone operation.

Delete a URL Category

Before deleting a URL category, ensure that the URL category is not referenced in any content security profiles that are, in turn, used in firewall policy rules or in the content security settings. If you try to delete such a URL category, an error message is displayed.

To delete one or more URL categories:

1. Select **Shared Services > Objects > URL Categories**.

The URL Categories page appears, displaying the existing URL categories.

2. Select one or more custom URL categories that you want to delete and click the delete icon.

An alert message appears, asking you to confirm the delete operation.

3. Click **Yes** to delete the selected URL categories.

A confirmation message appears, indicating the status of the delete operation.

Advanced Threat Prevention

IN THIS CHAPTER

- [Enroll an SRX Series Firewall using Juniper ATP Cloud Web Portal | 932](#)
- [Remove an SRX Series Firewall From Juniper Advanced Threat Prevention Cloud | 936](#)
- [Search for SRX Series Firewalls Within Juniper Advanced Threat Prevention Cloud | 937](#)
- [Device Information | 937](#)
- [File Inspection Profiles Overview | 939](#)
- [Create File Inspection Profiles | 941](#)
- [Email Management Overview | 942](#)
- [Configure SMTP Email Management | 944](#)
- [Configure IMAP Email Management | 948](#)
- [Adaptive Threat Profiling Overview | 951](#)
- [Create an Adaptive Threat Profiling Feed | 954](#)
- [Allowlist and Blocklist Overview | 956](#)
- [Create Allowlists and Blocklists | 957](#)
- [SecIntel Feeds Overview | 963](#)
- [Juniper Threat Feeds Overview | 969](#)
- [Global Configuration for Infected Hosts | 969](#)
- [Enable Logging | 972](#)
- [Configure Threat Intelligence Sharing | 973](#)
- [Configure Trusted Proxy Servers | 975](#)
- [Configure DAG Filter | 976](#)
- [Configure Webhook | 977](#)

Enroll an SRX Series Firewall using Juniper ATP Cloud Web Portal

Only devices enrolled with Juniper ATP Cloud can send files for malware inspection.

Before enrolling a device, check whether the device is already enrolled. To do this, use the **Enrolled Devices** page or the Device Lookup option in the Juniper Security Director Cloud UI. If the device is already enrolled, disenroll it first before enrolling it again.

NOTE: If a device is already enrolled in a realm and you enroll it in a new realm, none of the device data or configuration information is propagated to the new realm. This includes history, infected hosts feeds, logging, API tokens, and administrator accounts.

As of Junos Release 19.3R1, there is another way to enroll the SRX Series Firewall without having to interact with the ATP Cloud Web Portal. You run the “enroll” command from the SRX and it performs all the necessary enrollment steps. See [Enroll an SRX Series Firewall Using the CLI](#).

Juniper ATP Cloud uses a Junos OS operation (op) script to help you configure your SRX Series Firewall to connect to the Juniper Advanced Threat Prevention Cloud service. This script performs the following tasks:

- Downloads and installs certificate authority (CAs) licenses onto your SRX Series Firewall.
- Creates local certificates and enrolls them with the cloud server.
- Performs basic Juniper ATP Cloud configuration on the SRX Series Firewall.
- Establishes a secure connection to the cloud server.

NOTE:

- Juniper ATP Cloud requires that both your Routing Engine (control plane) and Packet Forwarding Engine (data plane) is connected to the Internet.
- The data plane connection should not go through the management interface, for example, fxp0. You do not need to open any ports on the SRX Series Firewall to communicate with the cloud server. However, if you have a device in the middle, such as a firewall, then that device must have ports 8080 and 443 open.
- The SRX Series Firewall uses the default inet.0 routing table and an interface part of inet.0 as source-interface for control-plane connection from SRX Series Firewall to ATP Cloud. If the only Internet-facing interface on SRX Series Firewall is part of a routing instance, then we recommend that you add a static route pointing to the routing instance. Else, the control connection will fail to establish.

- Juniper ATP Cloud requires that your SRX Series Firewall host name contain only alphanumeric ASCII characters (a-z, A-Z, 0-9), the underscore symbol (_) and the dash symbol (-).



WARNING: If you are configuring explicit web proxy support for SRX Series services/ Juniper ATP Cloud connections, you must enroll SRX Series Firewalls to Juniper ATP Cloud using a slightly different process, see [Explicit Web Proxy for Juniper ATP Cloud](#).

To enroll a device in Juniper ATP Cloud using the Web Portal, do the following:

1. From the Juniper Security Director Cloud UI, select **Shared Services > Advanced Threat Prevention > ATP Devices**. Click the **Enroll** button on the **Enrolled Devices** page.
2. Copy the command to your clipboard and click **OK**.
3. Paste the command into the Junos OS CLI of the SRX Series Firewall you want to enroll with Juniper ATP Cloud and press Enter. (Note that this command must be run in operational mode.)

NOTE: If the script fails, disenroll the device (see "[Remove an SRX Series Firewall From Juniper Advanced Threat Prevention Cloud](#)" on page 936) and then re-enroll it.

NOTE: (Optional) Use the `show services advanced-anti-malware status` CLI command to verify that a connection is made to the cloud server from the SRX Series Firewall.

Once configured, the SRX Series Firewall communicates to the cloud through multiple persistent connections established over a secure channel (TLS 1.2) and the SRX Series Firewall is authenticated using SSL client certificates.

In the Juniper Security Director Cloud UI **Enrolled Devices** page, basic connection information for all enrolled devices is provided, including serial number, model number, tier level (free or not) enrollment status in Juniper ATP Cloud, last telemetry activity, and last activity seen. Click the serial number for more details. In addition to **Enroll**, the following buttons are available:

Table 331: Button Actions

Actions	Definition
Enroll	Use the Enroll button to obtain a enroll command to run on eligible SRX Series Firewalls. This command enrolls them in Juniper ATP Cloud and is valid for 7 days. Once enrolled, SRX Series Firewall appears in the Devices and Connections list.
Disenroll	Use the Disenroll button to obtain a disenroll command to run on SRX Series Firewalls currently enrolled in Juniper ATP Cloud. This command removes those devices from Juniper ATP Cloud enrollment and is valid for 7 days.

NOTE: Running the Enroll or Disenroll command will commit any uncommitted configuration changes on the SRX Series Firewall.

NOTE: Generating a new Enroll or Disenroll command invalidates any previously generated commands.

Device Lookup	Use the Device Lookup button to search for the device serial number(s) in the licensing database to determine the tier (premium, feed only, free) of the device. For this search, the device does not have to be currently enrolled in Juniper ATP Cloud.
Delete	Removing an SRX Series Firewall is different than disenrolling it. Use the Delete option only when the associated SRX Series Firewall is not responding (for example, hardware failure). Clicking the delete button disassociates the SRX Series Firewall from the cloud without running the Junos OS operation (op) script on the device (see Enrolling and Disenrolling Devices). You can later enroll it using the Enroll option when the device is again available.

For HA configurations, you only need to enroll the cluster primary. The cloud will detect that this is a cluster and will automatically enroll both the primary and backup as a pair. Both devices, however, must be licensed accordingly. For example, if you want premium features, both devices must be entitled with the premium license.

NOTE: Juniper ATP Cloud supports both active-active and active-passive cluster configurations. The passive (non-active) node does not establish a connection to the cloud until it becomes the active node.

NOTE: The License Expiration column contains the status of your current license, including expiration information. There is a 60 day grace period after the license expires before the SRX Series Firewall is disenrolled from Juniper ATP Cloud.

RELATED DOCUMENTATION

[Remove an SRX Series Firewall From Juniper Advanced Threat Prevention Cloud | 936](#)

[Search for SRX Series Firewalls Within Juniper Advanced Threat Prevention Cloud | 937](#)

Remove an SRX Series Firewall From Juniper Advanced Threat Prevention Cloud

If you no longer want an SRX Series Firewall to send files to the cloud for inspection, use the disenroll option to disassociate it from Juniper Advanced Threat Prevention Cloud. The disenroll process generates an ops script to be run on SRX Series Firewalls and resets any properties set by the enroll process.

To disenroll an SRX Series Firewall:

1. Select **Shared Services** > Advanced Threat Prevention > ATP Devices. Select the check box associated with the device you want to disassociate and click **Disenroll**.
2. Copy the highlighted command to your clipboard and click **OK**.
3. Paste this command into the Junos OS CLI of the device you want to disenroll and press **Enter**.

You can re-enroll this device at a later time using the **Enroll** option.

RELATED DOCUMENTATION

[Search for SRX Series Firewalls Within Juniper Advanced Threat Prevention Cloud | 937](#)

[Enroll an SRX Series Firewall using Juniper ATP Cloud Web Portal | 932](#)

Search for SRX Series Firewalls Within Juniper Advanced Threat Prevention Cloud

You can search for any SRX Series Firewall enrolled within your security realm of Juniper Advanced Threat Prevention Cloud using the **Device Lookup** option. You can view the type of license the device is using: basic, premium, or free.

NOTE: You can only search for device using serial numbers.

To search for devices enrolled with Juniper Advanced Threat Prevention Cloud:

1. Select **Shared Services > Advanced Threat Prevention > ATP Devices**.
2. Click **Device Lookup**.
The Device Lookup window appears.
3. Enter the serial number of the device you want to search for and click **Next**. You can enter multiple serial numbers, separating each entry with a new line.

The search results window appears.

NOTE: The Juniper Security Director Cloud UI does not check for valid serial numbers. If you enter an invalid serial number, you will see an empty result. If you enter multiple serial numbers and one is an invalid number, you will see an empty result.

RELATED DOCUMENTATION

[Enroll an SRX Series Firewall using Juniper ATP Cloud Web Portal | 932](#)

[Remove an SRX Series Firewall From Juniper Advanced Threat Prevention Cloud | 936](#)

Device Information

Use this page to view the following information on the selected SRX Series Firewall.

Table 332: Device Information Fields

Field	Definition
Device Information	
Serial Number	SRX Series Firewall serial number
Host	Host name of the device.
Model Number	SRX Series Firewall model number
OS Version	SRX Series Firewall JunOS version
Submission Status	Allowed or Paused. This indicates whether the device can submit files to Juniper ATP Cloud or if it has reached its daily limit. (At this time, the limit is 10,000 files per day for premium accounts.)
Configuration Information	<p>The Device and Cloud fields indicate the version numbers of each list, both on the device and in the cloud. You can compare the following to see if they are in sync:</p> <ul style="list-style-type: none"> • Global Config • Profile Config • Global Allowlist • Global Blocklist • Global DNS Allowlist • Global DNS Blocklist • Customer Allowlist • Customer Blocklist • Customer ETA Allowlist • PHASE Signature

Table 332: Device Information Fields (Continued)

Field	Definition
Connection Type	
Telemetry	The time when the last telemetry submission was received.
Submission	The time when the last file submission was received.
C&C Event	The time when the last Command and Control event was received.

RELATED DOCUMENTATION

[Enroll an SRX Series Firewall using Juniper ATP Cloud Web Portal | 932](#)

[Remove an SRX Series Firewall From Juniper Advanced Threat Prevention Cloud | 936](#)

[Search for SRX Series Firewalls Within Juniper Advanced Threat Prevention Cloud | 937](#)

File Inspection Profiles Overview

Access this page from **Shared Services > ATP > File Inspection Profiles**.

Juniper ATP Cloud profiles let you define which files to send to the cloud for inspection. You can group types of files to be scanned together (such as .tar, .exe, and .java) under a common name and create multiple profiles based on the content you want scanned. Then enter the profile names on eligible Juniper Secure Edge devices to apply them.

Benefits of File Inspection Profiles

- Allows you to create file categories to send to the cloud for scanning rather than having to list every single type of file you want scanned.
- Allows you to configure multiple scanning categories based on file type, adding and removing file types when necessary, increasing or decreasing granularity.

Table 333: File Category Contents

Category	Description
Archive	Archive files
Configuration	Configuration files
Document	All document types except PDFs
Executable	Executable binaries
ELF	Executable and Linkable Format (ELF) is a standard file format for executable files, object code, and libraries.
Java	Java applications, archives, and libraries
Library	Dynamic and static libraries and kernel modules
Mobile	Mobile formats
OS package	OS-specific update applications
PDF	PDF, e-mail, and MBOX files
Rich Application	Installable Internet Applications such as Adobe Flash, JavaFX, Microsoft Silverlight
Script	Scripting files

You can also define the maximum file size requirement per each category to send to the cloud. If a file falls outside of the maximum file size limit the file is automatically downloaded to the client system.

NOTE: If you are using the free or basic model of Juniper ATP Cloud, you are limited to only the executable file category.

NOTE: The ELF file types support both static analysis and dynamic analysis.

Juniper ATP Cloud periodically polls for new and updated content and automatically downloads it to Juniper Secure Edge. There is no need to manually push your profile.

Create File Inspection Profiles

Use this page to group files under a common, unique name for scanning. By grouping files together into a profile, you can choose file categories to send to the cloud rather than having to list every single type of file you want to scan, such as .tar, .exe, and .java. Once you create your profile name, select one or more check boxes to add file types to be scanned to the profile. Optionally, enter a value limit for the file type in megabytes.

- Review the "[File Inspection Profiles Overview](#)" on page 939 topic.
- Note that a default profile, `default_profile`, is created as part of the initial configuration step. You can modify this default profile, but you cannot delete it.
- If you are using the free or basic model of Juniper Advanced Threat Prevention Cloud, you are limited to only the executable file category.

To create a device profile:

1. Select **Shared Services > ATP > File Inspection Profiles**.
2. Click the plus sign (+). Complete the configuration according to the guidelines provided in the table below.
3. Click **OK**.

Table 334: Profile Settings

Setting	Guideline
Name	Enter a unique name for the profile. This must be a unique string that begins with an alphanumeric character and can include letters, numbers, and underscores; no spaces are allowed; 63-character maximum.

Table 334: Profile Settings (Continued)

Setting	Guideline
File Categories	<p>You can create several profiles and each profile can contain different options for how each file type is scanned. From the pulldown list for each file type, you can select:</p> <p>Do not scan – This file type is not processed for scanning and is always allowed through.</p> <p>Hash lookup only – Instead of the file, a sha256 hash of the file is sent for matching against known malware. This may provide a faster result because only a matching of the hash is done and all the file data does not have to be sent. The danger here is that the hash will only match known malware. If the file is a new type of malware that is not known, it will not be recognized as malicious using this method.</p> <p>Scan files up to max size – The full content of the file is sent to the cloud for scanning as long as it falls within the set file size limits. If a file exceeds this limit, it is not sent to the cloud for inspection and is transferred to the client. If you do not set the maximum file size, a default of 32 MB is used.</p>

NOTE: You can create up to 32 profiles.

NOTE: Juniper ATP Cloud periodically polls for new and updated content and automatically downloads it to Juniper Secure Edge. There is no need to manually push your profile.

Email Management Overview

With Email Management, Juniper Secure Edge transparently submit potentially malicious email attachments to the cloud for inspection. Once an attachment is evaluated, Juniper ATP Cloud assigns the file a threat score between 0-10 with 10 being the most malicious.

NOTE: If an email contains no attachments, it is allowed to pass without any analysis.

Benefits of Email Management

- Allows attachments to be checked against allowlists and blocklists.
- Prevents users from opening potential malware received as an email attachment.

Configure Juniper ATP Cloud to take one of the following actions when an email attachment is determined to be malicious:

For SMTP

- **Quarantine Malicious Messages**—If you select to quarantine emails with attachments found to be malicious, those emails are stored in the cloud in an encrypted form and a replacement email is sent to the intended recipient. That replacement email informs the recipient of the quarantined message and provides a link to the quarantine portal where the email can be previewed. The recipient can then choose to release the email by clicking a Release button (or request that the administrator release it) or Delete the email.
- **Deliver malicious messages with warning headers added**—When you select this option, headers are added to emails that most mail servers recognize and filter into Spam or Junk folders.
- **Permit**—You can select to permit the email and the recipient receives it intact. Optionally, you can choose to send a notification to the end user about the permitted message.

For IMAP

- **Block Malicious Messages**—Block emails with attachments that are found to be malicious.
- **Permit**—You can select to permit the email and the recipient receives it intact.

Quarantine Release

If the recipient selects to release a quarantined email, it is allowed to pass through Juniper Secure Edge with a header message that prevents it from being quarantined again, but the attachments are placed in a password-protected ZIP file. The password required to open the ZIP file is also included as a separate attachment. The administrator is notified when the recipient takes an action on the email (either to release or delete it).

If you configure Juniper ATP Cloud to have the recipient send a request to the administrator to release the email, the recipient previews the email in the quarantine portal and can select to Delete the email or Request to Release. The recipient receives a message when the administrator takes action (either to release or delete the email.)

Blocklist and Allowlist

Emails are checked against administrator-configured blocklists and allowlists using information such as Envelope From (MAIL FROM), Envelope To (RCPT TO), Body Sender, Body Receiver. If an email matches

the allowlist, that email is allowed through without any scanning. If an email matches the blocklist, it is considered to be malicious and is handled the same way as an email with a malicious attachment.

Configure SMTP Email Management

Access this page from **Shared Services > ATP > Email Management > SMTP**.

NOTE: SMTP is supported only for Security Director Cloud use cases.

- Read the "[Email Management Overview](#)" on [page 942](#) topic.
- Decide how malicious emails are handled: quarantined, delivered with headers, or permitted.

1. Select **Configure > Email Management > SMTP**.

The SMTP page appears.

2. Based on your selections, configuration options will vary. See the tables below.

Table 335: Configure Quarantine Malicious Messages

Setting	Guideline
Action to take	Quarantine malicious messages—When you select to quarantine malicious email messages, in place of the original email, intended recipients receive a custom email you configure with information on the quarantining. Both the original email and the attachment are stored in the cloud in an encrypted format.

Table 335: Configure Quarantine Malicious Messages *(Continued)*

Setting	Guideline
Release option	<ul style="list-style-type: none"> Recipients can release email—This option provides recipients with a link to the quarantine portal where they can preview the email. From the portal, recipients can select to Release the email or Delete it. Either action causes a message to be sent to the administrator. <p>NOTE: If a quarantined email has multiple recipients, any individual recipient can release the email from the portal and all recipients will receive it. Similarly, if one recipient deletes the email from the portal, it is deleted for all recipients.</p> <ul style="list-style-type: none"> Recipients can request administrator to release email—This option also provides recipients with a link to the quarantine portal where they can preview the email. From the portal, recipients can select to Request to Release the email or Delete it. Either choice causes a message to be sent to the administrator. When the administrator takes action on the email, a message is sent to the recipient. <p>NOTE: When a quarantined email is released, it is allowed to pass through the Juniper Secure Edge with a header message that prevents it from being quarantined again, but the attachment is placed inside a password-protected zip file with a text file containing the password that the recipient must use to open the file.</p>
<i>Email Notifications for End Users</i>	
Learn More Link URL	If you have a corporate web site with further information for users, enter that URL here. If you leave this field blank, this option will not appear to the end user.
Subject	When an email is quarantined, the recipient receives a custom message informing them of their quarantined email. For this custom message, enter a subject indicating a suspicious email sent to them has been quarantined, such as "Malware Detected."
Custom Message	Enter information to help email recipients understand what they should do next.

Table 335: Configure Quarantine Malicious Messages *(Continued)*

Setting	Guideline
Custom Link Text	Enter custom text for the quarantine portal link where recipients can preview quarantined emails and take action on them.
Buttons	<ul style="list-style-type: none"> • Click Preview to view the custom message that will be sent to a recipient when an email is quarantined. Then click Save. • Click Reset to clear all fields without saving. • Click Save if you are satisfied with the configuration.

Table 336: Configure Deliver with Warning Headers

Setting	Guideline
Action to take	Deliver with warning headers—When you select to deliver a suspicious email with warning headers, you can add headers to emails that most mail servers will recognize and filter into spam or junk folders.
SMTP Headers	<ul style="list-style-type: none"> • X-Distribution (Bulk, Spam)—Use this header for messages that are sent to a large distribution list and are most likely spam. You can also select “Do not add this header.” • X-Spam-Flag—This is a common header added to incoming emails that are possibly spam and should be redirected into spam or junk folders. You can also select “Do not add this header.” • Subject Prefix—You can prepend headers with information for the recipient, such as “Possible Spam.”
Buttons	<ul style="list-style-type: none"> • Click Reset to clear all fields without saving. • Click OK if you are satisfied with the configuration.

Table 337: Permit

Setting	Guideline
Action to take	Permit—You can select to permit the message. Optionally, you can choose to send a notification to the end user about the permitted message containing an unknown malware.
Notify end users	Enable this option to configure the protected domain and send custom notifications to the protected domain users and administrators. If this field is disabled, then the notification is sent only to the administrators.
Protected Domains	(Optional) Enter comma-separated list of domain names. By default, malware notification is sent to configured administrators and end users of all domains. When you specify the protected domains, the malware notification will only be sent to the users in the specified domains.
Subject	When an email is permitted and Notify end user is enabled, the recipient receives a custom message informing them of their permitted email containing an unknown malware. For this custom message, enter a subject indicating a suspicious email sent to them has been permitted, such as "Malware Notification."
Custom Message	(Optional). Enter information to help email recipients understand what they should do next. Default predefined message will be sent if left blank.
<i>Email Notifications for Administrators</i>	
Subject	When an email is permitted, the administrator receives a custom message informing them of the permitted email. For this custom message, enter a subject indicating a suspicious email sent to them has been permitted, such as "Malware Notification."
Custom Message	Enter information to help email recipients understand what they should do next.

Table 337: Permit (Continued)

Setting	Guideline
Buttons	<ul style="list-style-type: none"> • Click Preview to view the custom message that will be sent to a recipient when an email is permitted. Then click Save. • Click Reset to clear all fields without saving. • Click Save if you are satisfied with the configuration.

Administrators Who Receive Notifications

To send notifications to administrators when emails are quarantined or released from quarantine:

1. Click the + sign to add an administrator.
2. Enter the administrator's email address.
3. Select the **Quarantine Notification** check box to receive those notifications.
4. Select the **Release Notifications** check box to receive those notifications.
5. Click **OK**.

Configure IMAP Email Management

To access this page, navigate to **Shared Services > ATP > Email Management > IMAP**.

NOTE: IMAP is supported only for Security Director Cloud use cases.

- Read the "[Email Management Overview](#)" on page 942 topic.
 - Decide how malicious emails are handled. For IMAP, the available options are to block or permit email. Unlike SMTP, there is no quarantine option for IMAP and no method for previewing a blocked email.
1. Select **Shared Services > ATP > Email Management > IMAP**.
The IMAP page appears.
 2. Based on your selections, configuration options will vary. See the tables below.

Table 338: Configure Block Malicious Messages

Setting	Guideline
Action to take	<ul style="list-style-type: none"> • Permit download of attachments—Allow email attachments, either from all IMAP servers or specific IMAP servers, through to their destination. NOTE: In Permit mode, black and allowlists are not checked. Emails from blocklisted addresses are not sent to the cloud for scanning. They are allowed through to the client. • Block download of attachments—Block email attachments, either from all IMAP servers or specific IMAP servers, from reaching their destination. NOTE: In Block mode, black and allowlists are checked. Emails from blocklisted addresses are blocked. Emails from allowlisted addresses are allowed through to the client. Recipients can send a request to an administrator to release the email. Enter the email address to which recipients should send a release request. NOTE: If a blocked email has multiple recipients, any individual recipient can request to release the email and all recipients will receive it. <p>When you select to block email attachments, in place of the original email, intended recipients receive a custom email you configure with information on the block action. Both the original email and the attachment are stored in the cloud in an encrypted format.</p>
IMAP Server	<ul style="list-style-type: none"> • All IMAP Servers—The permitting or blocking of email attachments applies to all IMAP servers. • Specific IMAP Server—The permitting or blocking of email attachments applies only to IMAP servers with hostnames that you add to a list. A configuration section to add the IMAP server name appears when you select this option. <p>When you add IMAP servers to the list, it is sent to Juniper Secure Edge to filter emails sent to Juniper ATP Cloud for scanning. For emails that are sent for scanning, if the returned score is above the set policy threshold on Juniper Secure Edge, then the email is blocked.</p>

Table 338: Configure Block Malicious Messages *(Continued)*

Setting	Guideline
IMAP Servers	<p>Select the Specific IMAP Server option above and click the + sign to add IMAP server hostnames to the list.</p> <p>NOTE: You must use the IMAP server hostname and not the IP address.</p>
<i>Email Notifications for End Users</i>	
Learn More Link URL	If you have a corporate web site with further information for users, enter that URL here. If you leave this field blank, this option will not appear to the end user.
Subject	When an email is blocked, the recipient receives a custom message informing them of their blocked email. For this custom message, enter a subject indicating a suspicious email sent to them has been blocked, such as "Malware Detected."
Custom Message	Enter information to help email recipients understand what they should do next.
Custom Link Text	Enter custom text for the quarantine portal link where recipients can preview blocked emails and take action on them.
Buttons	<ul style="list-style-type: none"> • Click Preview to view the custom message that will be sent to a recipient when an email is blocked. Then click Save. • Click Reset to clear all fields without saving. • Click Save if you are satisfied with the configuration.

Administrators Who Receive Notifications

To send notifications to administrators when emails are blocked or released from quarantine:

1. Click the **+** sign to add an administrator.
2. Enter the administrator's email address and click **OK**.

3. Once the administrator is created, you can uncheck or check which notification types the administrator will receive.
 - Block Notifications—When this check box is selected, a notification is sent when an email is blocked.
 - Unblock Notifications—When this check box is selected, a notification is sent when a user releases a blocked email.

Adaptive Threat Profiling Overview

IN THIS SECTION

- [Overview | 951](#)
- [Configure Adaptive Threat Profiling | 954](#)

Overview

Juniper ATP Cloud Adaptive Threat Profiling allows Juniper Secure Edge to generate, propagate, and consume threat feeds based on their own advanced detection and policy-match events.

This feature allows you to configure security or IDP policies that, when matched, inject the source IP address, destination IP address, source identity, or destination identity into a threat feed, which can be leveraged by other devices as a dynamic-address-group (DAG). While this feature is focused on tracking and mitigating threat actors within a network, you can also use it for non-threat related activities, such as device classification.

With adaptive threat profiling, the Juniper ATP Cloud service acts as a feed-aggregator and consolidates feeds from Juniper Secure Edge across your enterprise and shares the deduplicated results back to all Juniper Secure Edge devices in the realm at regular intervals. Juniper Secure Edge can then use these feeds to perform further actions against the traffic.

NOTE: This feature requires Secure Edge Advanced or higher license to function.

Benefits of adaptive threat profiling

- Enables new deployment architectures, whereby Juniper Secure Edge can be deployed as sensors throughout the network on Tap ports, identifying and sharing intelligence to in-line devices for real-time enforcement.
- Allows administrators near-infinite adaptability to changing threats and network conditions. Security policies can be staged with adaptive threat profiling feeds, which automatically populate with entries in the event of an intrusion or a malware outbreak.
- Provides the ability to perform endpoint classification. You can classify endpoints based on network behavior and/or deep packet inspection (DPI) results. For example, you can leverage AppID, Web-Filtering, or IDP to place hosts that communicate with Ubuntu's update servers into a dynamic-address-group that can be used to control Ubuntu-Server behavior on your network.

Access this page from **Configure > Adaptive Threat Profiling**.

Table 339: Adaptive Threat Profiling

Field	Guideline
Feed Name	Name of the adaptive threat profiling feed.
Items	Number of entries in the feed.
Feed Type	Content type of the feed. The following options are supported: <ul style="list-style-type: none"> • IP • USER_ID
Added to Infected Hosts	Displays whether the feed content (for example, source or destination IP address) is added to the Infected host feed. <ul style="list-style-type: none"> • True—The feed content is added to the Infected host feed. • False—The feed content is not added to the Infected host feed. <p>NOTE: Currently you can add only IP address feed type to the Infected host feed.</p>
Time to Live (days)	Defines how long an entry will "live" inside the feed. Once the TTL is reached, the entry is removed automatically.

NOTE:

- The feeds can only be used as dynamic-address groups (DAG) /IP filter.

You can perform the following tasks from this page:

- Add a new feed—See "[Create an Adaptive Threat Profiling Feed](#)" on page 954 .
- Modify a feed—Select a feed and click the edit icon (pencil). The Edit *<feed-name>* page appears, displaying the same fields that were presented when you create a feed. Modify the fields as needed. Click **OK** to save your changes.

NOTE: You cannot edit the feed name and feed type.

- Delete a feed—Select a feed and click the delete icon in the title bar. A pop-up requesting confirmation for the deletion appears. Click **Yes** to confirm that you want to delete the feed.
- Filter or Search for a feed—Click the filter icon. Enter partial text or full text of the keyword in the search bar and click the search button or press **Enter**. The search results are displayed. You can also filter by feed type and Time to Live (days).
- View detailed information about a feed—Click on a feed name to view the following information:
 - Feed Items—Lists all the IP addresses or User IDs that are associated with the feed. To exclude an IP address or User ID from the feed, select the IP address or User ID and click **Add to Excluded Items**.
 - Excluded Items—Lists all the IP addresses or User IDs that are excluded from the feed. To remove an IP address or User ID for the excluded items list, select the IP address or User ID and click the Delete icon.

To manually exclude an IP address or User ID from the feed:

1. Click the plus (+) icon in the Excluded Items tab.

The Add to Excluded List page appears.

2. Enter the IP address or User ID that you want to exclude from the feed.
3. Click **OK**.

The IP address or User ID is listed in the Excluded items page.

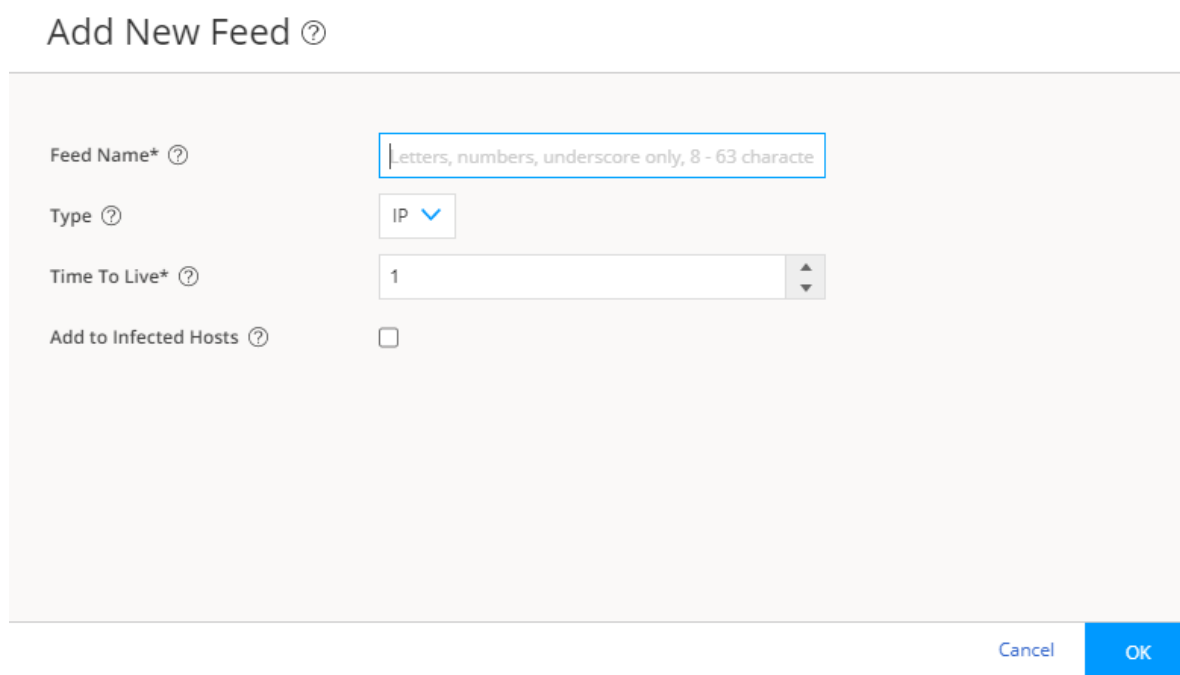
Configure Adaptive Threat Profiling

Juniper Secure Edge that has already been enrolled with Juniper ATP Cloud should include all the necessary configuration to begin leveraging adaptive threat profiling.

To configure adaptive threat profiling:

1. Create an adaptive threat profiling feed, select **Shared Services > ATP > Adaptive Threat Profiling > +**. The Adaptive Threat Profiling page appears as shown in [Figure 29 on page 954](#) . In this example, we will use the feed name **High_Risk_Users** with a time-to-live (TTL) of seven days.

Figure 29: Add New Feed



The screenshot shows a dialog box titled "Add New Feed" with a help icon. It contains four configuration fields:

- Feed Name*** with a help icon and a text input field containing the placeholder text "Letters, numbers, underscore only, 8 - 63 characte".
- Type** with a help icon and a dropdown menu currently set to "IP".
- Time To Live*** with a help icon and a numeric input field set to "1", with up and down arrow controls on the right.
- Add to Infected Hosts** with a help icon and an unchecked checkbox.

At the bottom right of the dialog are two buttons: "Cancel" and "OK".

2. Click **OK** to save changes. For more information, see "[Create an Adaptive Threat Profiling Feed](#)" on [page 954](#) .
3. Ensure that the feed has been downloaded by Juniper Secure Edge. This is done automatically at regular intervals but can take a few seconds.

Create an Adaptive Threat Profiling Feed

Use this page to add a new adaptive threat profiling feed.

Review the ["Adaptive Threat Profiling Overview" on page 951](#) topic.

To add a new adaptive threat profiling feed:

1. Select **Shared Services > ATP > Adaptive Threat Profiling**.

The Adaptive Threat Profiling page appears.

2. Click the plus sign (+).

The Add New Feed page appears as shown in [Figure 30 on page 955](#) .

Figure 30: Add New Feed Settings

The screenshot shows a dialog box titled "Add New Feed" with a help icon. It contains the following fields:

- Feed Name***: A text input field with a placeholder "Letters, numbers, underscore only, 8 - 63 characte".
- Type**: A dropdown menu with "IP" selected.
- Time To Live***: A numeric input field with "1" and up/down arrows.
- Add to Infected Hosts**: An unchecked checkbox.

At the bottom right, there are "Cancel" and "OK" buttons.

3. Complete the configuration according to the guidelines provided in the [Table 340 on page 955](#) .
4. Click **OK** to save the changes.

Table 340: Add New Feed Settings

Setting	Guideline
Feed Name	Enter a unique name for the threat feed. The feed name must begin with an alpha-numeric character and can include letters, numbers, and underscores; no spaces are allowed. The length is 8–63 characters.

Table 340: Add New Feed Settings (Continued)

Setting	Guideline
Type	<p>Select the content type of the feed. The following options are available:</p> <ul style="list-style-type: none"> • IP • User ID
Data Source	The data source (User Policy) of the feed is auto-selected. You cannot modify this field.
Time to Live	<p>Enter the number of days for the required feed entry to be active. After the feed entry crosses the time to live (TTL) value, the feed entry is automatically removed. The available range is 1–365 days.</p>
Add to Infected Hosts	<p>(Optional) Enable this setting to add the contents (for example, source or destination IP address) from this feed to the Infected host feed.</p> <p>NOTE: Currently, you can only add IP addresses to Infected host feed.</p>

NOTE:

- You can create a maximum of 64 feeds.
- You can add all 64 feeds to infected host feeds.

Allowlist and Blocklist Overview

An allowlist contains known trusted IP addresses, Hashes, Email addresses, and URLs. Content downloaded from locations on the allowlist does not have to be inspected for malware. A blocklist contains known untrusted IP addresses and URLs. Access to locations on the blocklist is blocked, and therefore no content can be downloaded from those sites.

Benefits of Allowlists and Blocklists

- Allowlist allows users to download files from sources that are known to be safe. Allowlist can be added to in order to decrease false positives.
- Blocklists prevent users from downloading files from sources that are known to be harmful or suspicious.

The Custom allowlists or custom blocklists allow you to add items manually. Both are configured on the Juniper ATP Cloud server. The priority order is as follows:

1. Custom allowlist
2. Custom blocklist

If a location is in multiple lists, the first match wins.

Allowlists support the following types:

- Anti-malware—IP address, URL, file hash, and e-mail sender
- SecIntel—C&C, ETI, and DNS

Blocklists support the following types:

- Anti-malware—IP address, URL, file hash, and e-mail sender
- SecIntel—C&C

NOTE:

- For IP and URL, The Web UI performs basic syntax checks to ensure your entries are valid.
- A hash is a unique signature for a file generated by an algorithm. You can add custom allowlist and blocklist hashes for filtering, but they must be listed in a text file with each entry on a single line. You can only have one running file containing up to 15,000 file hashes. For upload details see ["Create Allowlists and Blocklists" on page 957](#) . Note that Hash lists are slightly different than other list types in that they operate on the cloud side rather than the Juniper Secure Edge side. This means the web portal is able to display hits on hash items.

Juniper Secure Edge makes requests approximately every two hours for new and updated feed content. If there is nothing new, no new updates are downloaded.

Create Allowlists and Blocklists

Access these pages from **Shared Services > ATP > Allowlists or Blocklists**.

Use these pages to configure custom trusted and untrusted lists. You can also upload hash files.

Content downloaded from locations on the allowlist is trusted and does not have to be inspected for malware. Hosts cannot download content from locations on the blocklist, because those locations are untrusted.

- Read the "[Allowlist and Blocklist Overview](#)" on page 956 topic.
- Decide on the type of item you intend to define: URL, IP, Hash, E-mail sender, C&C, ETI, or DNS,
- Review current list entries to ensure the item you are adding does not already exist.
- If you are uploading hash files, the files must be in a text file with each hash on its own single line.

To create Juniper ATP Cloud allowlists or blocklists:

1. Select **Shared Services > ATP > Allowlists** or **Blocklists**.
2. For either Allowlist or Blocklist, select one of the following tabs: **Anti-Malware** or **SecIntel**. Enter the required information. See the tables below.

Allowlists support the following types:

- Anti-malware—IP address, URL, file hash, and e-mail sender
- SecIntel—C&C, ETI, and DNS

Blocklists support the following types:

- Anti-malware—IP address, URL, file hash, and e-mail sender
- SecIntel—C&C

3. Click **OK**.

Refer to the following tables for the data required by each tab.

IP

When you create a new IP list item, you must select the Type of list as **IP**. You must enter the required information. See the following table.

Table 341: IP Configuration

Setting	Guideline
IP	<p>Enter the IPv4 or IPv6 IP address. For example: 1.2.3.4 or 0:0:0:0:FFFF:0102:0304. CIDR notation and IP address ranges are also accepted.</p> <p>Any of the following IPv4 formats are valid: 1.2.3.4, 1.2.3.4/30, or 1.2.3.4-1.2.3.6.</p> <p>Any of the following IPv6 formats are valid: 1111::1, 1111::1-1111::9, or 1111:1::0/64.</p> <p>NOTE: Address ranges: No more than a block of /16 IPv4 addresses and /48 IPv6 addresses are accepted. For example, 10.0.0.0-10.0.255.255 is valid, but 10.0.0.0-10.1.0.0 is not.</p> <p>Bitmasks: The maximum amount of IP addresses covered by bitmask in a subnet record for IPv4 is 16 and for IPv6 is 48. For example, 10.0.0.0/15 and 1234::/47 are not valid.</p>

NOTE: To edit an existing allowlist or blocklist IP entry, select the check box next to the entry you want to edit, click the pencil icon and click **OK**.

URL

When you create a new URL list item, you must choose the Type of list: **URL**. Enter the required information. See the following table.

Table 342: URL Configuration

Setting	Guideline
URL	<p>Enter the URL using the following format: juniper.net. Wildcards and protocols are not valid entries. The system automatically adds a wildcard to the beginning and end of URLs. Therefore juniper.net also matches a.juniper.net, a.b.juniper.net, and a.juniper.net/abc. If you explicitly enter a.juniper.net, it matches b.a.juniper.net, but not c.juniper.net. You can enter a specific path. If you enter juniper.net/abc, it matches x.juniper.net/abc, but not x.juniper.net/123.</p>

NOTE: To edit an existing allowlist or blocklist URL entry, select the check box next to the entry you want to edit, click the pencil icon and click **OK**.

Hash File

When you upload a hash file, it must be in a text file with each hash on its own single line. You can only have one running hash file. To add to it or edit it, see the instructions in the following table.

Table 343: Hash File Upload and Edit Configuration

Field	Guideline
SHA-256 Hash Item	<p>To add to hash entries, you can upload several text files and they will automatically combine into one file. See all, merge, delete and replace options below.</p> <p>Download—Click this button to download the text file if you want to view or edit it.</p> <p>You can select any of the following options from the Select Hash File Items Upload Option drop-down list:</p> <ul style="list-style-type: none"> • Replace current list—Use this option when you want to change the existing list, but do not want to delete it entirely. Download the existing file, edit it, and then upload it again. • Merge with current list—Use this option when you upload a new text file and want it to combine with the existing text file. The hashes in both files combine to form one text file containing all hashes. • Delete from current list—Use this option when you want to delete only a portion of the current list. In this case, you would create a text file containing only the hashes you want to remove from the current list. Upload the file using this option and only the hashes in the uploaded file are deleted from the current active list. <p>Delete All or Delete Selected—Sometimes it's more efficient to delete the current list rather than downloading it and editing it. Click this button to delete the current selected list or all lists that have been added and accumulated here.</p>
Source	This says either Allowlist or Blocklist.

Table 343: Hash File Upload and Edit Configuration (Continued)

Field	Guideline
Date Added	The month, date, year, and time when the hash file was last uploaded or edited.

Email Sender

Add email addresses to be allowlist or blocklist if found in either the sender or recipient of an email communication. Add addresses one at a time using the + icon.

Table 344: Email Sender Configuration

Field	Guideline
Email address	Enter an email address in the format name@domain.com. Wildcards and partial matches are not supported, but if you want to include an entire domain, you could enter only the domain as follows: domain.com

If an email matches the blocklist, it is considered to be malicious and is handled the same way as an email with a malicious attachment. The email is blocked and a replacement email is sent. If an email matches the allowlist, that email is allowed through without any scanning. See ["SMTP Quarantine Overview" on page 149](#).

It is worth noting that attackers can easily fake the "From" email address of an email, making blocklists a less effective way to stop malicious emails.

C&C Server

When you allowlist a C&C server, the IP or hostname is sent to Juniper Secure Edge to be excluded from any security intelligence blocklists or C&C feeds (both Juniper's global threat feed and third party feeds). The server will also now be listed under the C&C allowlist management page.

You can enter C&C server data manually or upload a list of servers. That list must be a text file with each IP or Domain on its own single line. The text file must include all IPs or all Domains, each in their own file. You can upload multiple files, one at a time.

NOTE: You can also manage allowlist and blocklist entries using the Threat Intelligence API. When adding entries to the allowlist/blocklist data, these will be available in the Threat Intelligence API under the following feed names: "whitelist_domain" or "whitelist_ip", and

“blacklist_domain” or “blacklist_ip.” See the [Juniper ATP Cloud Threat Intelligence Open API Setup Guide](#) for details on using the API to manage any custom feeds.

Table 345: C&C Configuration

Field	Guideline
Type	Select IP to enter the IP address of a C&C server that you want to add to the allowlist. Select Domain to allowlist an entire domain on the C&C server list.
IP or Domain	For IP, enter an IPv4 or IPv6 address. An IP can be IP address, IP range or IP subnet. For domain, use the following syntax: juniper.net. Wildcards are not supported.
Description	Enter a description that indicates why an item has been added to the list.

You can also allowlist C&C servers directly from the C&C Monitoring page details view. See [Command and Control Server Details](#).

WARNING: Adding a C&C server to the allowlist automatically triggers a remediation process to update any affected hosts (in that realm) that have contacted the whitelisted C&C server. All C&C events related to this allowlisted server will be removed from the affected hosts’ events, and a host threat level recalculation will occur.

If the host score changes during this recalculation, a new host event appears describing why it was rescored. (For example, “Host threat level updated after C&C server 1.2.3.4 was cleared.”) Additionally, the server will no longer appear in the list of C&C servers because it has been cleared.

Encrypted Traffic Insights (ETI)

You can specify the IP address or domain names that you want to allowlist from encrypted traffic analysis. Use this tab to add, modify, or delete the allowlists for encrypted traffic analysis.

Table 346: Encrypted Traffic Configuration

Field	Guideline
Type	Select whether you want to specify the IP address or domain name for the allowlist.

Table 346: Encrypted Traffic Configuration (Continued)

Field	Guideline
IP or Domain	Enter the IP address or domain name for the allowlist.

Domain Name System (DNS)

You can specify the domains that you want to allowlist from DNS filtering. Use this tab to add, modify, or delete the allowlists for DNS filtering.

Table 347: Domains Configuration

Field	Guideline
URL	Enter the URL for domain that you want to allowlist.
Comments	Enter a description that indicates why the domain has been added to the list.

NOTE: Juniper ATP Cloud periodically polls for new and updated content and automatically downloads it to Juniper Secure Edge. There is no need to manually push your allowlist or blocklist files.

SecIntel Feeds Overview

SecIntel provides carefully curated and verified threat intelligence from Juniper Networks' Advanced Threat Prevention (ATP) Cloud, Juniper Threat Labs, Dynamic Address Group (DAG), and industry-leading threat feeds to Juniper Secure Edge, MX Series routers, SRX Series Firewalls, and NFX Series Network Services Platform to block Command and Control (C&C) communications at line rate. SecIntel delivers real-time threat intelligence by enabling automatic and responsive traffic filtering.

SecIntel integrates with EX Series and QFX Series switches and enables these switches to subscribe to SecIntel's infected host feed. This enables you to block compromised hosts at the switch port. You can now extend SecIntel throughout your entire network and increase the number of security enforcement points.

Benefits of SecIntel Feeds

You can view all the default feeds that are available with your current license.

Using this page, you can enable the following feeds for integration with Juniper ATP Cloud.

- Juniper threat feeds
- Third party threat feeds—IP threat feeds and URL threat feeds.
- Dynamic address group feeds—Juniper DAG feeds and Third-party DAG feeds.

NOTE: The total number of CC feeds are 32, out of which four feeds are reserved for cc_ip, cc_url, cc_ipv6, and cc_cert_sha1. So, you can enable up to 28 feeds to the CC category, which includes CC custom feeds and CC third-party feeds. This limit is applicable if you are injecting additional feeds using the available open API.

Information to know if you are enabling external feeds:

- If a hit is detected on an enabled external feed, this event appears under **Monitor>ATP** with a threat level of 10.
- On Juniper Secure Edge, you can configure policies with the permit or block action for each feed. Note that C&C and Infected Host feeds require an enabled Security Intelligence policy on Juniper Secure Edge in order to work.
- External feeds are updated once every 24 hours.



WARNING: Understand that these are open source feeds managed by third parties and determining the accuracy of the feed is left up to the Juniper ATP Cloud administrator. Juniper will not investigate false positives generated by these feeds.



WARNING: Juniper Secure Edge policies will block malicious IP addresses based on enabled third party feeds, but these events do not affect host threat scores. Only events from Juniper ATP Cloud feeds affect host threat scores.

To enable the available feeds, do the following:

1. Navigate to **Configure>SecIntel Feeds**.
2. For each feed, select the toggle button to enable the feed. Refer to the guidelines in [Table 348 on page 965](#).

NOTE: The Infected Host feed is enabled for all license tiers. All other Juniper SecIntel feeds are enabled only with Secure Edge Advanced or higher license.

Click the **Go to feed site** link to view feed information, including the contents of the feed.

Table 348: SecIntel Feeds

Field	Guidelines
Juniper Threat Feeds	
Command and Control	Displays whether the C&C feed is enabled or not.
Malicious Domains	Displays whether the DNS feed is enabled or not.
Infected Host Feed	Displays whether the infected host feed is enabled or not.
Third Party Threat Feeds	
<i>IP Threat Feeds</i>	
Block List	Click the toggle button to enable block list feeds as third party feeds.
Threatfox IP	Click the toggle button to enable Threatfox feeds as third party feeds.
Feodo Tracker	Click the toggle button to enable Feodo feeds as third party feeds.
DShield	Click the toggle button to enable DShield feeds as third party feeds.
Tor	Click the toggle button to enable tor feeds as third party feeds.
<i>URL Threat Feeds</i>	

Table 348: SecIntel Feeds (*Continued*)

Field	Guidelines
Threatfox URL	Click the toggle button to enable Threatfox feed as third party feeds. ThreatFox is a free platform from abuse.ch with the goal of sharing indicators of compromise (IOCs) associated with malware with the infosec community, AV vendors and threat intelligence providers. The IOC can be an IP address, domain name, or URL.
URLhaus URL Threat Feed	Click the toggle button to enable URLhaus feed as third party feeds. URLhaus is a threat intelligence feed that shares malicious URLs that are used for malware distribution.
Open Phish	Click the toggle button to enable OpenPhish feed as third party feeds. OpenPhish is a fully automated self-contained platform for phishing intelligence. It identifies phishing sites and performs intelligence analysis in real time without human intervention and without using any external resources, such as blocklists. For malware inspection, SecIntel will analyze traffic using URLs in this feed.
<i>Domain Threat Feeds</i>	
Threatfox Domains	Click the toggle button to enable Threatfox feed as third party feeds.
Dynamic Address Group Feeds	
<i>Juniper DAG Feeds</i>	
GeoIP Feed	Displays whether the GeoIP feed is enabled or not. GeoIP feed is an up-to-date mapping of IP addresses to geographical regions. This gives you the ability to filter traffic to and from specific geographies in the world.
<i>Third Party DAG Feeds</i>	

Table 348: SecIntel Feeds (Continued)

Field	Guidelines
office365	<p>Click the toggle button to enable office365 IP filter feed as a third party feed. The office365 IP filter feed is an up-to-date list of published IP addresses for Office 365 service endpoints which you can use in security policies. This feed works differently from others on this page and requires certain configuration parameters, including a pre-defined cloud feed name of "ipfilter_office365".</p> <p>Pre-defined cloud feed name— ipfilter_office365</p>
facebook	<p>Click the toggle button to enable feeds from Facebook.</p> <p>Pre-defined cloud feed name— ipfilter_facebook</p>
google	<p>Click the toggle button to enable feeds from Google.</p> <p>Pre-defined cloud feed name— ipfilter_google</p>
atlassian	<p>Click the toggle button to enable feeds from Atlassian.</p> <p>Pre-defined cloud feed name— ipfilter_atlassian</p>
zscaler	<p>Click the toggle button to enable feeds from Zscaler.</p> <p>Pre-defined cloud feed name— ipfilter_zscaler</p>
oracleoci	<p>Click the toggle button to enable feeds from Oracle oci.</p> <p>Pre-defined cloud feed name— ipfilter_oracleoci</p>
cloudflare	<p>Click the toggle button to enable feeds from Cloudflare.</p> <p>Pre-defined cloud feed name— ipfilter_cloudflare</p>
zoom	<p>Click the toggle button to enable feeds from Zoom.</p> <p>Pre-defined cloud feed name— ipfilter_zoom</p>

Table 348: SecIntel Feeds (Continued)

Field	Guidelines
microsoftazure	Click the toggle button to enable feeds from Microsoft Azure. Pre-defined cloud feed name— ipfilter_microsoftazure
amazonaws	Click the toggle button to enable feeds from Amazon AWS. Pre-defined cloud feed name— ipfilter_amazonaws
okta	Click the toggle button to enable feeds from Okta. Pre-defined cloud feed name— ipfilter_okta
paypal	Click the toggle button to enable feeds from Paypal. Pre-defined cloud feed name— ipfilter_paypal

NOTE:

- Since Ransomware Tracker and Malware Domain list are deprecated, ransomware tracker and malware domain list IP feeds are not supported on Juniper ATP Cloud. If you had enabled this feed earlier, you might stop receiving these feeds.
- The update interval for a third party Internet service feed is one day.

Using the office365 Feed

Enable the **Using the office365 Feed** check box in Juniper ATP Cloud to push Microsoft Office 365 services endpoint information (IP addresses) to Juniper Secure Edge. The office365 feed works differently from other feeds on this page and requires certain configuration parameters, including a pre-defined name of "ipfilter_office365".

After you enable the check box, you must create a dynamic address object on Juniper Secure Edge that refers to the ipfilter_office365 feed.

Juniper Threat Feeds Overview

SecIntel feeds include threat feeds provided by Juniper Networks, 3rd party threat feeds, or Dynamic Address Group (DAG) feeds. The SecIntel threat feeds provided by Juniper Networks is shown in [Table 349 on page 969](#).

NOTE: The Infected Host feed is enabled by default for all license tiers. All other Juniper Threat feeds are enabled by default with Secure Edge Advanced or higher license.

Table 349: Juniper Threat Feeds

Field	Guidelines
Command and Control Feed	C&C feeds are essentially a list of servers that are known command and control for botnets. The list also includes servers that are known sources for malware downloads.
Malicious Domains (DNS)	List of domains that are known to be connected to malicious activity.
Infected Host Feed	Infected hosts indicate local devices that are potentially compromised because they appear to be part of a C&C network or exhibit other symptoms.

Global Configuration for Infected Hosts

Threat Level Threshold

Set the global threat level to block infected hosts. When a host is found to be compromised, it is assigned a threat level. Based on the global threat level you set here, 1-10 with 10 being the highest threat, compromised hosts with the set threat level and above are added to the infected hosts lists and can subsequently be blocked by policies configured on Juniper Secure Edge. See "[Hosts Overview](#)" on [page 108](#) for more information.

You can configure Juniper ATP Cloud to send e-mails when certain threat levels are reached for infected hosts. For example, you can send e-mails to an IT department when thresholds of 5 are met and send e-mails to an escalation department when thresholds of 9 are met.

You can send e-mails to any account; you are not restricted to administrator e-mails defined in the Users window. The Web UI does not verify if an e-mail account is valid.

Configure Threat Level Threshold and Email Alerts

Benefits of the Global Infected Hosts Alerts

- Email alerts for infected hosts call immediate attention to administrators when a possible network security issue arises.
- Email alerts can be configured for only specific administrators and not all users of the web portal, targeting alerts more narrowly.

1. Select **Shared Services > ATP > Misc Configuration > Infected Hosts**.
2. (Premium licenses only) Set the default threat level threshold.
3. Click the plus sign to create e-mail alerts, or click the pencil icon to edit existing ones. Configure the fields described in the table below.
4. Click **OK**.

Table 350: Email alerts for infected hosts fields

Setting	Guideline
Threat Level	Select a threat level between 1 and 10. When this level is reached, an e-mail is sent to the address you provided.
E-mail	Enter an e-mail address.

Automatically Expire Blocked Hosts

When a host is marked as infected and added to the infected hosts feed, it is blocked from the network by policies configured on Juniper Secure Edge. There are options for unblocking individual hosts on the **Infected Hosts** page in the Portal. See "[Hosts Overview](#)" on page 108 for information. If you want to unblock multiple host IP addresses based on time period and threat level, you will use the **Automatically Expire Blocked Hosts** feature on the **Misc Configuration > Infected Hosts** page in the Web Portal.

From the Infected Hosts page, you can set infected hosts to expire after a configured time based on a minimum and maximum threat level. Once the time period is reached, blocked IP addresses are no longer marked as infected and therefore no longer blocked.

One example of when you might use this feature is if you are using DHCP addressing and reallocating addresses on a set schedule. In that case, you may want to set an expiration time for infected hosts (based on IP address lease times), after which addresses are no longer marked as infected.

Configure Automatic Expiration of Infected Hosts

1. Select **Shared Services > ATP > Misc Configuration > Infected Hosts**.
2. (System Administrators and Operators only) Enable **Automatically Expire Blocked Hosts** and select one of the following:

- **Unblock all hosts**
- **Unblock a range of hosts**—Enter a range of IPv4 or IPv6 addresses.

Any of the following IPv4 formats are valid: 10.2.3.4/30, or 10.2.3.4-1.2.3.6

Any of the following IPv6 formats are valid: 1111::1-1111::9, or 1111:1::0/64

NOTE: No more than a block of /16 IPv4 addresses and /48 IPv6 addresses are accepted. For example, 10.0.0.0-10.0.255.255 is valid, but 10.0.0.0-10.1.0.0 is not.

Bitmasks: The maximum amount of IP addresses covered by bitmask in a subnet record for IPv4 is 16 and for IPv6 is 48. For example, 10.0.0.0/15 and 1234::/47 are not valid. CIDR notation is also accepted.

3. For both **Unblock all hosts** or **Unblock a range of hosts**, you must also set expiration intervals and threat levels. Click the plus + sign to create a new entry and set the following in the **Unblocked Expiration Intervals** table.

Table 351: Unblock expiration interval fields

Setting	Guideline
Set the Minimum Threat Level	Click the table entry under Minimum Threat Level to access a pulldown menu. Select a minimum threat level (1-10). The level you select is included in the minimum setting.
Set the Maximum Threat Level	Click the table entry under Maximum Threat Level to access a pulldown menu. Select a maximum threat level (1-10). The level you select is included in the maximum setting.

Table 351: Unblock expiration interval fields (*Continued*)

Setting	Guideline
Set the Hours to Unblock	Click the table entry under Hours to Unblock . You can select Never, 6, 12, 18, or 24 hours. After the set amount of hours, the infected label expires and the hosts are no longer blocked.

For example, if you set the minimum at 6 and the maximum at 8 with hours to unblock as 24, the following would occur. All infected hosts with a threat level of 6 and above and 8 and below would expire after 24 hours.

NOTE: You can create multiple entries in this table, setting different expiration times for different threat levels.

Once unblock settings are entered in the table, you can use the table to change existing settings or to delete settings.

4. You must click **Save** or your settings are lost.

Enable Logging

You can select the event types that you want to log for the devices in your realm. The Juniper ATP Cloud logs yields information such as malware name, action taken, infected host, source of an attack, and destination of an attack. The devices in your realm use the event logs to generate system logs (syslogs).

To enable logging, do the following:

1. Select **Shared Services > ATP > Misc Configuration > Logging**.
2. Click the **Malware** toggle button to log malware in your realm.
3. Click the **Host Status** toggle button to log the host status in your realm.

NOTE: You can log the Malware or the Host Status event or both the event types.

Configure Threat Intelligence Sharing

Using the TAXII service, Juniper ATP Cloud can contribute to STIX reports by sharing the threat intelligence it gathers from file scanning. Juniper ATP Cloud also uses threat information from STIX reports as well as other sources for threat prevention. See ["HTTP File Download Details" on page 120](#) for more information on STIX reports.

- STIX (Structured Threat Information eXpression) is a language used for reporting and sharing threat information using TAXII (Trusted Automated eXchange of Indicator Information). TAXII is the protocol for communication over HTTPS of threat information between parties.
- STIX and TAXII are an open community-driven effort of specifications that assist with the automated exchange of threat information. This allows threat information to be represented in a standardized format for sharing.
- If you enable TAXII (it is disabled by default), you can limit who has access to your shared threat information by creating an application token.

To enable and configure threat intelligence sharing, do the following:

1. Select **Shared Services > ATP > Misc Configuration > Threat Intelligence Sharing**.
2. Move the knob to the right to **Enable TAXII**.
3. Move the slide bar to designate a file sharing threshold. Only files that meet or exceed the set threshold will be used in STIX reports. The default is threat level 6 or higher.

NOTE: You can limit who has access to your information by creating an application token.

TAXII URLs and Services	Description
Discovery URL	<p>Used by the TAXII client to discover available TAXII Services. The command to initiate a TAXII request is: <code>taxii-discovery</code></p> <p>NOTE: Refer to the TAXII documentation for information on additional commands. http://taxiiproject.github.io/documentation/</p> <p>Juniper ATP Cloud Discovery URLs are:</p> <p>US Region: https://taxii.sky.junipersecurity.net/services/discovery</p> <p>EU Region: https://taxii-eu.sky.junipersecurity.net/services/discovery</p> <p>APAC Region: https://taxii-apac.sky.junipersecurity.net/services/discovery</p> <p>Canada: https://taxii-canada.sky.junipersecurity.net/services/discovery</p>

At this time, there are two services supported by Juniper ATP Cloud on the TAXII server.

Collection Management	<p>Used by the TAXII client to request information about available data collections.</p> <p>Juniper ATP Cloud Collection Management URLs are:</p> <p>US Region: https://taxii.sky.junipersecurity.net/services/collection-management</p> <p>EU Region: https://taxii-eu.sky.junipersecurity.net/services/collection-management</p> <p>APAC Region: https://taxii-apac.sky.junipersecurity.net/services/collection-management</p> <p>Canada: https://taxii-canada.sky.junipersecurity.net/services/collection-management</p>
-----------------------	--

(Continued)

TAXII URLs and Services	Description
Poll URL	<p>Used by the TAXII client to poll for STIX files - looking for malware that has been identified on the network.</p> <p>Juniper ATP Cloud Polling URLs are:</p> <p>US Region: https://taxii.sky.junipersecurity.net/services/poll</p> <p>EU Region: https://taxii-eu.sky.junipersecurity.net/services/poll</p> <p>APAC Region: https://taxii-apac.sky.junipersecurity.net/services/poll</p> <p>Canada: https://taxii-canada.sky.junipersecurity.net/services/poll</p>

Configure Trusted Proxy Servers

Use this page to add trusted proxy server IP addresses to Juniper ATP Cloud. This feature is optional

Access this page from **Shared Services > ATP > Misc Configuration > Proxy Servers**.

When there is a proxy server between users on the network and a firewall, the firewall might see the proxy server IP address as the source of an HTTP or HTTPS request instead of the actual address of the user making the request.

With this in mind, X-Forwarded-For (XFF) is a standard header added to packets by a proxy server that includes the real IP address of the client making the request. Therefore, if you add trusted proxy servers IP addresses to the list in Juniper ATP Cloud, by matching this list with the IP addresses in the HTTP header (X-Forwarded-For field) for requests sent from Juniper Secure Edge, Juniper ATP Cloud can determine the originating IP address.

NOTE: X-Forwarded-For (XFF) only applies to HTTP or HTTPS traffic, and only if the proxy server supports the XFF header.

To add trusted proxy servers to the list, do the following:

1. Navigate to **Shared Services > ATP > Misc Configuration > Proxy Servers**.
2. Click the + sign.

3. Enter the IP address of the proxy server in the available field.
4. Click **OK**.

Configure DAG Filter

Access the DAG Filters page from the **Shared Services > Advanced Threat Prevention > SecIntel Feeds** menu.

Use a Dynamic Address Group (DAG) filter to add feeds for the AWS regions and services that you select. You can configure a maximum of 10 DAG filters for the AWS.

Benefits of DAG filter

You can filter and view the feeds from specific AWS regions and services that are relevant to you.

NOTE: If you do not configure a DAG filter, the generic feeds from all regions and services are displayed. You must configure at least one DAG filter to not get the generic feeds.

To configure DAG filters, do the following:

1. Select **Shared Services > Advanced Threat Prevention > SecIntel Feeds > DAG Filters**.

The DAG Filters page appears.

2. Click the plus sign (+).

The Create DAG Filter window appears.

3. (Optional) Enter a description for the DAG filter.
4. Select region from the **Region** list.
5. Select service from the **Service** list.

The name for the DAG filter is automatically generated in the **Name** field when you select the region and service. You cannot edit the DAG filter name.

NOTE: The exact names for AWS regions and services are displayed in the **Name** field for the DAG filter. This mapping is applicable only for the manifest file so that the DAG feed name is supported on the SRX Series Firewall.

Junos OS supports a maximum length of 32 characters for the DAG filter name. If the feed name exceeds the limit, the cloud feeds manifest file will not display the feed name.

6. Click **OK**.

You can see the DAG feeds for the selected AWS region and service in the DAG Filter page.

Configure Webhook

Access the Audit Log Web Hook page from the **Shared Services > Advanced Threat Prevention > Misc Configuration > Webhook** menu.

A webhook is an automated message or real-time notification that your application receives from another application that triggers an event. It communicates data about the occurrence of an event in one system to another system. This communication of data happens over the Web through a webhook URL.

You can use an audit log webhook to send Juniper ATP Cloud audit log notifications to a remote server. You can enable the webhook and configure the remote server URL to receive the audit log notifications in a chat application that can process JavaScript Object Notation (JSON) responses.

Before you begin:

- Configure your chat application to receive the audit log notifications. See [Create Incoming Webhooks](#) page for instructions to create a webhook URL. Copy and save the webhook URL.

To enable and configure the webhook, do the following:

1. Select **Shared Services > Advanced Threat Prevention > Misc Configuration > Webhook**.
The Audit Log Webhook page appears.
2. Select **Enable Webhook** toggle button to enable the Audit Log Webhook.
3. Paste the webhook URL in the **Webhook URL** field.
4. Click **Save**.

You will now receive the audit log notifications in your chat application.

Insights-On-prem Collectors

IN THIS CHAPTER

- [About the Collectors Page | 978](#)
- [About the Log Parsers Page | 979](#)
- [Create a Log Parser | 980](#)
- [Edit and Delete a Log Parser | 985](#)
- [About the Log Sources Page | 986](#)
- [Create a Log Source | 987](#)
- [Edit and Delete a Log Source | 987](#)
- [About the Identity Settings Page | 988](#)
- [Add JIMS Configuration | 989](#)
- [Edit and Delete an Identity Setting | 991](#)

About the Collectors Page

IN THIS SECTION

- [Tasks You Can Perform | 979](#)
- [Field Descriptions | 979](#)

To access this page, select **Juniper Security Director Cloud > Shared Services > Insights > On-prem Collectors > Status**.

If you have any third party security product, you'll need to download the Security Director Cloud Insights OVA file from the software download site and deploy. See [Deploy and Configure Security Director Cloud Insights On-premises Collector with OVA Files](#).

After you deploy and configure an on-premises log collector, you can use the Collectors page to view collector details such as name, IP address, disk, memory, CPU, and status.

Tasks You Can Perform

You can perform the following tasks from the Collectors page:

- View the on-premises collector details—Select the collector, right-click and select **Detail**. You can also select **Detail** from the More list.

Field Descriptions

[Table 352 on page 979](#) provides guidelines on using fields on the Collectors page.

Table 352: Fields on the Collectors Page

Field	Description
Name	Name of the on-premises collector.
IP Address	IP address of the on-premises collector.
Disk	Specifies the disk usage.
Memory	Specifies the memory usage of the collector.
CPU	Specifies the CPU usage.
Last Seen	Timestamp specifies that the collector is connected.
Status	Specifies the health of the collector.

About the Log Parsers Page

IN THIS SECTION

- [Tasks You Can Perform | 980](#)

To access this page, select **Juniper Security Director Cloud > Shared Services > Insights > On-prem Collectors > Log Parsers**.

Use the flexible log parser to define how the system log data must be parsed. The flexible parser enables you to provide a sample of your logs to create a new parser, parse the logs, normalize the fields, filter logs based on your configured criteria, and assign severity and semantics to various fields. You can create multiple parsers for different log sources.

Tasks You Can Perform

You can perform the following tasks from the Log Parsers page:

- Create a new log parser. See ["Create a Log Source" on page 987](#) .
- Edit and delete a log parser. See ["Edit and Delete a Log Parser" on page 985](#) .

Field Descriptions

[Table 353 on page 980](#) provides guidelines to configure log parsers.

Table 353: Fields on the Log Parsers Page

Field	Description
Name	Specifies the name of the log parser that you have created.
Description	Specifies the corresponding description provided for the log parser.

Create a Log Parser

Use the Create Log Parser page to create your own log parser by using sample logs. You can build your own parser by mapping fields in your sample logs to Security Director Cloud Insights event fields, indicating which types of events will generate an incident.

To create a new log parser:

1. Log in to Juniper Security Director Cloud.
2. Select **Shared Services > Insights > On-prem Collectors > Log Parsers**.
The Log Parsers page is displayed.
3. Select the plus icon (+).
The Create Log Parser page is displayed.
4. Complete the configuration according to the guidelines provided in [Table 354 on page 981](#).
5. Click **Finish**, and you are presented with the results of your flexible log parser as they are applied to the sample logs provided.
Review the results carefully to determine whether your mapping, filtering, and assignment conditions are as expected.

Table 354: Create Log Parser

Setting	Guideline
<i>Create/Edit Log Parser</i>	
Name	Enter a unique and descriptive name for the log parser.
Description	Enter a description for the log parser.
<i>Log File</i>	
Raw Log File	Upload the raw log file by browsing to it.
Raw Log Content	Paste the log data. Ensure the log file contains an RFC-compliant syslog header.
Log File Format	Specify the format of the sample log file. The available options are: <ul style="list-style-type: none"> • XML • JSON • CSV • Others

Table 354: Create Log Parser (Continued)

Setting	Guideline
CSV Headers (if the log file format is CSV)	If your log file is in CSV format, you may provide a comma-delimited list of field names in this field. If the CSV headers are not provided, the fields will be named as csv <i>N</i> , where <i>N</i> is the field position.
Grok Pattern (if the log file format is others)	If you select the Others option for the log file format, you must supply a grok pattern for the log file. A grok pattern may consist of one or more lines. The grok pattern line beginning with LOGPATTERN is the pattern that will be applied to the logs. A grok pattern must include a pattern named LOGPATTERN, otherwise the parser will not have any pattern to use.
<i>Field Mapping</i>	
Field Mapping	<p>In the Field Mapping section, click the + icon. Then on the Field mapping page, select a field in the Parsed Fields column and then select a value in the Insights Fields Name column to map. After selecting both the fields, click Map. The mapped fields now appear in the Field Mapping section, which lists all fields that have been mapped to each other.</p> <p>You can perform the following action from the Field Mapping section:</p> <ul style="list-style-type: none"> • Enable the Counter to count the number of times a field appears. <p>NOTE: Fields marked with * are mandatory.</p>
<i>Date Format</i>	
Date Format	Select a date format that appears in the event logs.
<i>Log Filtering</i>	

Table 354: Create Log Parser *(Continued)*

Setting	Guideline
Log Filtering	<p>You can create filters to notify Security Director Cloud Insights about malicious and unmalicious events as you decide what logs are to be kept and which ones can be ignored. Log filtering removes logs that are “noisy” and not of particular interest and retains logs that are related to malicious events.</p> <p>Click + icon and configure filtering conditions as follows:</p> <ul style="list-style-type: none"> • Select a log file field from the list. • Select a suitable filter condition from the list such as Matches, Contains, Does not Contain, and so on. If you select Matches, your provided string must match the selected field exactly. If you select Contains, your provided string must appear as a substring within the selected field. • Enter a string to filter log files. <p>Click OK and your condition is added to the filter. You can add multiple filters by clicking the + icon.</p> <p>NOTE: Select the check box for a filter and click Edit or Delete icons to edit or remove the filter.</p>

Conditions Assignment

Table 354: Create Log Parser (Continued)

Setting	Guideline
Event Severity	<p>You can assign different conditions to an event, based on the filtering parameters you configure.</p> <ul style="list-style-type: none"> • Event Severity—Assign conditions to define the severity of an event. Click Add and set conditions as follows: <ul style="list-style-type: none"> • Select a severity level. The options are Benign, Low, Medium, High, and Critical. • Select a field from the list to set the severity level for that field. • Select a condition. For example, If you select Matches, your string must match the selected field exactly. If you select Contains, your string must appear as a substring within the selected field. • Enter a value to filter log files and click OK. • Progression—Assign conditions to define the progression of an event. Click the + icon and set conditions as follows: <ul style="list-style-type: none"> • Select a progression level. The options are Phishing, Exploit, Download, Infection, and Execution. • Select a field from the list to set the progression level for that field. • Select a condition. For example, If you select Matches, your string must match the selected field exactly. If you select Contains, your string must appear as a substring within the selected field. • Enter a value to filter log files and click OK. • Blocked—Assign conditions to define the event is blocked or not. Click the + icon and set conditions as follows: <ul style="list-style-type: none"> • Select a blocked level. The options are True and False. • Select a field from the list to set the block level for that field. • Select a condition. For example, If you select Matches, your string must match the selected field exactly. If you select Contains, your string must appear as a substring within the selected field. • Enter a value to filter log files and click OK.

Edit and Delete a Log Parser

IN THIS SECTION

- [Edit a Log Parser | 985](#)
- [Delete a Log Parser | 985](#)

You can edit and delete a log parser from the Log Parsers page.

Edit a Log Parser

To edit a log parser:

1. Log in to Juniper Security Director Cloud.
2. Select **Shared Services > Insights > On-prem Collectors > Log Parsers**.
The Log Parsers page is displayed.
3. Select the log parser that you want to edit, and click the pencil icon.
The Edit Log Parser page is displayed, that shows the same fields that were presented when you added new log parser.
4. Modify the log parser fields.
5. Click **Finish** to save your changes.
You are taken to the Log Parsers page. A confirmation message appears, indicating the status of the edit operation.

Delete a Log Parser

To delete a log parser:

1. Log in to Juniper Security Director Cloud.
2. Select **Shared Services > Insights > On-prem Collectors > Log Parsers**.
The Log Parsers page is displayed.
3. Select a log parser that you want to delete and click the delete icon.
An alert message appears, asking you to confirm the delete operation.
4. Click **Yes** to delete the log parser.
A confirmation message appears, indicating the status of the delete operation.

About the Log Sources Page

IN THIS SECTION

- [Tasks You Can Perform | 986](#)
- [Field Descriptions | 986](#)

To access this page, select **Juniper Security Director Cloud > Shared Services > Insights > On-prem Collectors > Log Sources**.

You can create multiple log parsers for different log sources. The log source name is the hostname portion of the syslog message that Security Director Cloud Insights uses to identify the log source, and how Security Director Cloud Insights parses its logged events.

Tasks You Can Perform

You can perform the following tasks from the Log Sources page:

- Create a log source. See "[Create a Log Source](#)" on page 987 .
- Edit and delete log sources. See "[Edit and Delete a Log Source](#)" on page 987 .
- View all incoming logs and all created events in last 7 days. Click **Counters**.

Field Descriptions

[Table 355 on page 986](#) provides guidelines on using the fields on the Log Sources page.

Table 355: Fields on the Log Sources Page

Field	Description
Identifier	Specifies the unique string that needs to be looked for.
Parser	Specifies the name of the log parser assigned to the log source.
Severity	Specifies the severity of the log parser.

Create a Log Source

Use the Create Log Source page to create a log source and assign the log parser with a severity level.

To add a log source:

1. Log in to Juniper Security Director Cloud.
2. Select **Shared Services > Insights > On-prem Collectors > Log Sources**.
The Log Sources page is displayed.
3. Click **Create**.
The Create Log Source page is displayed.
4. Complete the configuration according to the guidelines provided in [Table 356 on page 987](#).
5. Click **OK**.
A new log source is created and listed on the Log Sources page.

Table 356: Fields on the Create Log Source Page

Field	Guideline
Log Source Identifier	Enter the hostname of the log.
Parser	Select a required log parser from the list.
SSL	You can enable or disable SSL.
Severity	Assign a default severity level from the list.

Edit and Delete a Log Source

IN THIS SECTION

- [Edit a Log Source | 988](#)
- [Delete a Log Source | 988](#)

You can edit and delete log sources from the Log Sources page.

Edit a Log Source

To edit a log source:

1. Log in to Juniper Security Director Cloud.
2. Select **Shared Services>Insights> On-prem Collectors > Log Sources**.

The Log Sources page appears.

3. Select the log source that you want to edit and click the pencil icon.

The Update Log Source page is displayed, which shows the same fields that were presented when you added new log sources.

4. Modify the log source fields.
5. Click **OK** to save your changes.

You are taken to the Log Sources page. A confirmation message is displayed, indicating the status of the edit operation.

Delete a Log Source

To delete a log source:

1. Log in to Juniper Security Director Cloud.
2. Select **Shared Services>Insights> On-prem Collectors > Log Sources**.

The Log Sources page is displayed.

3. Select the log source that you want to delete and click the delete icon.

An alert message is displayed, asking you to confirm the delete operation.

4. Click **Yes** to delete the log source.

A confirmation message is displayed, indicating the status of the delete operation.

About the Identity Settings Page

IN THIS SECTION

- [Tasks You Can Perform | 989](#)
- [Field Descriptions | 989](#)

To access this page, select **Juniper Security Director Cloud > Shared Services > Insights > On-prem Collectors Identity Settings**.

Security Director Cloud Insights interfaces with Juniper Identity Management Service (JIMS) to map endpoint IP addresses in events and logs to usernames and hostnames. You can configure JIMS to provide access information to Security Director Cloud Insights.

Tasks You Can Perform

You can perform the following tasks from the Identity Settings page:

- Add JIMS configuration. See ["Add JIMS Configuration" on page 989](#) .
- Delete or edit an existing JIMS configuration. See ["Edit and Delete an Identity Setting" on page 991](#) .
- Select **Test** to test the JIMS configuration. You can verify the configuration and check whether the Security Director Cloud Insights VM can communicate with JIMS successfully.

Field Descriptions

[Table 357 on page 989](#) provides guidelines to use fields on the Identity Settings page.

Table 357: Fields on the Identity Settings Page

Field	Description
Hostname/IP	Valid IPv4 or IPv6 address or the hostname of the JIMS server.
Port	Connection port of the JIMS server.

Add JIMS Configuration

Use the Add JIMS Configuration page to configure a JIMS profile to obtain user identities. Ensure that you have added the IP address of Security Director Cloud Insights in the JIMS server.

To add JIMS configuration:

1. Log in to Juniper Security Director Cloud.
2. Select **Shared Services > Insights > On-prem Collectors > Identity Settings**.

The Identity Settings page is displayed.

3. Click the + icon to add the JIMS configuration.

The Add JIMS Configuration page is displayed.

4. Complete the configuration according to the guidelines provided in [Table 358 on page 990](#).

5. Click **OK**.

A new JIMS configuration is added to Security Director Cloud Insights and listed on the Identity Settings page.

Table 358: Add JIMS Configuration

Setting	Guideline
JIMS	Enter a valid IPv4 or IPv6 address or the hostname of the JIMS server.
JIMS Port Number	Select the connection port of the JIMS server from the list.
TLS	Enable or Disable the TLS setting.
Identity Sources	Select an identity source to collect data from: Active Directory, Syslog, or both.
Use Reverse DNS	Reverse DNS lookup converts an IP address to hostname to identify the domain name of the source. Choose to enable or disable the Use Reverse DNS setting. This option is disabled by default.
Exclude hostnames	You can disallow identity mapping for certain hosts. Enter the hostnames separated by commas. Identity mappings for these hosts are ignored and not included in event handling and displays.
OAuth Client ID	<p>Enter the Open Authorization (OAuth) client ID that the Security Director Cloud Insights provides to the JIMS server as part of its authentication. Security Director Cloud Insights must authenticate itself with the JIMS server to obtain an access token that allows it to query the JIMS server for user identity information.</p> <p>The client ID must be consistent with the API client configured on JIMS.</p>
OAuth Client Secret	Enter the client secret that Security Director Cloud Insights provides to the JIMS server as part of its authentication. The client secret must be consistent with the API client configured on JIMS.

Edit and Delete an Identity Setting

IN THIS SECTION

- [Edit a JIMS Configuration | 991](#)
- [Delete a JIMS Configuration | 991](#)

You can edit and delete a JIMS configuration from the Identity Settings page.

Edit a JIMS Configuration

To edit a JIMS configuration:

1. Log in to Juniper Security Director Cloud.
2. Select **Shared Services>Insights> On-prem Collectors> Identity Settings**.
The Identity Settings page is displayed.
3. Select the JIMS configuration that you want to modify, and click the **Edit** icon.
The Edit JIMS Configuration page appears, displaying the same fields that were presented when you added the JIMS configuration.
4. Modify the JIMS configuration fields.
5. Click **OK** to save your changes.
You are taken to the Identity Settings page. A confirmation message is displayed, indicating the status of the edit operation.

Delete a JIMS Configuration

To delete a JIMS configuration:

1. Log in to Juniper Security Director Cloud.
2. Select **Shared Services>Insights> On-prem Collectors> Identity Settings**.
The Identity Settings page is displayed.
3. Select the JIMS configuration that you want to delete, and click the **Delete** icon.
An alert message is displayed, asking you to confirm the delete operation.
4. Click **Yes** to delete the selected JIMS configuration.
A confirmation message is displayed, indicating the status of the delete operation.

Insights-Cloud Collector

IN THIS CHAPTER

- [About the Cloud Collector Page | 992](#)

About the Cloud Collector Page

IN THIS SECTION

- [Tasks You can Perform | 992](#)

To access this page, select **Juniper Security Director Cloud > Shared Services > Insights > Cloud Collector**.

If you have SRX logs from Juniper Secure Edge or from SRX firewall, then you can enable insights functionality for all logs directly incoming from SRX Series Firewall.

Tasks You can Perform

- Enable or disable the **Log Source:Juniper SRX Parser** option to enable or disable insights functionality for all logs directly incoming from SRX Series Firewall.

Insights-Rules

IN THIS CHAPTER

- [About the Event Scoring Rules Page | 993](#)
- [Create an Event Scoring Rule | 994](#)
- [Edit and Delete Event Scoring Rules | 995](#)
- [About the Incident Scoring Rules Page | 996](#)
- [Create an Incident Scoring Rule | 998](#)
- [Edit and Delete Incident Scoring Rules | 999](#)

About the Event Scoring Rules Page

IN THIS SECTION

- [Tasks You Can Perform | 994](#)
- [Field Descriptions | 994](#)

To access this page, select **Juniper Security Director Cloud > Shared Services > Insights > <Rules> Event Scoring Rules**.

You can use the event scoring rules to customize the log event to match your security operation center (SOC) processes. Rules comprise the following elements:

- **Condition**—The rules engine supports several match operations for different field types. For example, the matching operations include conditions such as Matches, Contains, Greater Than, and Less Than. You can combine multiple matching criteria in an ANY (OR) configuration or an ALL (AND) configuration. To apply a condition, select a normalized field from the event and match the criteria that trigger the rule.

- **Action**—An action is a response to an event. You can configure, increase, or lower the severity or look up a threat intelligence source.

Tasks You Can Perform

You can perform the following tasks from the Event Scoring Rules page:

- Create an event scoring rule. See ["Create an Event Scoring Rule" on page 994](#) .
- Edit and delete an event scoring rule. See ["Edit and Delete Event Scoring Rules" on page 995](#) .
- Enable or disable an event scoring rule. Click **Enable** or **Disable** to either enable the event scoring rule or disable it.

Field Descriptions

[Table 359 on page 994](#) provides guidelines on using the fields on the Event Scoring Rules page.

Table 359: Fields on the Event Scoring Rules Page

Field	Description
Rule Name	Specifies the name of the rule.
Rule Description	Specifies the condition applied for the rule.
Match Any/All Rules	Specifies the matching criteria set for the rule.
Actions	Specifies the action to be taken when the condition of a rule is met.
Status	Specifies the status of the rule, whether enabled or disabled.

Create an Event Scoring Rule

You can create rules for the log events by defining the matching condition and corresponding actions to take when a condition is met.

To create a rule for scoring log events:

1. Log in to Juniper Security Director Cloud.
2. Select **Shared Services > Insights > Rules > Event Scoring Rules**.
The Event Scoring Rules page appears.
3. Click the plus icon (+).
The New Event Scoring Rules page appears, on which you can define the rule's condition and actions.
4. In the Rule Name text box, enter a unique name for the rule and the select the match type **Match Any** or **Match All**.
5. In the Condition section:
 - Select the field name from the list.
 - For the selected event, select a condition from the list.
 - For the selected condition, provide the value.
 - If you are defining more than one condition, click the + icon.
6. In the Actions section:
 - a. Select a required action from the list, such as Raise or Lower Severity, Set Severity (value), Check feed, and Skip remaining rules.
 - b. For the selected action, assign the additional actions from the list.
 - c. If you are defining more than one action, click the + icon.
7. Click **OK**.
A new rule is created and listed on the Event Scoring Rules page.

Edit and Delete Event Scoring Rules

IN THIS SECTION

- [Edit an Event Scoring Rule | 995](#)
- [Delete an Event Scoring Rule | 996](#)

You can edit and delete event rules from the Event Scoring Rules page.

Edit an Event Scoring Rule

To edit an event scoring rule:

1. Log in to Juniper Security Director Cloud.
2. Select **Shared Services > Insights > Rules > Event Scoring Rules**.
The Event Scoring Rules page is displayed.
3. Select the rule that you want to edit, and click the pencil icon.
The Edit Event Scoring Rule page appears, displaying the same fields that were presented when you created a new rule.
4. Modify the rule.
5. Click **OK** to save your changes.
You are taken to the Event Scoring Rules page. A confirmation message appears, indicating the status of the edit operation.

Delete an Event Scoring Rule

To delete an event scoring rule:

1. Log in to Juniper Security Director Cloud.
2. Select **Shared Services > Insights > Rules > Event Scoring Rules**.
The Event Scoring Rules page is displayed.
3. Select the rule that you want to delete, and click the delete icon.
An alert message appears, asking you to confirm the delete operation.
4. Click **Yes** to delete the rule.
A confirmation message appears, indicating the status of the delete operation.

About the Incident Scoring Rules Page

IN THIS SECTION

- [Tasks You Can Perform | 997](#)
- [Field Descriptions | 997](#)

To access this page, select **Juniper Security Director Cloud > Shared Services > Insights > <Rules> Incident Scoring Rules**.

Use incident scoring rules to score the risk of an incident by verifying that the indicators of compromise are already blocked from execution or mitigated by other events that contributed toward this incident.

Rules comprise the following elements:

- Condition—The matching condition available for any field type are *mitigated by another event* and *not mitigated by another event*.
- Action—An action is a response to an incident. You can raise or lower the severity, set the severity value, or skip the remaining rules.

Tasks You Can Perform

You can perform the following tasks from the Incident Scoring Rules page:

- Create an incident scoring rule. See ["Create an Incident Scoring Rule" on page 998](#) .
- Edit and delete an incident scoring rule. See ["Edit and Delete Incident Scoring Rules" on page 999](#) .
- Enable or disable an incident scoring rule. Click **Enable** or **Disable** to either enable the incident scoring rule or disable it.

Field Descriptions

[Table 360 on page 997](#) provides guidelines on using the fields on the Incident Scoring Rules page.

Table 360: Fields on the Incident Scoring Rules Page

Field	Description
Rule Name	Specifies the name of the rule.
Rule Description	Specifies the condition applied for the rule.
Match Any/All Rules	Specifies the match criteria set for the rule.
Actions	Specifies the action to be taken when the condition of a rule is met.
Status	Specifies the status of the rule, whether enabled or disabled.

Create an Incident Scoring Rule

You can create rules for incidents by defining the matching condition and corresponding actions to take when a condition is met.

To create a rule for scoring incidents:

1. Log in to Juniper Security Director Cloud.
2. Select **Shared Services > Insights > Rules > Incident Scoring Rules**.
The Incident Scoring Rules page is displayed.
3. Click the **+** icon.
The New Incident Scoring Rule page is displayed, where you can define rule's condition and actions.
4. In the Rule Name field, enter a unique name for the rule and select a matching condition from the list: **Match Any** or **Match All**.
5. In the Condition section:
 - a. Select the type of incident from the list: **File Hash**, **Threat Source IP**, or **URL**.
 - b. For the selected incident, select **mitigated by another event** or **not mitigated by another event** as the condition.

NOTE: To add multiple conditions, click **+**.

6. In the Action section:
 - a. Select a required action from the list, such as **Raise or Lower Severity**, **Set Severity (value)**, or **Skip remaining rules**.
 - b. Based on the action you have selected, provide additional data.

NOTE: To add multiple actions, click **+**.

7. Click **OK**.

A new rule is created and listed in the New Incident Scoring Rules page.

Click **Enable** or **Disable** to either enable the incident scoring rule or disable it.

Edit and Delete Incident Scoring Rules

IN THIS SECTION

- [Edit an Incident Scoring Rule | 999](#)
- [Delete an Incident Scoring Rule | 999](#)

You can edit and delete an incident scoring rule from the Incident Scoring Rules page.

Edit an Incident Scoring Rule

To edit an incident scoring rule:

1. Log in to Juniper Security Director Cloud.
2. Select **Shared Services > Insights > Rules > Incident Scoring Rules**.
The Incident Scoring Rules page is displayed.
3. Select the rule that you want to edit, and click the pencil icon.
The Edit Incident Scoring Rules page is displayed, which shows the same fields that were presented when you created a new rule.
4. Modify the rule.
5. Click **OK** to save your changes.
You are taken to the Incident Scoring Rules page. A confirmation message appears, indicating the status of the edit operation.

Delete an Incident Scoring Rule

To delete an incident scoring rule:

1. Log in to Juniper Security Director Cloud.
2. Select **Shared Services > Insights > Rules > Incident Scoring Rules**.
The Incident Scoring Rules page is displayed.
3. Select the rule that you want to delete, and click the delete icon.
An alert message is displayed, asking you to confirm the delete operation.
4. Click **Yes** to delete the rule.
A confirmation message is displayed, indicating the status of the delete operation.

Insights-Settings

IN THIS CHAPTER

- [About the Threat Intelligence Page | 1000](#)
- [Configure Threat Intelligence Source | 1001](#)
- [Edit and Delete Threat Intelligence Source | 1002](#)
- [About the Service Now Configuration | 1003](#)
- [About the Correlation Time Page | 1004](#)

About the Threat Intelligence Page

IN THIS SECTION

- [Tasks You Can Perform | 1001](#)
- [Field Descriptions | 1001](#)

To access this page, select **Juniper Security Director Cloud > Shared Services > Insights > Settings > Threat Intelligence**.

Look up your trusted threat intelligence providers for indicators of compromise to confirm the maliciousness of the reported event. Indicators of compromise include IP addresses, URLs, and file hash observed in the log data. What is considered malicious is based on available knowledge about the threat intelligence provider's output.

Security Director Cloud Insights supports the following threat intelligence sources:

Source	Data
IBM X-Force	IP lookup and file hash
VirusTotal	File hash and URL lookup
OPSWAT Metadefender	File hash, URL lookup, and IP lookup

Tasks You Can Perform

You can perform the following tasks from the Threat Intelligence page:

- Configure a threat intelligence source. See ["Configure Threat Intelligence Source" on page 1001](#) .
- Edit and delete an existing threat intelligence source. See ["Edit and Delete Threat Intelligence Source" on page 1002](#) .
- Click **Test** to test the validity of the API key and check whether the Security Director Cloud VM can reach a threat intelligence source.

Field Descriptions

[Table 361 on page 1001](#) provides guidelines on using the fields on the Threat Intelligence page.

Table 361: Fields on the Threat Intelligence Page

Field	Description
Source	Specifies the threat intelligence source.
Description	Specifies the corresponding API details configured for the threat intelligence source.

Configure Threat Intelligence Source

Configure the threat intelligence providers for IP address, URL, file hash to confirm the maliciousness of the reported event.

To configure the threat intelligence source:

1. Log in to Juniper Security Director Cloud.
2. Select **Shared Services > Insights > Settings > Threat Intelligence**.
The Threat Intelligence page is displayed.
3. Click the **+** icon.
The Create Configuration page is displayed.
4. Complete the configuration according to the guidelines provided in [Table 362 on page 1002](#).
5. Click **OK**.
A new threat intelligence source is configured and listed on the Threat Intelligence page.

Table 362: Configure Threat Intelligence Source

Field	Guideline
Source Name	Select the threat intelligence providers from the list. The supported threat intelligence providers are IBM X-Force, VirusTotal, and OPSWAT Metadefender.
API Key	Enter a valid API key to look up the threat intelligence provider's APIs. <ul style="list-style-type: none"> • VirusTotal API Key • OPSWAT API Key • IBM X-Force API Key
API Password	Enter a password, if you are using IBM X-Force, to look up the threat intelligence provider's APIs.

Edit and Delete Threat Intelligence Source

IN THIS SECTION

- [Edit a Threat Intelligence Source | 1003](#)
- [Delete a Threat Intelligence Source | 1003](#)

You can edit and delete the threat intelligence providers from the Threat Intelligence page.

Edit a Threat Intelligence Source

To edit a threat intelligence source configuration:

1. Log in to Juniper Security Director Cloud.
2. Select **Shared Services > Insights > <Settings> Threat Intelligence**.

The Threat Intelligence page is displayed.

3. Select the threat intelligence source that you want to modify, and click the pencil icon.

The Modify Configuration page is displayed, which shows the same fields that were presented when you configured the threat intelligence sources.

4. Modify the configuration fields as needed.
5. Click **OK** to save your changes.

You are taken to the Threat Intelligence page. A confirmation message appears, indicating the status of the edit operation.

Delete a Threat Intelligence Source

To delete a threat intelligence source:

1. Log in to Juniper Security Director Cloud.
2. Select **Shared Services > Insights > <Settings> Threat Intelligence**.

The Threat Intelligence page is displayed.

3. Select the threat intelligence source that you want to delete and click the **Delete** icon.

An alert message is displayed, asking you to confirm the delete operation.

4. Click **Yes** to delete the selected threat intelligence source.

A confirmation message is displayed, indicating the status of the delete operation.

About the Service Now Configuration

IN THIS SECTION

- [Tasks You Can Perform | 1004](#)
- [Field Descriptions | 1004](#)

To access this page, select **Juniper Security Director Cloud > Shared Services > Insights > Settings > Service Now**.

You can configure your Service Now account to create tickets for incidents.

Tasks You Can Perform

You can perform the following tasks from the Service Now Configuration page:

- Configure your Service Now account.

Field Descriptions

[Table 363 on page 1004](#) provides guidelines on using the fields on the Service Now page.

Table 363: Fields on the Service Now Page

Field	Description
URL	Specify the URL of your Service Now account. Ensure that you have provided the correct URL. For example, https://example.service-now.com/ .
Username	Specify the username to access the Service Now instance URL.
Password	Specify the password to access the Service Now instance URL.

After you configure the Service Now account successfully, you can start creating Service Now tickets for any incidents on the **Monitor > Insights > Incidents** page. Click an incident and click **Service Now Ticket** to create the ticket.

About the Correlation Time Page

IN THIS SECTION

- [Task You can Perform | 1005](#)

To access this page, select **Juniper Security Director Cloud > Shared Services > Insights > <Settings> Miscellaneous**.

Correlation time is the time in minutes required to create the window in which related events are grouped within an incident.

Task You can Perform

- Set correlation time window. Select the time in minutes.

7

PART

Administration

[Subscriptions](#) | 1007

[Users & Roles](#) | 1013

[Single Sign-On Configuration](#) | 1026

[Audit Logs](#) | 1028

[Service Updates](#) | 1032

[Jobs](#) | 1034

[Data Management](#) | 1040

[Log Streaming](#) | 1043

[URL Recategorization](#) | 1047

[Organization](#) | 1051

[ATP Mapping](#) | 1059

[ATP Audit Logs](#) | 1062

Subscriptions

IN THIS CHAPTER

- Subscriptions Overview | 1007
- Subscription Notifications | 1008
- About the Subscriptions Page | 1009
- Add a Subscription | 1011
- Delete a Subscription | 1012

Subscriptions Overview

IN THIS SECTION

- SRX Management Subscriptions | 1007
- Secure Edge Subscriptions | 1007
- Storage Subscriptions | 1008

SRX Management Subscriptions

The SRX Management subscription manages the devices within Juniper Security Director Cloud. After you purchase a device subscription and add it in Juniper Security Director Cloud, associate the device with the subscription. See "[Device Subscriptions Overview](#)" on page 228 for details

Secure Edge Subscriptions

Secure Edge has the following types of subscriptions:

- The Secure Edge subscription that enables the service for all licensed users. The subscription also entitles you to deploy the service in two cloud service locations.
- The Extra Service Location subscription that provides additional service locations for the licensed users of the base license.

Storage Subscriptions

The storage subscription provides additional storage space in Juniper Security Director Cloud and Secure Edge for longer retention of data gathered from devices. After you purchase the storage subscription and add it in Juniper Security Director Cloud, the storage subscriptions are associated with the organization.

For more details about these subscriptions, see [Datasheet](#). To purchase these subscriptions, contact your sales representative or account manager.

Subscription Notifications

The following table summarizes the frequency of the e-mail notifications and the notifications displayed on the Juniper Security Director Cloud UI:

NOTE: If the subscription has expired, in grace period, or beyond the grace period, you must delete the subscription and then add a new subscription. For instructions to add a subscription, see ["Add a Subscription" on page 1011](#) .

Table 364: Subscription Notifications

Account Type	Duration	SRX Management Subscription	Secure Edge Subscription	Storage Subscription
Paid	28 days to 3 days before the expiry	Weekly once	Weekly once	Weekly once
	3 days before the expiry	Daily	Daily	Daily
	During the grace period ¹	Weekly once	Weekly once	Weekly once

Table 364: Subscription Notifications (*Continued*)

Account Type	Duration	SRX Management Subscription	Secure Edge Subscription	Storage Subscription
	After the grace period ends	No notifications	No notifications	No notifications
Trial	48 hours before the expiry	Once	Once	Not applicable
	During the grace period ²	Weekly once	Weekly once	Not applicable
	After the grace period ends	No notifications	No notifications	Not applicable

1 – The grace period for paid accounts is 30 days.

2 – The grace period for trial accounts of SRX Management and Secure Edge subscription is 30 days and 2 days respectively.

About the Subscriptions Page

IN THIS SECTION

- [Tasks You Can Perform | 1009](#)
- [Field Descriptions | 1010](#)

To access the Juniper Security Director Cloud subscriptions page, click **Administration > Subscriptions**.

Use the Subscriptions page to add and manage your Juniper Security Director Cloud and Juniper Secure Edge subscriptions.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a subscription. See ["Add a Subscription" on page 1011](#) .
- Delete a subscription. See ["Delete a Subscription" on page 1012](#) .
- Show or hide columns. Click the **Show Hide Columns** icon at the top right corner of the page.

Field Descriptions

["Field Descriptions" on page 1010](#) describes the fields on the Subscriptions page.

Table 365: Fields on the Subscriptions Page

Field	Description
Name	Displays the name of the subscription.
Entitlement	Displays the device and the log subscription information. Device subscriptions are displayed as number of devices that you can subscribe to, along with the number of years this subscription is valid. Log subscriptions are displayed as the amount of storage space entitled, along with the number of years this subscription is valid.
Actual Usage	Displays the number of devices associated with the device subscription. Hover over the number to view the names of the devices that are subscribed to this subscription.
Status	Displays whether the subscription is active or expired.
Expiry Date	Displays the expiry date on the subscription.
Plan	Displays the name of the plan associated with the device subscription and the log subscription.
SSRN	Displays the software support reference number (SSRN) which is the serial number of the subscription.

RELATED DOCUMENTATION

[About the Devices Page | 202](#)

[Manage Device Subscriptions | 228](#)

Add a Subscription

After you purchase your subscription, you must add it to your account. You can add one or more subscriptions as follows:

- You can add only one trial account of a subscription type.
- You can add multiple paid accounts of a subscription type.
- You can add trial and paid accounts of different subscription types. For example, if you add a trial account of an SRX Management Subscription, you can only add a paid account of an Secure Edge Subscription.
- You cannot add trial and paid accounts of the same subscription type. For example, if you add a trial account of an SRX Management Subscription, you cannot add a paid account of the same subscription type.

NOTE:

- If a trial account is not renewed within the grace period of 30 days after the expiry, all the organization data is deleted.
- If all the purchased subscriptions are expired and not renewed within the grace period, the storage logs are deleted.

1. Log in to Juniper Security Director Cloud.
2. Click **Administration > Subscriptions**.
The **Subscriptions** page is displayed.
3. Click **Add Subscriptions**.
The **Add Subscriptions** window is displayed.
4. Enter a name for the subscription.
5. Enter the Software Support Reference Number (SSRN) of the subscription.
6. To add multiple subscriptions, click **+** and repeat steps 4 and 5.
7. Click **OK**.
 - The subscription SSRN is verified.

- The subscription is activated.
- The subscription details are displayed in the corresponding section in the **Subscriptions** page.

Next, review your subscription details, such as activation state, expiration date, number of devices that you can subscribe to with this subscription, and so on.

Delete a Subscription

NOTE:

- You cannot delete active subscriptions.
- You can delete the subscriptions with unsuccessful SSRN activation or paid subscriptions that are expired. If you delete the subscriptions, you will not receive e-mail notifications about subscription renewal.
- When a device subscription is deleted, the devices that were associated with that subscription lose the entitlements provided by the subscription.

1. Log in to Juniper Security Director Cloud.
2. Click **Administration > Subscriptions**.
The Subscriptions page opens.
3. Select the subscriptions, and click the delete icon on the top-right corner of the page.

The selected subscriptions are deleted from your Juniper Security Director Cloud account.

Users & Roles

IN THIS CHAPTER

- [Users Overview | 1013](#)
- [About the Users Page | 1014](#)
- [Add a User | 1015](#)
- [Edit and Delete a User | 1017](#)
- [Roles Overview | 1019](#)
- [About the Roles Page | 1020](#)
- [Add a Role | 1021](#)
- [Edit, Clone, and Delete a Role | 1023](#)

Users Overview

Juniper Security Director Cloud supports authentication and role-based access control (RBAC) to its resources and services. You can access only the resources and actions that are defined in the roles assigned to you. For example, if you are assigned the operator role, you can only view the details of objects, such as devices and configuration templates. You do not have the permission to create, add, modify, or delete objects.

The use of access controls allows the assignment of different access privileges to different users.

Juniper Security Director Cloud provides the following default users and permissions:

- **administrator**—Users with the administrator role have full access to the Juniper Security Director Cloud GUI and API capabilities. They can add users, create custom roles, and user groups.
- **operator**—Users with the operator role have read-only access to the Juniper Security Director Cloud GUI.

About the Users Page

IN THIS SECTION

- [Tasks You Can Perform | 1014](#)
- [Field Descriptions | 1014](#)

To access this page, click **Administration > Users & Roles > Users**.

Tasks You Can Perform

You can perform the following tasks from this page:

- View the details of a user.

To view the details of a specific user, select the user, and click **More > Detail**. Alternatively, hover over the user name, and click the **Details** icon.

The user details are displayed in a pane on the right side of the page. The details contain basic information, such as the roles assigned to the user, the provider type of the user, and the status of the user.

- Add a User. See ["Add a User" on page 1015](#) .
- Edit and delete a user. See ["Edit and Delete a User" on page 1017](#) .
- Show/Hide Columns—Choose to show or hide a specific column in the table.

Hover over the vertical ellipses, select **Show/Hide Columns**, and select the check box of the columns to display in the table.

- Reset Preference—Reset the displayed columns to the default set of columns for each tab in the table.

Hover your mouse cursor over the vertical ellipses, and select **Reset Preference**.

Field Descriptions

[Table 366 on page 1015](#) displays the fields on the Users page.

Table 366: Fields on the Users Page

Field	Description
E-mail	The e-mail of the user.
Full Name	The name of the user.
Roles	<p>The roles assigned to the user.</p> <p>By default, this column lists only one role assigned to the user. When a user is assigned more than one role, a +(integer), such as +2, is displayed to the right side of the role. The integer indicates the number of additional roles assigned to the user. Click the integer to view additional roles.</p>
Status	<p>Indicates a user's account status.</p> <p>A user can log in to Juniper Security Director Cloud only if their account is active.</p>
Last Logged in	The date and time stamp when the user last logged in to their account.

Add a User

An administrator or a user with the privileges to add, edit, and delete users can add the following types of users to Juniper Security Director Cloud:

- Local users where the user is authenticated and authorized by Juniper Security Director Cloud.
- LDAP users where the user is authenticated by the LDAP server and authorized by Juniper Security Director Cloud.

1. Click **Administration > Users & Roles > Users**.

The Users page opens.

2. Click the + icon.

The Create User page opens.

3. Complete the configuration as described in [Table 367 on page 1016](#) .
4. Click **OK** to save the changes.

A confirmation message indicating that the user account is created is displayed and the user account is listed on the Users page.

After the user is created, if SMTP is configured on the device, the user receives an activation e-mail from Juniper Security Director Cloud. The e-mail contains the link to activate the new user account. By default, the activation link expires within 24 hours. If the user does not click the activation link and set a password, the account is not activated. To activate the account, you must resend the activation link by clicking **More > Resend activation mail**.

[Table 367 on page 1016](#) lists the fields on the Create User page.

Table 367: Fields on the Create User Page

Field	Description
Full Name	Enter the full name of the user containing maximum 32 alphanumeric characters. The name can contain special characters, such as underscores and hyphens.
Email	Enter a valid e-mail address in the user@domain format.
Action	Click the toggle button to enable or disable the user. By default, this option is enabled. A user can log in to Juniper Security Director Cloud only when you enable the user.
Role	Assign one or more roles to the user. To assign roles, select the roles in the left column, and click >. The selected roles are moved to the right column.

Edit and Delete a User

IN THIS SECTION

- [Edit a User | 1017](#)
- [Delete a User | 1019](#)

Edit a User

An administrator or a user with the privileges to add, edit, and delete users can edit a user.

NOTE:

- Administrator can view an e-mail address and edit the full name of the user for the selected organization account.
- As a user, you can view and edit all the details of your account.

1. Click **Administration > Users & Roles > Users**.

The Users page opens.

2. Select the user, and click the pencil icon.

The Edit User page opens.

3. Modify the parameters by following the guidelines provided in [Table 368 on page 1017](#).

Table 368: Fields on the Edit User Page

Field	Description
Full Name	<p>Enter the full name of the user containing maximum 32 alphanumeric characters.</p> <p>The name can contain special characters, such as underscores and hyphens.</p>

Table 368: Fields on the Edit User Page (Continued)

Field	Description
Email	<p>Enter a valid e-mail address in the user@domain format.</p> <p>You cannot change the email address of a user account after creating the account.</p>
Company name	<p>Enter the company name for the user having maximum 64 alphanumeric characters.</p> <p>The company name can contain spaces, underscores, and hyphens.</p> <p>You can change the company name only for your own user account.</p>
Country	<p>Select the country for the user.</p> <p>You can change the country only for your own user account.</p>
Phone number	<p>Enter a valid phone number containing between 7 to 18 characters.</p> <p>The phone number can contain numbers, plus sign, hyphens, and parentheses.</p> <p>You can change the phone number only for your own user account.</p>
Action	<p>Click the toggle button to enable or disable the user.</p> <p>By default, this option is enabled. A user can log in to Juniper Security Director Cloud only when you enable the user.</p>
Role	<p>Assign one or more roles to the user.</p> <p>To assign roles, select the roles in the left column, and click >. The selected roles are moved to the right column.</p>

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

A confirmation message indicating that the user account is modified is displayed and the updated information about the user is displayed on the Users page.

Delete a User

1. Click **Administration > Users & Roles > Users**.

The Users page opens.

2. Select the user, and click the trash can icon.

A message asking you to confirm the delete operation is displayed.

3. Click **Yes** to delete the users.

A confirmation message indicating that the selected user account is deleted from Juniper Security Director Cloud is displayed, and the user account is removed from the Users page.

Roles Overview

IN THIS SECTION

- [Types of Roles | 1019](#)
- [Access Privileges | 1020](#)

A role is a function assigned to a user that defines the tasks that the user can perform in Juniper Security Director Cloud. Each user can be assigned one or more roles depending on the tasks that the user is expected to perform.

User roles enable you to classify users based on the privileges assigned to them to perform tasks.

Types of Roles

Juniper Security Director Cloud provides the following types of roles:

- Pre-canned roles—System-defined roles with a set of predefined access privileges. Predefined roles are created while installing Juniper Security Director Cloud.
- Custom roles—User-defined roles with a set of access privileges. Customized roles can be created by the administrator or a user with the privilege to create users.

Access Privileges

User roles define the access privileges and actions to access objects, such as the dashboard, device templates, and devices in Juniper Security Director Cloud. For example, a user role can contain permissions to read device configurations and delete alert objects.

Juniper Security Director Cloud provides the following privileges:

- Read
- Create
- Update
- Delete
- Other actions, such as stage and deploy for the device software images

About the Roles Page

IN THIS SECTION

- [Tasks You Can Perform | 1020](#)
- [Field Descriptions | 1021](#)

To access this page, click **Administration > Users & Roles > Roles**.

Tasks You Can Perform

You can perform the following tasks from this page:

- View the details of a role.

To view the details of a specific role, select the role, and click **More > Detail**. Alternatively, hover over the role name, and click the **Details** icon.

The details of the role is displayed in a pane on the right side of the page. The details contain basic information, such as the roles scope and a link to the Preview Roles page. The Preview Roles page lists the access privileges assigned to the role.

- Create a customized role. See ["Add a Role" on page 1021](#) .
- Edit, clone, or delete a role. See ["Edit, Clone, and Delete a Role" on page 1023](#) .
- Show/Hide Columns—Choose to show or hide a specific column in the table.

Hover your mouse cursor over the vertical ellipses, select **Show/Hide Columns**, and select the check box of the columns to display in the table.

- Reset Preference—Reset the displayed columns to the default set of columns for each tab in the table.
Hover your mouse cursor over the vertical ellipses, and select **Reset Preference**.
- Sort Entries—Click on a column name to highlight the up and down arrows next to the column name. Sort the table entries in ascending or descending order of that column by clicking the up or down arrow respectively.

Field Descriptions

[Table 369 on page 1021](#) describes the fields on the Roles page.

Table 369: Fields on the Roles Page

Field	Description
Role Name	The name of the role.
Role Scope	The scope of the role is Organization. This is a read-only field.
Role Type	The type of role, which can be pre-canned and custom.
Created By	The user who created the role. The system indicates that the roles are pre-canned.

Add a Role

An administrator or a user with the privileges to add, edit, clone, and delete roles can add a role.

1. Select **Administration > Users & Roles > Roles**.

The Roles page opens.

2. Click the + icon to add a new role.

The Create Role page opens.

3. Complete the configuration according to the guidelines provided in [Table 370 on page 1022](#) .

4. Click **OK**.

A confirmation message indicating that the role is created is displayed, and the role is listed on the Roles page.

Table 370: Fields on the Add Roles Page

Field	Description
Role Name	Enter a unique name containing maximum alphanumeric 32 characters for the role. The name can contain special characters such as underscores, periods, and spaces.
Description	Enter a description containing maximum 255 characters for the role.
Role Scope	The scope of the role is Organization. This is a read-only field.

Table 370: Fields on the Add Roles Page (Continued)

Field	Description
Access Privileges	<p>Displays the objects in Juniper Security Director Cloud.</p> <p>You must select the check box against each object and select the privileges to assign to the user for the selected object. You can select multiple access privileges to assign to the user role.</p> <p>NOTE: You must assign at least one access privilege to a role.</p> <p>If you select the first-level objects, the submenu items that belong to the main object and the corresponding access privileges are also selected.</p> <p>The following access privileges can be assigned to a user role:</p> <ul style="list-style-type: none"> • Read— Enables the user to read existing objects. • Create—Enables the user to add new objects. • Update—Enables the user to edit or modify the existing objects. • Delete—Enables the user to delete objects. • Other Actions—Includes actions such as deploy, stage, upload, and simulate.

Edit, Clone, and Delete a Role

IN THIS SECTION

- [Edit a Role | 1024](#)
- [Clone a Role | 1024](#)
- [Delete a Role | 1024](#)

An administrator or a user with the privileges can edit, clone, and delete roles.

Edit a Role

You cannot edit pre-canned roles.

1. Select **Administration > Users & Roles > Roles**.

The Roles page opens displaying the details of the available roles.

2. Select the role, and click the pencil icon to modify the attributes.

The Edit Role page opens. The fields on the Edit Role page are available for editing.

3. Modify the role description and privileges.

You cannot modify the role name and the role scope.

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

A message indicating that the role is successfully edited opens, and the updated role information is displayed in the Roles table.

Clone a Role

You can clone a customized or pre-canned role when you want to quickly create a copy of an existing role and modify its access privileges.

1. Select **Administration > Users & Roles > Roles**.

The Roles page opens displaying the details of the available roles.

2. Select the role, and click the **Clone** button at the top-right corner of the page.

The Clone Role *Role-Name* page opens.

3. Specify an appropriate name for the cloned role.

The name must contain maximum 32 alphanumeric characters and can contain special characters such as underscores, periods, and spaces.

4. Click **OK** to save your changes.

A clone of the role is created and listed on the Roles page.

5. Select the new cloned role, and click the pencil icon to modify the parameters.

The Edit Role page opens.

6. Select the objects, and modify the access privileges of the role.

You cannot modify the role name and the role scope.

7. Click **OK** to save your changes.

A confirmation message indicating the status of the edit operation is displayed.

Delete a Role

You cannot delete a pre-canned role or a role that is assigned to a user.

1. Select **Administration > Users & Roles > Roles**.

The Roles page displaying the details of the available roles opens.

2. Select a role, and click the trash can icon.

A message asking you to confirm the delete operation is displayed.

3. Click **Yes** to delete the selected role.

A confirmation message indicating that the selected role is deleted is displayed, and the role is no longer listed on the Roles page.

Single Sign-On Configuration

IN THIS CHAPTER

- [Single Sign-On Configuration Overview | 1026](#)
- [Configure Single Sign-On Settings | 1027](#)

Single Sign-On Configuration Overview

IN THIS SECTION

- [Benefits | 1026](#)

Single Sign-On (SSO) is an authentication method that allows you to securely log in to multiple applications and websites with a single set of login credentials. Juniper Security Director Cloud enables you to manage access to the portal using network credentials.

Security Assertion Markup Language (SAML) is a framework for authentication and authorization between a service provider (SP) and an identity provider (IdP). Here, authentication is exchanged using digitally signed XML documents. The service provider agrees to trust the IdP to authenticate a user. In return, the IdP generates an authentication assertion indicating that the user is authenticated.

Benefits

- With SAML authentication, you can easily integrate Juniper Security Director Cloud with your corporate identity provider (IdP) to provide single sign-on. If you are authenticated to your IdP, you are automatically authenticated to Juniper Security Director Cloud. You need not remember separate passwords or type in credentials every time you access the Juniper Security Director Cloud portal.
- We support SAML protocol for both identity provider-initiated and service provider-initiated SSO. Juniper Security Director Cloud is compatible with SAML 2.0 web SSO profile as a service provider.

Configure Single Sign-On Settings

Ensure that Juniper Security Director Cloud is added as an application in Identity Providers (IdP) such as Okta or Microsoft Azure.

The **Single Sign-On Configuration** page enables you to configure SSO settings to allow users to sign in to Juniper Security Director Cloud portal using their network credentials. If a user is not added as a local user, they are redirected to the Identity Provider (IdP) portal to authenticate their credentials.

NOTE: You can configure SSO settings for a specific domain for an organization. You cannot configure SSO settings for multiple domains.

If a user is added as a local user and also a part of the domain configured in the **Single Sign-On Configuration** page, they can sign in using their account password and network credentials. For information about adding users and assigning roles, see ["Users Overview" on page 1013](#) and ["Roles Overview" on page 1019](#).

1. Go to Administration > SSO Configuration.

The **Single Sign-On Configuration** page is displayed.

2. Enable the SAML Profile toggle button to configure a SAML profile.

3. In the Identity Provider (IdP) section, select one of the following methods to configure IdP settings:

- **Enter metadata URL**-Select and enter the IdP metadata URL that must be used by the service provider to validate the SAML assertions.
- **Import settings**-Select and upload the XML file that contains the IdP metadata.
- **Enter settings manually**-Select and enter the IdP issuer URL, IdP portal URL, and then upload the IdP certificate to decrypt the SAML response.

4. In the Service Provider (SP) section, perform the following steps:

- a. Enter the user domain name.
- b. Enable the **Sign authentication requests** toggle button to sign the authentication requests from Juniper Security Director Cloud to your IdP. If you enable the toggle button, you must also provide the private key and public key certificates that is used to sign and validate the requests respectively.
- c. Select the role that must be assigned to the user. You can also create a new user role, if necessary. For information about users and roles, see ["Users Overview" on page 1013](#) and ["Roles Overview" on page 1019](#).

5. Click Save.

Audit Logs

IN THIS CHAPTER

- [Audit Logs Overview | 1028](#)
- [About the Audit Logs Page | 1029](#)
- [Export Audit Logs | 1031](#)

Audit Logs Overview

An audit log is a record of a sequence of activities that have affected a specific operation or procedure. Audit logs are useful for tracing events and for maintaining historical data.

Audit logs contain information about tasks initiated by using the Juniper Security Director Cloud GUI or APIs. In addition to providing information about the resources that were accessed, audit log entries usually include details about user-initiated operations, such as the name, role, and IP address of the user who initiated an operation, the status of the operation, and date and time of execution.

NOTE:

- Juniper Security Director Cloud retains the audit log for 6 months.
- Device-driven tasks (that is, tasks not initiated by the user) are not recorded in audit logs.

Administrators can use audit logs to review events. For example, administrators can identify the user accounts associated with an event, determine the chronological sequence of events. For audit log entries that have an associated job, you can click the hyperlinked job ID to go to the Jobs page, where you can view the details of the job.

About the Audit Logs Page

IN THIS SECTION

- [Tasks You Can Perform | 1029](#)

To access this page, select **Administration > Audit Logs**.

Use the Audit Logs page to view the tasks that you have initiated either by using the Juniper Security Director Cloud GUI or APIs. You can also export audit logs as a comma-separated values (CSV) file or a portable data format (PDF) file.

Tasks You Can Perform

You can perform the following tasks from this page:

- View the details of various user-initiated tasks by selecting **More > Details**. You can also mouse over the audit log and click on the **Detailed View** icon.
- Export audit logs as a CSV file or a PDF file—See "[Export Audit Logs](#)" on page 1031 .
- Sort and filter audit logs:
 - Click a column name to sort the audit logs based on the column name.
 - Click the filter icon and select whether you want to show or hide column filters or apply a quick filter. For example, you can use audit log filtering to track user accounts that were added on a specific date, track configuration changes across a particular type of device, view services that were provisioned on specific devices.
- Show or hide columns—Click the **Show Hide Columns** icon at the top right corner of the page and select the columns that you want to display on the Audit Logs page.

[Table 371 on page 1030](#) provides description of the fields on the Audit Logs page.

Table 371: Fields on the Audit Logs Page

Field	Description
Username	Displays the username of the user who initiated the task.
Object Name	Displays the name of the object on which the task was initiated. An object can be a tenant, site, device, device image, template, and so on.
Source IP	Displays the IP address of the client from which the user initiated the task. For tasks that do not have an associated user IP address, this field is blank.
Operation	Displays the name of the task that triggered the audit log. For example, create address, delete address, create NAT policy, and so on.
Description	Displays details about the task.
Status	<p>Displays the status of the task that triggered the audit log:</p> <ul style="list-style-type: none"> • Success—Job or task was completed successfully. • Failure—Job or task failed and was terminated. • Job Scheduled—Job is scheduled but has not yet started. • Recurring Job Scheduled—Recurring job is scheduled.
Logged Time	Displays the date and time at which the execution of the task was completed. This timestamp is stored in UTC time in the database, but is mapped to the local time zone of the client computer.

Table 371: Fields on the Audit Logs Page (Continued)

Field	Description
Job ID	<p>For tasks that have associated jobs, displays the ID of the job associated with the task.</p> <p>You can click the job ID to go to the Jobs page, where you can view the status of the job.</p>

Export Audit Logs

You can export audit logs as comma-separated values (CSV) file or portable document format (PDF). You can view and analyze the exported audit logs, as needed.

To export the audit logs:

1. Select **Administration > Audit Logs**.

The Audit Logs page appears displaying the audit logs.

2. Click **Export Logs** and select the format (CSV or PDF) for the exported logs.

You can export audit logs for a maximum of 180 days prior to the current date and time. For example, if the current date is July 1, 2021, you can export the audit logs starting from January 1, 2021.

3. Click **OK** to export the audit logs.

Depending on the settings of the browser that you are using and the format you selected, you can download the audit logs directly or save the file.

You are returned to the Audit Logs page.

After the file is downloaded, you can open the CSV or PDF file and analyze the logs as required.

Service Updates

IN THIS CHAPTER

- [About the Service Updates Page | 1032](#)

About the Service Updates Page

IN THIS SECTION

- [E-mail Notifications for Regular Updates and Maintenance | 1033](#)

To access this page, select **Administration** > **Service Updates**.

The **Service Updates** page contains a record of scheduled update activities that are planned for updating Security Director Cloud and its features. You can use the **Service Updates** page to trace the maintenance activities which are in-progress, completed or planned for future.

NOTE:

- When you subscribe to the e-mail notification for updates and maintenance activities, you receive the first notification seven days before the scheduled maintenance and the second notification three days before the scheduled maintenance.

And a final notification is sent 24 hours before the scheduled maintenance.

- When the maintenance activity is complete, you will receive an e-mail notification with details of the completion.

For more details on e-mail subscription, see "[E-mail Notifications for Regular Updates and Maintenance](#)" on page 1033 .

When an update is in progress, the GUI might not be available and displays a **We'll be right back** message.

E-mail Notifications for Regular Updates and Maintenance

You can subscribe to e-mail notifications for updates and maintenance activities of the Security Director Cloud and its features.

NOTE: The below message appears on the top-right banner of the GUI when a user is on-board for the first time:

To get notifications on updates and maintenance, click this icon and the option "Receive Update Notifications".

1. Click the user icon at the upper-right corner of the banner and select **Receive Update Notifications** option with a **No** in the parenthesis.

The **Receive Update Notifications** wizard appears.

NOTE: If you see **Receive Update Notifications** option with a **Yes** in the parenthesis, then you are already subscribed to the e-mail notifications.

2. Select **I want to receive email notifications on regular updates and maintenance** check box.
3. Click **OK**.

Jobs

IN THIS CHAPTER

- [Jobs Management in Juniper Security Director Cloud | 1034](#)
- [Jobs Main Page Fields | 1035](#)
- [Using Jobs in Juniper Security Director Cloud | 1037](#)
- [Viewing the Details of a Job in Juniper Security Director Cloud | 1037](#)
- [Canceling Scheduled Jobs in Juniper Security Director Cloud | 1039](#)

Jobs Management in Juniper Security Director Cloud

A job is an action that is performed on any object that is managed by Juniper Security Director Cloud, such as a device, service, or user. On the Jobs page, you can monitor the status of jobs that have run or are scheduled to run in Juniper Security Director Cloud. Jobs can be scheduled to run immediately or in the future.

Depending on the settings in your user account or remote profile, you can view only your own jobs or all jobs.

NOTE: A user with the Super Administrator or Job Administrator role assigned can view all jobs triggered by all users.

Juniper Security Director Cloud maintains a history of job status for all jobs. When a job is initiated, Juniper Security Director Cloud assigns a unique ID to that job, which serves to identify the job, along with the job type on the Jobs page. The following is a list of some of the job types supported in Juniper Security Director Cloud:

- Device management—Device onboarding, license installation, security package installation, security certificate importation and installation, software image upgradation, and device deletion.
- Firewall—Automatic importation, manual importation, preview, deployment, and deletion.

- NAT—Automatic importation, manual importation, preview, deployment, and deletion,
- IPSec VPN—Importation, preview, deployment, and deletion.
- Active Directory—Preview and deployment.
- JIMS profiles—Preview and deployment.
- Access profiles—Preview and deployment.
- User role—Creation.
- Subscriptions—Addition and deletion.
- Policy hits.

Jobs Main Page Fields

Use this page to view jobs and cancel scheduled jobs. You can retry jobs that failed. You can filter and sort the jobs displayed, and view details of each job. [Table 372 on page 1035](#) describes the fields on this page.

Table 372: Jobs Main Page Fields

Field	Description
All	
Job Name	The name of the job. For most jobs, the job type is assigned as the name.
Status	The state of the job execution: <ul style="list-style-type: none"> • Success—The job completed successfully. • Failure—The job failed and was terminated. • In Progress—The job is in progress.
Owner	The email address of the owner who initiated the job.

Table 372: Jobs Main Page Fields (Continued)

Field	Description
Start Time	The time when the job is started.
End Time	The time when the job was completed or terminated if the job execution failed.
Job ID	The unique identifier of the job.
Scheduled	
Name	The name of the job. For most jobs, the job type is assigned as the name.
Owner	The email address of the owner who initiated the job.
Status	The state of the job execution: <ul style="list-style-type: none"> • Scheduled—The job is scheduled to run in the future. • Success—The job completed successfully. • Failed—The job failed and was terminated. • In Progress—The job is in progress. • Cancelled—The job was canceled by a user.
Next Run Time	The date and time when the job is scheduled to start. NOTE: The time is stored as UTC time in the database but mapped to the local time zone of the client from which the UI is accessed.
UUID	The unique identifier of a job. You can use the UUID to fetch a relevant job from Juniper Security Director Cloud.

Using Jobs in Juniper Security Director Cloud

Use the Jobs page to view all that jobs that have been scheduled to run or have run from Juniper Security Director Cloud. By default, jobs are sorted by the Scheduled Start Time column. Depending on your user account settings, you can view all jobs or only your jobs.

Before You Begin

- Read the ["Jobs Management in Juniper Security Director Cloud" on page 1034](#) topic.
- Review the Jobs main page for an understanding of the existing jobs See ["Jobs Main Page Fields" on page 1035](#) for the field descriptions.

1. Click **Administration** > **Jobs**.

The Jobs page opens.

2. Use the guidelines provided in [Table 373 on page 1037](#) to learn about the page.

Table 373: Jobs Page Actions

Action	Guideline
View the details of a job	View the details of a job, such as the tasks involved in each job. See "Viewing the Details of a Job in Juniper Security Director Cloud" on page 1037 .
Retry Job	Try to complete failed jobs again. From the More menu, click Retry Job .
Cancel jobs	Select one or more scheduled or in-progress jobs on the Scheduled tab. See "Canceling Scheduled Jobs in Juniper Security Director Cloud" on page 1039 .

Viewing the Details of a Job in Juniper Security Director Cloud

You can view the details of a job, which allows you to view information about the job at a quick glance on one page, from the Jobs page.

1. Click **Administration** > **Jobs**.

The Jobs page opens.

2. Select the job, and from the More menu, select **View Job Details**.

The Job Status page opens. The fields displayed vary depending on the job.

[Table 374 on page 1038](#) describes some of the fields on the Job Status page.

3. Click **OK**.

The Jobs page opens.

Table 374: Job Status Fields

Field	Description
Details	
Name	The name of the job. For most jobs, the job type is assigned as the name.
Status	The state of the job execution: <ul style="list-style-type: none"> • Tasks Succeeded—The tasks related to the job that successfully completed. • Tasks Failed—The tasks related to the job that failed. You can expand each task to view the subtask details.
Start Time	The time when the job is started. NOTE: The time is stored as UTC time in the database but mapped to the local time zone of the client from which the UI is accessed.
End Time	The time when the job was completed or terminated if the job execution failed.
Owner	The owner of the job can be the system or the user who started the job.
Job ID	The unique identifier of the job.
Tasks	
Tasks Succeeded	The status of the individual tasks that are executed for the job.

Table 374: Job Status Fields *(Continued)*

Field	Description
Tasks Failed	The status of the individual tasks that failed to execute for the job.

Canceling Scheduled Jobs in Juniper Security Director Cloud

You can cancel the jobs that are scheduled for execution. You can cancel jobs only before their scheduled start time, not the jobs that are already in progress.

If you are an administrator, you can cancel jobs scheduled by any user. If you are assigned a role that does not allow you to cancel any job, you cannot cancel any jobs.

1. Click **Administration > Jobs**.

The Jobs page opens.

2. Click the **SCHEDULED** tab.

3. Select the job, and click **Cancel**.

A confirmation message is displayed.

4. Click **Yes** to confirm that you want to cancel the selected jobs.

The Jobs page opens, and the status of the jobs that were canceled changes to **Canceled**.

Data Management

IN THIS CHAPTER

- [About the Data Management Page | 1040](#)
- [Export Log Data | 1042](#)
- [Delete Device Logs | 1042](#)

About the Data Management Page

IN THIS SECTION

- [Tasks You can Perform | 1041](#)
- [Field Descriptions | 1041](#)

To access this page, click **Administration > Data Management**.

The Data Management page displays device logs related to security and data traffic. You can export these logs generated up to the past one week or one month, while you can delete the logs that are older than one week, one month, or one year. Juniper Security Director Cloud exports log data in the CSV format.

NOTE: After 60% of your licensed storage capacity is consumed, Juniper Security Director Cloud notifies you in the following manner to purchase additional storage or free up storage:

- Displays notifications when you log in to the portal.
- Sends e-mail notifications every two hours.

If you do not purchase additional storage or free up the existing storage after your storage usage reaches 90% of the capacity, Juniper Security Director Cloud automatically deletes data based on first-in-first-out basis to reduce the storage usage to 70%.

Tasks You can Perform

You can perform the following tasks from this page:

- Export the device logs related to security and data traffic from Juniper Security Director Cloud. See ["Export Log Data" on page 1042](#) .
- Delete the device logs to free up storage. See ["Delete Device Logs" on page 1042](#) .

Field Descriptions

Table 375: Fields on the Data Management Page

Field	Description
Action	The type of action selected.
Time Range Selected	The period of logs selected to either export or delete.
Status	The status of the export or delete job. Click View Job to view the job status details.
Activity Completed On	The time when the export or delete job completes.
Action Taken By	The user who starts the export or delete job.
Download	The option to download the logs in the CSV format. Click Download Data in export-related jobs to download the logs.

Export Log Data

You can export log data as CSV files. You can export log data for the last one week, one month, or a custom date range.

NOTE: If you are using a Juniper Security Director Cloud trial subscription, you can export the log data only for the last one week.

1. Click **Administration > Data Management**.

The **Data Management** page is displayed.

2. Select **Export log data**.

3. Select the time range of the log data you want to export.

4. Click **Export log data**.

- If you selected **Custom**, the **Export Data** page is displayed.
- If you selected **Last 1 week** or **Last 1 month**, a job is created and displayed in the **Data Management Activity** table. You can click **View Job** to view the details of the export job and click **Download Data** to download the CSV file after the job is complete.

5. If the **Export Data** page is displayed, select the required date range and click **OK**.

A job is created and displayed in the **Data Management Activity** table. You can click **View Job** to view the details of the export job and click **Download Data** to download the CSV file after the job is complete.

Delete Device Logs

You can delete the device logs older than one week, one month, or one year.

If you are using a Juniper Security Director Cloud trial subscription, you cannot delete device logs.

1. Select **Administration > Data Management**.

The **Data Management** page opens.

2. Select **Delete log data** as the action.

3. Select the period of the logs to delete from the **Time range**.

4. Click **Delete log data**.

Juniper Security Director Cloud creates a job in the **Data Management Activity** section. You can click **View Job** to view the details of the delete job.

Log Streaming

IN THIS CHAPTER

- [About the Log Streaming Page | 1043](#)
- [Add a Log Stream | 1045](#)
- [Edit and Delete a Log Stream | 1045](#)

About the Log Streaming Page

IN THIS SECTION

- [Tasks You Can Perform | 1043](#)
- [Field Descriptions | 1044](#)

To access the Log Streaming page, click **Administration > Log Streaming**.

Log streaming supports forwarding of audit logs, session logs, and security events to an external Security Information and Event Management (SIEM) system. Microsoft Sentinel is currently supported.

Streaming logs from Juniper Secure Edge cloud results in data transfer charges.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a log stream. See ["Add a Log Stream" on page 1045](#)
- Edit and delete a log stream. See ["Edit and Delete a Log Stream" on page 1045](#)

Field Descriptions

Table 376 on page 1044 provides guidelines on using the fields on the Log Streaming page.

Table 376: Fields on the Log Streaming Page

Field	Description
Log Streams	
Name	Specifies the name of the log stream.
Log Type	The type of log to forward to the external SIEM system. You can forward audit logs, session logs, and security events to Microsoft Sentinel. The data forwarded to SIEM system is in JSON format.
Connection Type	The type of external SIEM system to which you can transfer the logs. By default, the connection type is Microsoft Sentinel.
Status	Specifies if the log forwarding is enabled.
Status	
Log Stream Name	Specifies the name of the log stream.
Current Status	Specifies the current status of the logs forwarded to the external SIEM system.
Bytes Sent this Month	Specifies the total bytes forwarded to the external SIEM system in the current month.
Last Failure Time	Specifies the time when any logs failed to be sent to the external SIEM system.

Add a Log Stream

Configure the type of log to forward to the external SIEM system. You can also enable or disable the log stream.

To add a log stream:

1. Select **Administration > Log Streaming**.

2. Click **+**.

The Add Log Stream page is displayed.

3. Enter the log stream name.

4. Select the log type to forward to the external SIEM system.

You can forward audit logs, session logs, or security events. By default, the connection type is MSSentinel.

5. Enter the workspace ID associated with MSSentinel.

6. Enter the primary key associated with MSSentinel.

7. Click **Test** to verify if the connection to the external system is successful.

8. Click **OK**.

The added log stream is displayed on the Log Streaming page.

Edit and Delete a Log Stream

IN THIS SECTION

● [Edit a Log Stream | 1045](#)

● [Delete a Log Stream | 1046](#)

Edit a Log Stream

1. Select **Administration > Log Streaming**.

The Log Streaming page is displayed.

2. Select a log stream and click the pencil icon.

The Edit Log Stream page is displayed.

3. Edit the required fields.

4. Click **OK**.

Delete a Log Stream

1. Select **Administration** > **Log Streaming**.

The Log Streaming page is displayed.

2. Select a log stream and click the delete icon.

A confirmation page is displayed.

3. Click **Yes** to delete the log stream.

URL Recategorization

IN THIS CHAPTER

- [About the URL Recategorization Page | 1047](#)
- [Request URL Recategorization | 1049](#)

About the URL Recategorization Page

IN THIS SECTION

- [Tasks You Can Perform | 1047](#)
- [Field Descriptions | 1048](#)

To access this page, select **Administration > URL Recategorization**.

Use the URL Recategorization page to request to change a URL's category. You can also view the status of URL recategorization requests.

NOTE: You can request URL recategorization only for the predefined Juniper NextGen URL categories.

Tasks You Can Perform

You can perform the following tasks from this page:

- Request URL recategorization. See "[Request URL Recategorization](#)" on page 1049 .
- Delete a URL recategorization request. To do this:

1. Select the URL which you want to delete and then click the delete icon (trash can).

An alert message appears, verifying that you want to delete the URL.

2. Click **Yes** to delete the URL. If you do not want to delete, click **Cancel** instead.

If you click **Yes**, the selected URL recategorization request is deleted.

- Add and hide advanced filter.

To add filters:

1. Click the filter icon and then select **Show advanced filter**.

The Add Criteria window opens.

2. Select the values for Field and Conditions from the list.

3. Enter the value for the selected field and conditions.

4. Click **Add** and then click **Save**.

The Save Filter page opens.

5. Enter a filter name. If you want to make this saved filter as default, then enable **Set as default**.

The filter is saved.

NOTE: Click **X** to clear the saved filters.

6. Click **Close** once the successful message is displayed.

To hide a filter, click the filter icon and then select **Hide advanced filter**.

- Show or hide the columns displayed on the page. To do this, click the vertical ellipses on the upper-right corner of the page and then select **Hide/Show Columns**. Then, select the columns that you want to display on the table.
- Reset the displayed columns to the default set of columns for each tab in the table. Hover over the vertical ellipses and select **Reset Preference**.

Field Descriptions

[Table 377 on page 1049](#) describes the fields on the URL Recategorization page.

Table 377: URL Recategorization Page Fields

Field	Description
URL	Displays the URL for which you requested the recategorization.
Request Type	Displays the request was for recategorizing a URL.
Requested Category	Displays the predefined Juniper NextGen categories that you requested for recategorization.
Status	<p>Displays if your request is successful, rejected, or deleted.</p> <p>Once the request is submitted, the status shows as Your request is being processed. The request takes approximately 24 hours to undergo review and update the corresponding status.</p>
Timestamp	Displays the date and time details when the URL recategorization was requested.
Requested By	Displays the user email ID who requested for URL recategorization.

RELATED DOCUMENTATION

[About the Web Filtering Profiles Page | 401](#)

Request URL Recategorization

To access this page, select **Administration > URL Recategorization**.

Use the Request URL Recategorization page to request to change a URL's category.

NOTE: You can request URL recategorization only for the predefined Juniper NextGen URL categories.

To request for URL recategorization:

1. Select Administration > URL Recategorization.

The URL Recategorization page opens.

2. Click Request URL Recategorization.

The Request URL Recategorization page opens.

3. Configure the fields on the Request URL Recategorization page according to the guidelines in [Table 378 on page 1050](#).

Table 378: Fields on the Request URL Recategorization Page

Field	Description
Recategorize URL	<p>Do the following:</p> <ol style="list-style-type: none"> 1. Click +. 2. Enter the following details: <ul style="list-style-type: none"> • URL—Enter the URL domain name or IP address. For example: www.abc.com or https://xyz.xy.xy.xy. • Category—Select the predefined Juniper NextGen URL category from the list to which you want to add the URL. 3. Click the tick icon below the row once done with the configuration. 4. Click Submit.

RELATED DOCUMENTATION

[About the URL Recategorization Page](#) | 1047

Organization

IN THIS CHAPTER

- [About the Organization Page | 1051](#)
- [Create an Organization | 1054](#)
- [Edit and Delete an Organization | 1056](#)

About the Organization Page

IN THIS SECTION

- [Tasks You Can Perform | 1051](#)
- [Field Descriptions | 1052](#)

To access this page, click **Administration>Organizations**.

An organization account helps you to add devices, subscribe your devices, and start managing the devices. An administrator, operator, or user with read-only access of organization can create multiple organization accounts in Juniper Security Director Cloud.

Having multiple organization accounts can help you to segregate large groups into smaller, more manageable groups and control administrative access. For example, you can have different organization accounts based on location or business units. When an organization is not functional or no longer required due to business situation, you can delete an organization account. Deleting an organization account will remove the entire organization including its devices, user accounts, reports, and logs.

Tasks You Can Perform

- Create new organization. See "[Create an Organization](#)" on page 1054 .

- Edit and delete an organization. See ["Edit and Delete an Organization" on page 1056](#) .

Field Descriptions

[Table 379 on page 1052](#) displays the fields on the Organization page.

Table 379: Fields on the Organization Page

Field	Description
Details	
Organization account name	The name of the organization.
Home PoP	<p>The home region, which is usually the geographical area where your SRX Series Firewalls are located.</p> <p>NOTE: Make sure that each of the SRX Series Firewall ports can communicate with an FQDN of Juniper Security Director Cloud . The FQDN of each home region is different.</p> <p>Table 103 on page 223</p>
Organization ID	The auto-generated universally unique identifier (UUID) for an organization. This unique ID is used to identify organizations that have identical name.
Settings	
Allow Juniper support to debug	Enable to allow the Juniper Networks support team to remotely troubleshoot and resolve issues.
Auto-import device after device discovery	<p>Enable to automatically import firewall and NAT policies when the device discovery process completes successfully.</p> <p>This setting is enabled by default.</p>

Table 379: Fields on the Organization Page (Continued)

Field	Description
Update disabled rules to device	<p>Enable to automatically delete rules on the device when the rules are disabled in Juniper Security Directory Cloud.</p> <p>This setting is disabled by default.</p>
Hit count	<p>Enable to track the number of times a policy is used based on traffic flow. The hit count is the number of hits since the last reset.</p> <p>The hit count is especially useful to check the usage frequency of the rules in a large policy set. If you see that some of the rules are not being used, you can verify that the rules are not being shadowed by another policy. This helps you manage the device without having to generate traffic manually.</p> <p>This setting is enabled by default.</p>
Hit count start time	<p>Set the time from when the policy use must be tracked.</p> <p>The hit count collects the policy use statistics every 24 hours and updates the count to all the policies. The default start time is 0200 hours.</p>
Save rule option	<p>While creating or editing a security policy rule, allow user to select if the rule is a zone-based rule or a global rule. This option is available only when the user selects a single source zone and a single destination zone.</p>
Unnumbered tunnels	<p>Enable to import unnumbered, matching tunnels as Site-to-Site topology. If this setting is disabled, the tunnels are imported as Hub-and-Spoke topology.</p> <p>This setting is disabled by default.</p>

Table 379: Fields on the Organization Page *(Continued)*

Field	Description
Snapshots per policy	<p>Set the number of configuration snapshots that must be stored for each device. You can use the snapshots to revert to a previous configuration of a device.</p> <p>Juniper Security Director Cloud stores the upto latest 10 snapshots.</p>
Automatic Signature Install to Devices	<p>Enable automatic installation of IPS signature, application signature, and URL category to the devices.</p> <p>This setting is enabled by default.</p>
Delete unused address and address groups	<p>Enable to automatically delete addresses and address groups on the devices when they are deleted in Juniper Security Director Cloud.</p> <p>This setting is enabled by default.</p>
Delete unused services and service groups	<p>Enable to automatically delete services and service groups on the devices when they are deleted in Juniper Security Director Cloud.</p> <p>This setting is enabled by default.</p>

RELATED DOCUMENTATION

[Users Overview](#) | 1013

Create an Organization

You must have a subscription (or multiple subscriptions as required) to create an organization. For more details, see "[Subscriptions Overview](#)" on page 1007 .

To create an organization:

1. From any of the pages, click the drop-down next to the organization name on the top right corner.

The create new organization page opens.

2. Click the **Create New Organization** link.

The Create New Organization page opens.

3. Configure the following fields:

- **Organization name**—Enter the organization account name. The organization account name must not be more than 32 characters. The string can contain alphanumeric characters hyphen(-) and underscore(_).
- **Home PoP**—Select your home region. The home region is usually the geographical area where your SRX Series Firewalls are located. Technically, you can select any region, but we recommend you select the region that is closest to your geographical location.

NOTE: The Juniper Security Director Cloud FQDN of each home region is different. You must configure your network firewall to allow access to the FQDN.

Make sure that each of the SRX Series Firewall ports can communicate with an FQDN of Juniper Security Director Cloud . The FQDN of each home region is different.

Table 380: Home Region to FQDN Mapping

Region	Purpose	Port	FQDN
North Virginia	ZTP	443	jsec2-virginia.juniperclouds.net
	Outbound SSH	7804	srx.sdcloud.juniperclouds.net
	Syslog TLS	6514	srx.sdcloud.juniperclouds.net
Ohio	ZTP	443	jsec2-ohio.juniperclouds.net
	Outbound SSH	7804	srx.jsec2-ohio.juniperclouds.net

Table 380: Home Region to FQDN Mapping (Continued)

Region	Purpose	Port	FQDN
	Syslog TLS	6514	srx.jsec2-ohio.juniperclouds.net

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

An account creation confirmation message is displayed. You will be navigated to dashboard page of the new organization.

5. Customize your organization by following the guidelines provided in [Table 379 on page 1052](#).
6. Click **Save**.

Edit and Delete an Organization

IN THIS SECTION

- [Edit an Organization | 1056](#)
- [Delete an Organization | 1058](#)

Edit an Organization

An administrator or user with required privileges can edit the organization's settings.

To edit an organization's settings:

1. Click **Administration > Organization**.

The Organization page opens.

2. Modify the organization account name.

- **Organization name**—Enter the organization account name. The organization account name must not be more than 32 characters. The string can contain alphanumeric characters hyphen(-) and underscore(_).

- **Home PoP**—Select your home region. The home region is usually the geographical area where your SRX Series Firewalls are located. Technically, you can select any region, but we recommend you select the region that is closest to your geographical location.

NOTE: The Juniper Security Director Cloud FQDN of each home region is different. You must configure your network firewall to allow access to the FQDN.

Make sure that each of the SRX Series Firewall ports can communicate with an FQDN of Juniper Security Director Cloud . The FQDN of each home region is different.

Table 381: Home Region to FQDN Mapping

Region	Purpose	Port	FQDN
North Virginia	ZTP	443	jsec2-virginia.juniperclouds.net
	Outbound SSH	7804	srx.sdcloud.juniperclouds.net
	Syslog TLS	6514	srx.sdcloud.juniperclouds.net
Ohio	ZTP	443	jsec2-ohio.juniperclouds.net
	Outbound SSH	7804	srx.jsec2-ohio.juniperclouds.net
	Syslog TLS	6514	srx.jsec2-ohio.juniperclouds.net

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

A confirmation message is displayed.

4. Modify your organization's settings by following the guidelines provided in [Table 379 on page 1052](#) .

5. Click **Save**.

Delete an Organization

An administrator or user with required privileges can delete an organization.

NOTE: If you delete an organization, entire organization including its devices, user accounts, reports and logs will be removed. This action will be permanent and the data will not be recoverable.

To delete an organization account from Juniper Security Director Cloud:

1. Click **Administration > Organization**.

The organization page opens.

2. Click the **Delete Organization** button.

A message asking you to confirm the delete operation is displayed.

3. Click **Delete Organization** to delete the organization account.

A confirmation message is displayed.

ATP Mapping

IN THIS CHAPTER

- [About the ATP Mapping Page | 1059](#)
- [Map an Existing ATP Realm to Juniper Security Director Cloud | 1060](#)
- [Map an Auto-generated Realm to Secure Edge | 1061](#)

About the ATP Mapping Page

IN THIS SECTION

- [Tasks You Can Perform | 1059](#)

A security realm is a group identifier for an organization that is used to restrict access to Web applications. You can access ATP related screens in the portal after mapping an ATP realm to Juniper Security Director Cloud or Secure Edge.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a new ATP realm—See ["Map an Auto-generated Realm to Secure Edge" on page 1061](#) .
- Map an existing ATP realm—See ["Map an Existing ATP Realm to Juniper Security Director Cloud" on page 1060](#) .
- Delete an existing realm—To remove an existing realm, click **Delete ATP**.

Map an Existing ATP Realm to Juniper Security Director Cloud

If you have already created a realm in ATP Cloud, you can map it to Juniper Security Director Cloud from the **Advanced Threat Prevention (ATP)** page. You can access ATP related screens in the portal only when you map an ATP realm to Juniper Security Director Cloud.

To map an existing ATP realm to Juniper Security Director Cloud:

1. Select Administration > ATP Mapping.

The Advanced Threat Prevention (ATP) page appears displaying a message that no ATP is created or mapped.

2. Click Map an Existing ATP Realm.

The Map an Existing ATP Realm page appears.

3. Complete the configuration according to the guidelines in [Table 382 on page 1060](#).

NOTE: Fields marked with an asterisk (*) are mandatory.

Table 382: Map Existing ATP Realm Settings

Setting	Guideline
Realm	Enter a name for the security realm. This should be a name that is meaningful to your organization. A realm name can only contain alphanumeric characters and the dash symbol. Once created, this name cannot be changed.
Email ID	Enter the e-mail address for the realm. The email address will be used as the user name to log in to the realm.
Password	Enter the password for the realm. The password must be a unique string with at least 8 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 user name.

4. Click OK.

A message is displayed indicating whether the ATP mapping is done successfully or not. If ATP mapping is successful, then the ATP page displays the region and realm details. You can access all ATP related screen in Juniper Security Director Cloud.

Map an Auto-generated Realm to Secure Edge

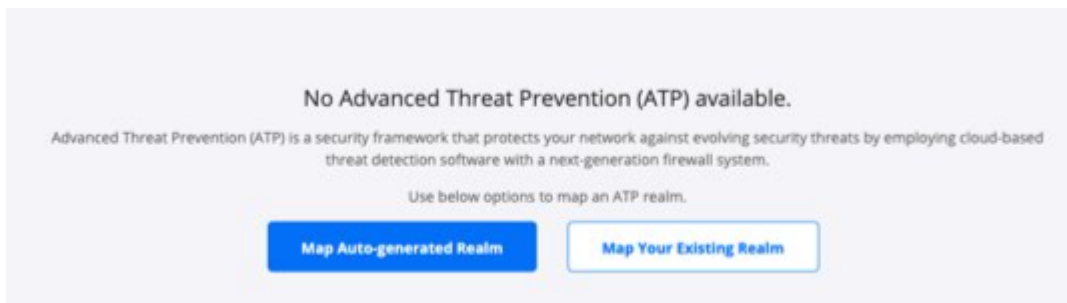
If you do not have an ATP realm configured, you can map an auto-generated realm to Secure Edge.

To map an auto-generated realm:

1. Select **Administration > ATP Mapping**.

The Advanced Threat Prevention (ATP) page appears displaying a message that no ATP is available.

Figure 31: ATP Mapping



2. Click **Map Auto generated Realm**.

The Map Auto-generated Realm page appears.

The ATP realm will be mapped to Secure Edge automatically.

ATP Audit Logs

IN THIS CHAPTER

- [About the ATP Audit Logs Page | 1062](#)
- [Export Audit Logs | 1063](#)

About the ATP Audit Logs Page

IN THIS SECTION

- [Tasks You Can Perform | 1062](#)

To access this page, select **Administration > ATP Audit Logs**.

Use the ATP Audit Logs page to view the information about the login activity and specific tasks that were completed successfully using the ATP Cloud Web Portal. Audit log entries include details about user-initiated tasks, such as the username, task name, task details, and date and time of execution of the task.

Tasks You Can Perform

You can perform the following tasks from this page:

- Export audit logs as a CSV file –See "[Export Audit Logs](#)" on page 1063 .
- Sort and filter audit logs:
 - Click a column name to sort the audit logs based on the column name.
 - Click the filter icon and select whether you want to show or hide column filters or apply a quick filter.

- Click **Timespan** and select the range to filter the audit logs.
- Search for audit logs by using keywords—Click the search icon. Enter partial text or full text of the keyword in the search bar and click the search button or press **Enter**. The search results are displayed.
- Show or hide columns—Click the Show Hide Columns icon at the top right corner of the page and select the columns that you want to display on the ATP Audit Logs page.

[Table 383 on page 1063](#) provides description of the fields on the ATP Audit Logs page.

Table 383: Fields on the ATP Audit Logs Page

Setting	Guideline
Timestamp	Timestamp for the audit log file that is stored in UTC time in the database but mapped to the local time zone of the client computer.
User Name	Username of the user that initiated the task.
Action	Name of the task that triggered the audit log.
Details	Detailed information about the task performed. Click the details link to view more details about the task.

Export Audit Logs

You can export audit logs as comma-separated values (CSV) file. You can view and analyze the exported audit logs, as needed.

To export the audit logs:

1. Select **Administration > ATP Audit Logs.**

The Audit Logs page appears displaying the audit logs.

2. Click **Export.**

The Set Date Range for Export page appears.

3. Specify the export type and the time period for which you want to export the audit logs according to the guidelines provided in [Table 384 on page 1064](#).

4. Click **OK** to export the audit logs.

Depending on the settings of the browser that you are using, the CSV file containing the audit logs for the specified time period is either downloaded directly, or you are asked to open or save the file.

You are returned to the ATP Audit Logs page.

After the file is downloaded, you can open the CSV file in any application and view and analyze the logs as required.

Table 384: Fields on the Set Date Range for Export Page

Field	Description
Export Type	<ul style="list-style-type: none"> • Export All—Select to export all audit logs. • Export for a specified period—Select to export audit logs for a specific time range. If you select this option, you must specify the start date and end date.
Start Date	Specify the date (in MM/DD/YYYY format) from when the audit logs should be exported.
End Date	Specify the date (in MM/DD/YYYY format) up to when the audit logs should be exported.